CSD | CENTER FOR THE STUDY OF DEMOCRACY

Shadow Alliances

Authoritarian Powers and the Hybrid Warfare Nexus in Latin America

Shadow Alliances

Authoritarian Powers and the Hybrid Warfare Nexus in Latin America

CSD
CENTER FOR
THE STUDY OF
DEMOCRACY

This report analyzes how Russia, China, and Iran have entrenched their influence in Latin America through a hybrid warfare strategy that leverages economic statecraft and transnational criminal networks. They often combine licit and illicit channels into an integrated system of influence, seeking to upend the global balance of power by seizing strategic assets, evading sanctions, and perpetuating fragile governance structures in the region.

Building on the Kremlin Playbook framework, the report identifies a sequenced strategy - from legitimate economic entry points to the expansion of illicit, covert and criminal-enabled operations. Transnational criminal networks provide logistics, financing, and credible deniability of direct complicity, further eroding democratic resilience and checks and balances.

Authors:
Martin Vladimirov, Director, Geoeconomics Program, Center for the Study of Democracy
Sara Gálvez, Analyst, Geoeconomics Program, Center for the Study of Democracy
Brendon Zhan, Analyst, Geoeconomics Program, Center for the Study of Democracy

ISBN: 978-954-477-559-9

2026, Center for the Study of Democracy

CONTENTS

LIST OF FIGURES

LIST OF BOXES

LIST OF ABBREVIATIONS

AIS	Automatic Identification System
BRICS	Brazil, Russia, India, China, South Africa
CANTV	Compañía Anónima Nacional Teléfonos de Venezuela
CLAP	Local Committees for Supply and Production
CGTN	China Global Television Network
EMTRASUR	Empresa de Transporte Aerocargo del Sur
GLONASS	Global Navigation Satellite System
GRU	Main Directorate of the General Staff of the Armed Forces of the Russian Federation
IRGC	Islamic Revolutionary Guard Corps
IRIB	Islamic Republic of Iran Broadcasting
NIOEC	National Iranian Oil Engineering and Construction Company
NIORDC	National Iranian Oil Refining and Distribution Company
OECD	Organization for Economic Co-operation and Development
PDVSA	Petróleos de Venezuela, S.A.
PPP	Public-Private Partnership
PRC	People's Republic of China
RT	Russia Today
SADRA	Iran Marine Industrial Company
SORM	System for Operative Investigative Activities
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TASS	Russian News Agency
TBML	Trade-Based Money Laundering
TOC	Transnational Organized Crime
UAV	Unmanned Aerial Vehicle
USDT	Tether
VVER-1200	Water-Water Energetic Reactor-1200
Xinhua	Xinhua News Agency

ACKNOWLEDGMENTS

This report builds upon the Center for the Study of Democracy's (CSD) decade-long research into the different dimensions of foreign malign influence projected by authoritarian states such as Russia, China and Iran. The assessment is the first CSD study in Latin America on hybrid warfare models that exploit the grey zone between licit and illicit tools of statecraft. Examining the convergence between criminal activities and foreign policy across the region has required a substantial effort from an international team of experts and partners whose regional expertise and sustained engagement have been indispensable.

We would like to express sincere gratitude to our partners for their contributions, including

- Vladimir Rouvinski, (ICESI University, Colombia);
- Guadalupe Correa-Cabrera (George Mason University, United States);
- Alejandro Cassaglia (the Global Initiative Against Transnational Organized Crime, Argentina);
- Henry Oporto and Ricardo Calla (Fundación Milenio, Bolivia)
- Christi Rangel and Mercedes De Freitas (Transparencia Venezuela).

Their expertise has been essential in grounding this report's analysis in the specific political, economic, and criminal dynamics shaping the region.

We are grateful to Brian Fonseca (Florida International University) for the collaboration in co-organizing the 11th annual Hemispheric Security Conference in Miami.

This assessment would not have been possible without the generous support of the National Endowment for Democracy, and its ongoing engagement and discussions on the intersection of authoritarian influence, illicit networks, and democratic resilience in Latin America.

The content and analysis in this report have also been enriched by our in-depth conversations with Carrie Filipetti, Executive Director of the Vandenberg Coalition, and Michael Miklaucic, Senior Fellow at CSD.

CSD's Atanas Rusev, Director, Security Program, Tatyana Novossiolova, Senior Analyst, and Ryan McClaren, Analyst, helped shape the theoretical underpinning of the assessment, based on CSD's prior experience in analyzing the state – crime nexus in Europe. The analysis benefited immensely from the practical experience of CSD's Associate Fellow, Estefania Melendez, who has been advising the Venezuelan opposition about the malign foreign influence risks in the region.

Special thanks go to CSD's Geoeconomics and Security Programs and the interns Sebastian Hacking and Elouan Pannegeon, as well as to Vivian Moreno and Juan José Guarín of ICESI University, and Meng-Hao Li of George Mason University, whose assistance in preparing background analyses, gathering data, compiling references, organizing expert workshops and interviews has been crucial to the completion of this report.

EXECUTIVE SUMMARY

China, Russia and Iran have increasingly turned to covert and asymmetric means to project influence globally. One of the most concerning and under-examined dimensions of this strategy is the **deepening engagement with transnational criminal networks** (TNCs), particularly in regions where institutional weaknesses and governance deficits provide fertile ground for illicit activities. Latin America, with its entrenched corruption, pervasive organized crime, and limited state control over certain territories, has become a crucial theatre for this evolving strategy.

China, Russia, and Iran project influence in Latin America via a **hybrid model** – one that fuses licit economic engagement with illicit, covert, and criminal-enabled activities.

At the core of this model lies a **structural convergence** between state power and transnational organized crime. Rather than treating criminality as incidental or opportunistic, China, Russia, and Iran increasingly rely on criminal networks as functional enablers of their geopolitical strategies. These networks provide logistics, financial channels, access to illicit markets, and operational deniability. The result is a form of **state-sponsored or state-enabled criminality** embedded within broader strategies and practices of hybrid and irregular warfare.

This assessment identifies a recurring sequence of influence channels. **Formal economic channels**, including trade, infrastructure investment, energy cooperation, and financial agreements, provide access to strategic sectors and create long-term dependencies. Over time, these entry points enable the integration of opaque and illicit practices, including sanctions evasion, trade-based money laundering, illegal commodity flows, and covert financial operations. **Legal economic infrastructures** such as ports, logistics corridors, financial systems, and digital networks **have become dual-use platforms** that support both legitimate activity and illicit operations.

Transnational organized crime has come to play a central role in this system. Rather than exercising direct control, these external actors rely on **tactical, transactional relationships with criminal organizations** reinforcing and often aggravating existing local governance vulnerabilities and failures. These relationships allow them to access smuggling routes, informal financial systems, document forgery, and illicit markets without assuming direct responsibility. This model is insidious, as activities can shift across jurisdictions and adapt to enforcement pressure while maintaining plausible deniability.

Although China, Russia, and Iran follow different operational approaches, they converge around this same underlying logic, often mutually borrowing practices or sharing common interests. **China's model** is based on large-scale economic and institutional embedding. It builds influence through trade, infrastructure, finance, and technology, creating structural dependencies

that can later support less visible forms of leverage. **Russia** relies more heavily on political influence, information manipulation and pressure, and the integration with opaque financial and criminal networks to leverage its economic footprint, often concentrating on strategic sectors where limited economic presence can generate disproportionate leverage. **Iran** operates through decentralized, network-based tactics avoiding sanctions pressure, and relying most heavily on illicit finance and proxies, particularly those associated with Hezbollah.

Across these models, influence is mediated through complex **networks of intermediaries**. These include local political and business elites, large, procurement-heavy state-owned and private companies, media platforms, diaspora networks, and criminal organizations. These actors embed external influence within domestic systems, reduce its visibility, and ensure continuity even when political conditions change. Influence is therefore not imposed externally but integrated into existing political-economic networks of local economies, institutions, and governance structures.

Several key domains are used to operationalize hybrid influence. **Financial systems** play a critical role, particularly through trade-based money laundering, offshore corporate structures, and informal or opaque digital money transfer mechanisms. **Commodity sectors**, especially oil and gold, provide both revenue streams and channels for sanctions evasion. **Logistics and trade corridors** enable the movement of goods, funds, and personnel across borders while obscuring origin and destination. **Digital ecosystems** add an emerging layer, facilitating financial transactions, information manipulation, and operational coordination.

In some cases, these systems extend into **security and military domains**, relying on paramilitary forces and proxy networks to protect strategic assets or expand operational reach. Even where direct violence is limited, the presence of logistical and organizational infrastructures linked to paramilitary or even terrorist armed groups sustain latent operational capabilities that can be activated when strategically advantageous.

Latin America's persistent governance gaps, regulatory weaknesses, and high levels of informality create permissive environments in which **licit and illicit systems overlap**. At the same time, responses remain largely national, even when influence networks operate across borders. This mismatch allows hybrid systems to adapt, relocate, and persist despite enforcement efforts.

The effects are cumulative and structural. Hybrid influence distorts competition in key sectors, embeds opaque practices within formal economic systems, and weakens regulatory and institutional capacity. It creates long-term dependencies that shape policy choices and constrain strategic autonomy, often without requiring overt political alignment.

The convergence of these domains demands integrated responses. Traditional approaches that separate economic policy, anti-corruption efforts, financial oversight, and organized crime enforcement are no longer sufficient:

- A first priority is **improving understanding and coordination across institutions**. Intelligence services, financial authorities, law enforcement, and anti-corruption bodies need to operate within shared analytical frameworks that recognize hybrid influence as a single, interconnected threat.

- **Regional cooperation** is equally important. Hybrid networks operate across jurisdictions, exploiting uneven enforcement, regulatory gaps and arbitrage. Strengthening intelligence-sharing mechanisms, **financial oversight cooperation, and joint investigative capacities** would improve visibility and reduce fragmentation.

- Targeting **illicit financial and commercial infrastructures** is also essential. Disrupting trade-based money laundering, shell company networks, and informal financial systems requires a stronger focus on high-risk sectors such as energy, extractives, logistics, and free trade zones. Following financial flows and increasing transparency in these sectors can significantly constrain hybrid operations.

- Organized crime needs to be recognized as a **strategic component of foreign influence rather than solely a domestic security issue**. This implies adjusting investigative priorities, legal frameworks, and resource allocation to reflect its role within broader geopolitical competition.

- Finally, **strengthening economic governance** is critical. Many vulnerabilities originate in sectors where foreign investment's effects are modulated through weak regulation and political discretion. Improving investment screening, procurement transparency, and regulatory enforcement can reduce exposure to opaque arrangements while maintaining openness to legitimate economic cooperation.

Hybrid influence in Latin America is not episodic but systemic. It operates through the interaction of economic, political, and illicit mechanisms that reinforce one another over time. Addressing it will depend less on isolated policy measures than on the ability to connect existing tools into coherent, coordinated strategies that strengthen institutional resilience and reduce the space in which these networks operate.

CONVERGENCE OF POWER, CRIME, AND INFLUENCE

China, Russia, and Iran project influence in Latin America through a hybrid model[1] that fuses formal economic and political engagement with illicit and covert networks. Influence moves beyond conventional analyses of diplomacy and investment, as economic statecraft, criminal facilitation, and hybrid warfare practices reinforce one another.

The hybrid warfare and state criminality convergence is not based on incidental occurrences, but reflects a **structural pattern of behavior**. China, Russia, and Iran increasingly embed criminal practices within their geopolitical strategies, transforming illicit activity into an instrument of statecraft rather than a deviation from it. In this context, criminality should be understood as a tool deployed by the state to achieve strategic objectives.[2]

Applying this perspective to Latin America, influence is exercised through the deliberate and coordinated use of illicit networks, economic coercion, and covert operations to secure geopolitical leverage. These practices unfold within the broader operational environment of hybrid warfare, where state and non-state actors interact across blurred boundaries of legality, attribution, and sovereignty.

Economic statecraft and illicit activity function as mutually reinforcing components of a single system of influence. Formal investments in infrastructure, energy, and critical minerals create entry points into national economies, generating **structural dependencies and access to key assets**.[3] These footholds can then be leveraged to facilitate grey-zone activities, including sanctions evasion, trade-based money laundering, illicit commodity flows, and covert financial operations. Legal economic infrastructures such as ports, logistics corridors, financial institutions, and digital systems become dual-use platforms that enable both legitimate commerce and illicit transactions.

At the core of this model lies the state–crime nexus as a strategic interface. Direct control over criminal organizations is not typically exercised. Instead, flexible, transactional relationships with transnational criminal networks provide specialized services that advance state objectives.[4] These include logistical support (transport routes, smuggling corridors), financial intermediation (informal transfer systems, shell companies, crypto-assets),[5] and access to illicit markets (illegal mining, narcotics, oil smuggling). In return, criminal actors benefit from protection, access, and integration into broader economic and political ecosystems.

---

1 Shentov, O., Stefanov, R. and Vladimirov, M., *The Kremlin Playbook in Europe*, Sofia: Center for the Study of Democracy, 2020.

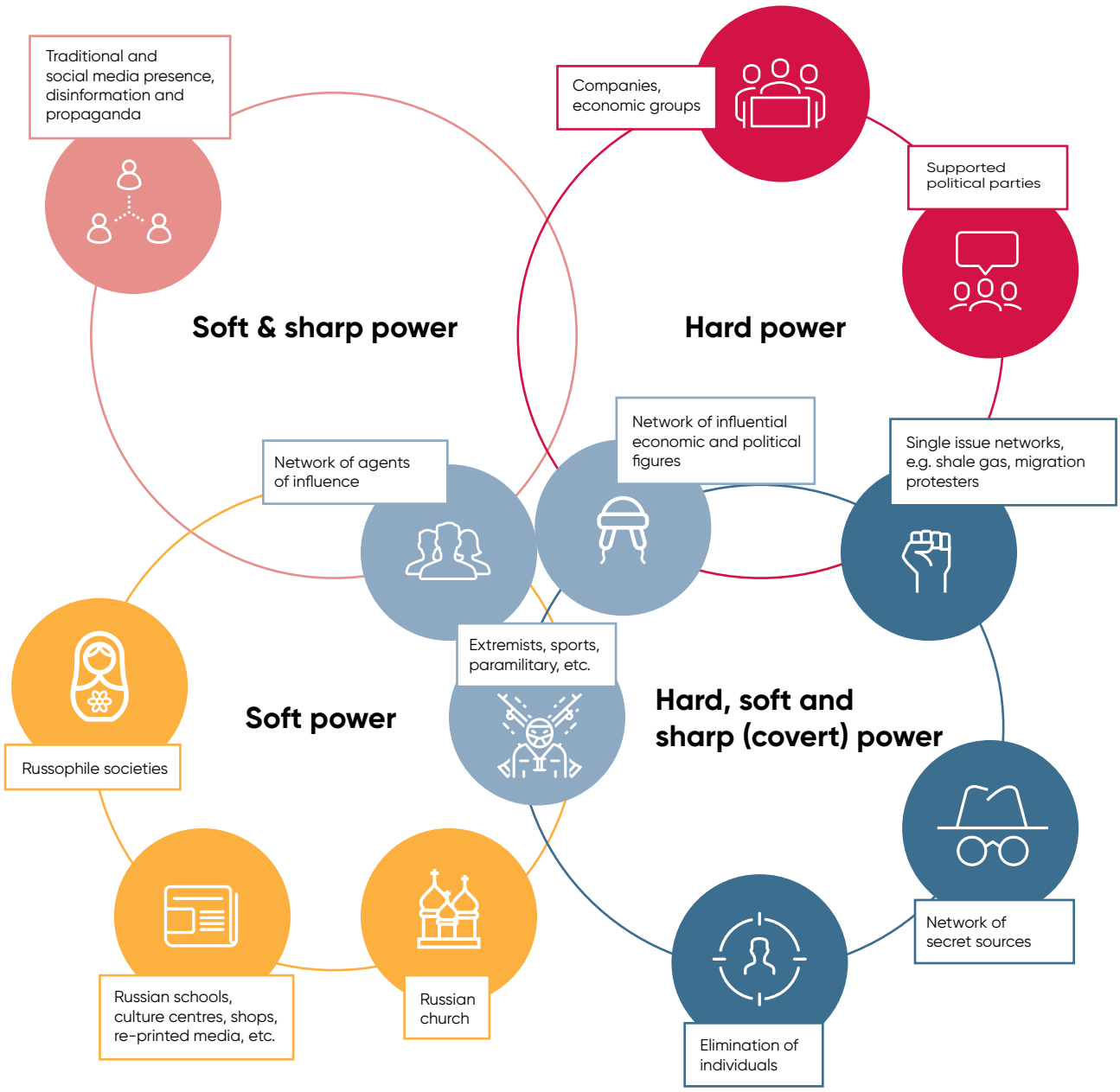
2 Rusev, A., McLaren, R., and Fito, E., *Shadow Fusions: The Convergence of Criminal Networks and the Russian State*, Sofia: Center for the Study of Democracy, 2025.

3 Vladimirov, M., Rueda, G., and Osipova, D., *Global Reach: The Kremlin Playbook in Latin America*, Sofia: Center for the Study of Democracy, 2024.

4 Koleva, R., and Rusev, A, *When States Go Rogue: Criminal Tools in Hybrid Warfare*, PRISM, Vol. 11, No.2, Spring, 2026.

5 Rusev, A. et al., *Financing of Organised Crime*, Sofia: Center for the Study of Democracy, 2015.

Figure 1. The Hybrid Warfare Power Mix



Source: CSD.

Hybrid warfare provides the operational logic for this convergence, enabling China, Russia, and Iran to deploy a mix of legal, semi-legal, and illegal instruments while maintaining plausible deniability. Criminal networks, private intermediaries, and corporate actors become part of layered influence architectures that translate geopolitical intent into operational capability.[6] Geographically, this convergence is most visible in environments characterized by governance gaps, weak regulatory frameworks, and high levels of informality, which are conditions that prevail across significant parts

[6] Triplett, H., "The US is Already Losing the Next War", *The National Interest*, June 16, 2025.

of Latin America.[7] In such contexts, licit and illicit systems frequently overlap, particularly in sectors such as energy, mining, logistics, and trade.

Influence is mediated through a diverse ecosystem of **enablers**, including political and business elites, state-owned and private companies, diaspora and cultural networks, media platforms, and criminal organizations. These intermediaries provide access to key nodes of power while ensuring operational flexibility and deniability.

While their strategies vary, they converge around the same underlying logic. **China** emphasizes institutional and economic embedding, operating primarily through formal channels but benefiting from weak regulatory environments. Beijing's approach to integrating organized crime into its statecraft involves both cyber and traditional criminal activities. Chinese cybercriminals have been co-opted by state intelligence agencies to conduct cyber espionage against foreign governments and corporations. This collaboration enables China to acquire sensitive information and intellectual property, bolstering its economic and strategic positioning on the global stage. In addition, China has used illicit networks to extend its reach, particularly in Southeast Asia, Africa, and Latin America.

Russia relies more heavily on coercive instruments, disinformation, and the direct integration of criminal and proxy networks into its statecraft.[8] Under Putin, the Kremlin has not merely tolerated organized crime but has absorbed and weaponized it, turning criminal actors into functional arms of hybrid warfare. Russian criminal networks, oligarch-linked intermediaries, mercenary formations, cybercriminals, and informal proxy actors provide the state with deniable capabilities for sabotage, smuggling, sanctions evasion, illicit finance, and political destabilization. This model is rooted in Soviet-era practices but has been adapted to today's globalized financial and security environment, allowing Russia to merge intelligence services, business elites, and transnational criminal networks into a single ecosystem of influence.

Iran operates through covert, network-based systems aiming at sanctions evasion, functioning through proxy actors, and leveraging illicit financial flows. Despite these differences, all three models illustrate how hybrid influence is In Latin America, this convergence is accelerating the erosion of governance, distorting markets, and creating durable channels of external leverage.[9]

---

[7] Vladimirov, M., and Galvez, S., *The Captured State: Energy Oligarchies and the Erosion of Democratic Resilience in Latin America*, Sofia: Center for the Study of Democracy, 2025.

[8] Conley, H.A. et al., *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe*, Washington, D.C.: Center for Strategic & International Studies, 2016.

[9] Vladimirov, M., and Galvez, S., *Authoritarian Shadows: The Kremlin Playbook in Central America*, Sofia: Center for the Study of Democracy, 2025.

PATTERNS OF STRATEGIC ENTRY

State–crime interactions are mutually beneficial arrangements where criminal actors provide services that advance strategic objectives. Several recurring patterns are visible across the region:

- **Facilitation of logistics**: whereby criminal networks provide transport routes, document fraud services, or smuggling corridors that allow goods, people, and funds to move across borders, particularly where sanctions or enforcement measures restrict formal channels.

- **Financial enablement**: whereas criminal actors provide access to shadow financial systems through informal remittance networks, exchange houses, shell companies, or trade-based money laundering mechanisms that allow sanctioned actors to circulate funds outside traditional banking structures.

- **Commodity partnerships**: in which criminal or semi-criminal networks give access to illicit resource economies, including illegal gold mining, oil smuggling, or the covert movement of strategic commodities, which is allowing external actors to acquire resources or convert them into financial assets beyond formal regulatory oversight.

- **Security and protection arrangements**: where criminal groups, armed actors, and irregular intermediaries provide local protection, intelligence, or logistical support for foreign actors operating in unstable or highly criminalized environments.

In Latin America licit and illicit systems frequently overlap, especially in sectors such as **energy, mining, logistics, and trade**. For example, **sanctions evasion mechanisms** linked to Venezuela illustrate how formal oil trade can intersect with opaque financial networks and intermediaries, enabling Russia and Iran to sustain revenue flows despite international restrictions.[10] Similarly, Russia's **use of offshore financial structures** and its links to **shadow shipping** and **commodity trade networks** demonstrate how formal economic presence can coexist with less transparent operational layers.[11] China also benefits from this blurred landscape, particularly where infrastructure, trade corridors, and commercial ecosystems intersect with informal or weakly regulated spaces.[12]

---

[10] Ahmed, M., "The Collapse of the Western Flank: The Implications of Maduro's Fall for Iran", Al Habtoor Research Centre, January 12, 2026.

[11] Center for the Study of Democracy, *Countering Kremlin's Global Influence in Latin America*, Policy Brief No. 153 December 2024.

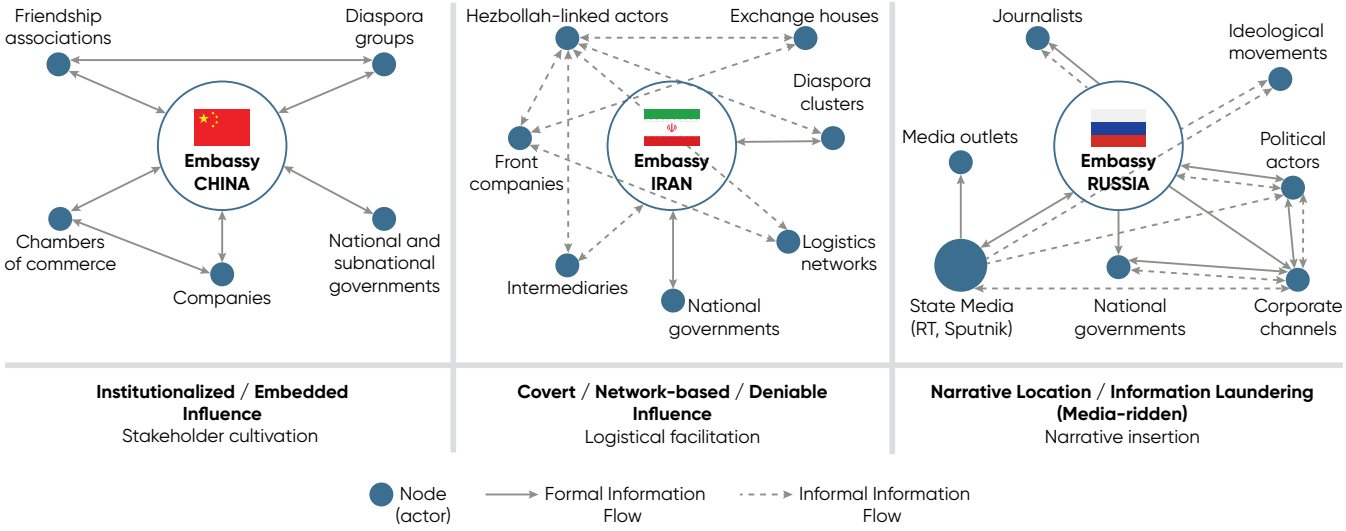
[12] Council on Foreign Relations, "China's Growing Influence in Latin America", June 6, 2025.

Influence is rarely exercised directly by these states; instead, it is mediated through a range of enablers, including:

- local political and business elites
- state-owned or private companies
- diaspora networks and cultural organizations
- media platforms and digital ecosystems
- criminal groups and logistical facilitators
- Proxy organizations
- Intelligence operatives

These actors allow China, Russia, and Iran to access key levers of power in Latin America while preserving plausible deniability.

Figure 2. Networks of Influence: Intermediary Architectures of China, Russia and Iran in Latin America



Source: CSD.

The composition of these ecosystems varies significantly: **Russia** relies heavily on media networks and political amplifiers;[13] **China** builds institutional and commercial relationships;[14] and **Iran** operates through more covert, network-based systems closely tied to sanctions evasion[15] and proxy structures, particularly through Hezbollah.[16]

[13] GIOR, "Russian Propaganda Expands in Latin America WIth RT Workshops", December 11, 2025.

[14] Vasquez, C., "China spent years building ties in Latin America. Can Trump make room for the US?", *BBC News*, March 7, 2026.

[15] SFS, "Iran's Latin American Strategy: Leveraging Asymmetric Warfare to Project Conflict into the Western Hemisphere", June 24, 2025.

[16] Ibid.

Legal economic activities often create the infrastructure through which illicit practices can emerge. Trade flows can facilitate money laundering; infrastructure projects can provide access to strategic logistics nodes; financial agreements can enable opaque transactions; and digital systems can be repurposed for surveillance or information control. This overlap allows actors to move fluidly between visibility and concealment depending on context.

As of 2024, **China** accounted for 10.2% of Mexico's trade, 19.6% of Colombia's, 13.5% of Argentina's, 24.3% of Venezuela's, and 20.8% of Bolivia's,[17] reflecting a region-wide strategy of commercial integration. This is reinforced through major infrastructure projects (e.g. the Bogota Metro)[18] and long-term investments in energy and critical minerals (China is likely to develop the vast lithium reserves of Bolivia). China's financial investment architecture using policy bank lending, swap lines (e.g., $5 billion in Argentina[19]), and project finance further locks in countries in long-term asymmetric dependencies.

Russia, on the other hand, **prioritizes coercive, political, and information-driven influence**, often combined with irregular warfare instruments.[20] Unlike China, its **economic footprint is limited in aggregate terms** – around $20 billion in total trade with Latin America, representing just 2.6% of its global trade,[21] but highly **concentrated in strategic sectors** such as petroleum products, fertilizers and raw materials**,** which can be used to provide the Kremlin with disproportionate leverage in strategic ties. In Brazil, Russia handles over 90% of foreign diesel imports (2022–2026) and around 40% of fertilizer imports,[22] while in Colombia it holds 22% of the fertilizer market.[23] Russia's corporate presence–around 270 companies generating around $10 billion annually, dominated by Rosneft, Gazprom, Lukoil, Rostec and EuroChem[24]–is often structured through offshore jurisdictions, with 65% registered in tax havens and an estimated $70 billion in assets routed through Caribbean financial centers.[25] Russia also uses financial tactics, such as the 90% write-off of Cuba's $32 billion debt, to secure allies in the Western Hemisphere, which it uses to project power regionally and undermine the U.S. clout.[26]

---

[17] Calculated with UNComtrade data.

[18] Bogotá Metro was awarded to a consortium led by China Harbour Engineering Company and Xi'an Metro Company, with partial financing from Chinese banks. The Bogotá Metro project has been shaped by decades of promises, delays, and technical studies that failed to materialize. It is one of the most significant infrastructure projects in Colombia. Beyond its scale, it represents the realization of a repeatedly postponed ambition to modernize the capital's transport system. Yet, its debt-financed structure and the Chinese political underpinning of the project will contribute to the long-term embedding of the Chinese influence in Colombia. Reuters, "Colombia awards $4 billion contract for Bogota metro to China-Canada consortium", October 17, 2019.

[19] Edgecliffe-Jones, M., "Argentina extends currency swap with China, defusing repayment fears", *Reuters*, June 12, 2024.

[20] Brandt, J., "Countering China and Russia's asymmetric activity in Latin America", CSIS, June 21, 2023.

[21] Sullivan, M. P., "Background and Questions for Hearing on Russia's Influence in Latin America and the Caribbean", *Congressional Research Service*, July 15, 2022.

[22] CSD based on commercial shipping data from Kpler.

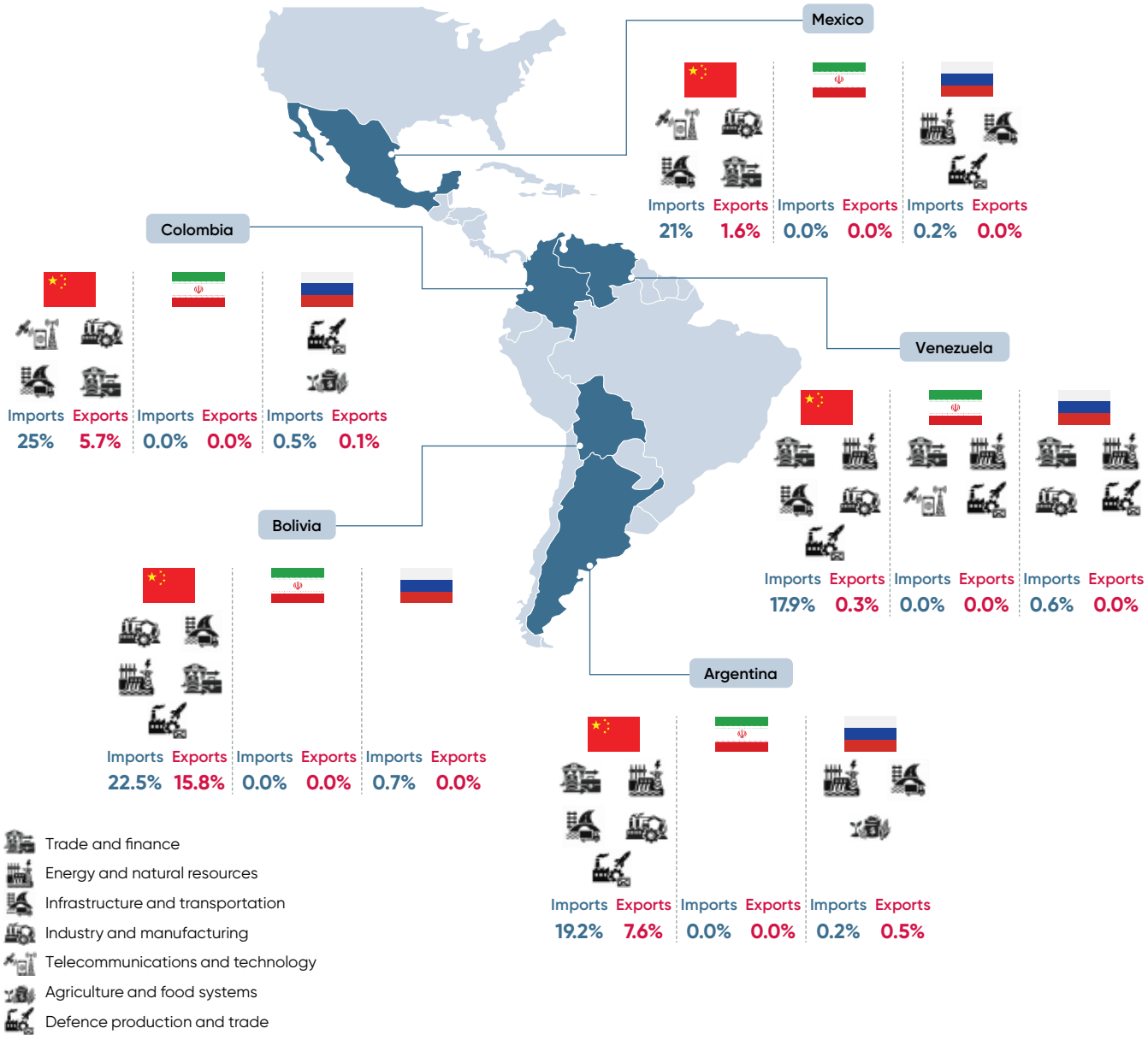
[23] International Trade Administration, "Colombia Fertilizer Market", U.S. Department of Commerce, May 13, 2022.

[24] Vladimirov, Rueda, and Osipova, *Global Reach*, CSD, 2024; CSD analysis of companies with Russian global ultimate beneficial ownership based on data, stemming from a private corporate database.

[25] Ibid.

[26] Vladimirov, and Gálvez, *Authoritarian Shadows*, CSD, 2025.

Figure 3. Economic Entry Points and Modes of Influence of China, Russia, and Iran in Latin America



* There is no available data in UN Comtrade for Venezuela for 2024. Reporting appears to have stopped in 2023, so data from this year is used instead.

	Scale	Strategy	Key sectors	Financial models	Dependency Type
CHINA	Very high	Systemic integration	Infrastructure, EVs, mining, telecom	Loans, swaps, banks	Structural
IRAN	Very Low	Adaptive / network based / Opportunistic	Energy, sanctions networks	Informal, barter	Network-based
RUSSIA	Low	Strategic concentration	Energy, fertilizers sanctions networks	Offshore, debt diplomacy	Sectoral

Source : CSD.

Iran relies on covert, network-based systems that involve intermediaries, and proxy relationships. Its economic presence is very limited and often opaque: between 2004 and 2024, 97% of Latin American exports to Iran came from Brazil (71%) and Argentina (22%), which still represented less than 1% of each country's total exports, with imports from Iran below 0.2% of the total across major economies. Rather than large-scale investment, **Iran has leveraged its vast oil sanctions evasion experience** to help Venezuela survive international economic pressure against its hydrocarbons sector by enabling oil-for-condensate swaps,[27] refinery rehabilitation agreements,[28] and shadow shipping logistics. Outside the oil sector, the Qods Aviation Industry (part of the sprawling Islamic Revolutionary Guard Corps (IRGC)-controlled global network of companies) has developed comprehensive cooperation on drone supply and manufacturing.[29] These activities are embedded in bilateral agreements exceeding $15 billion.[30] Iran's influence model relies on transnational intermediaries, exemplified by the Alex Saab network,[31] which helped the Venezuelan regime of Nicolas Maduro to evade sanctions by linking oil flows and using global financial circuits to siphon public resources in offshore bank accounts.

[27] Buitrago, D., Parraga, M., and Spetalnick, M., "Exclusive: Under U.S. sanctions, Iran and Venezuela strike oil export deal", *Reuters*, September 25, 2021.

[28] Buitrago, D, and Sequera, V., "Iran, Venezuela eye trade increase, sign petrochemical deal", *Reuters*, June 13, 2023.

[29] U.S. Department of the Treasury, "*Treasury Targets Iran-Venezuela Weapons Trade*", December 30, 2025.

[30] Johnson, S., *Iran's Influence in the Americas*, CSIS, 2012.

[31] Cohen, L., and Ulmer, A., "Explainer: Who is Maduro ally Alex Saab, who was granted clemency in prisoner swap?", *Reuters*, December 20, 2023.

NETWORKED INFORMATIONAL AND CULTURAL INFLUENCE

Economic influence alone does not explain how China, Russia, and Iran project their power in Latin America. Alongside trade, finance, and infrastructure, all three invest in informational and societal infrastructure of influence: media ecosystems, cultural diplomacy, diaspora engagement and elite cultivation. These mechanisms **shape perceptions, build local constituencies, and reduce the political costs of deeper strategic penetration**. Russia privileges high-intensity narrative projection and information laundering; China relies on institutionalized cultural and networked embedding; and Iran operates through a narrower mix of ideological outreach, ties to the diaspora in the region, and para-state dissemination mechanisms.

The clearest point of divergence is visibility. Russia fields the region's most overt sharp-power apparatus. Through its state-owned outlets, RT en Español and Sputnik, and through partnerships with local broadcasters,[32] journalists,[33] and ideological amplifiers,[34] it pushes narratives of sovereignty, anti-interventionism, and resistance to the West directly into the public debate. **China** is more selective and usually less confrontational in its public rhetoric. On sensitive issues it deploys assertive information tactics by trying to coordinate online behavior and tailor media ecosystems. In most contexts, however, it prefers reputational management, selective media engagement, and the cultivation of favorable institutional environments.[35] **Iran's** media posture is more limited in scale than either Russia's or China's. Its Spanish-language outlet HispanTV disseminates anti-imperialist and anti-sanctions narratives, but its regional impact is much more indirect[36] than the large-scale penetration achieved by Russian media or the broad institutional footprint built by China.

There is also a difference in **how public discourse is shaped**. **Russia relies on narrative penetration rather than ownership**: it inserts messages into domestic debates through local partners, ideological movements, and digital amplification. Russia's most sophisticated regional example has been a coordinated disinformation campaign, managed by the Russian Social Design Agency and Structura across at least 13 Latin American countries. Its likely operational hub has been Chile, where local journalists and public opinion leaders coordinated by the pro-Kremlin journalist Oleg Yasinskiy received content created in Russia, localized it, and published it in regional media so that it appeared organic. [37] Russian embassies reinforced these efforts by coordinating with local outlets and radio stations to further amplify the pro-Kremlin narratives.[38]

---

[32] Office of the Spokesperson, "The Kremlin's Efforts to Covertly Spread Disinformation in Latin America", *Media Note*, U.S. Department of State, November 7, 2023.

[33] Abi-Habib, M., "Russian Disinformation Comes to Mexico, Seeking to Rupture US Ties", *The New York Times*, November 24, 2025.

[34] Times/NA/Perfil, "Argentina's spies expose alleged Russian disinformation group", *Buenos Aires Times*, June 19, 2025.

[35] Ellis, R. E., "Mexico's Engagement with China and Choices for Its Future", *RevaNellis.com*, July 2, 2024.

[36] German Marshall Fund, "Media Vassalage How Venezuela's TeleSUR Acts as Russia's and China's Information Laundering Front", March 7, 2025.

[37] U.S. Department of State, "The Kremlin's Efforts to Covertly Spread Disinformation in Latin America", November 7, 2023.

[38] Ibid.

Box 1. Mexico is the Crown Jewel of the Russian Media Influence in Latin America

RT en Español has become one of the most influential foreign media outlets in Mexico. With over 6 million YouTube subscribers, its content consistently trends among Mexican audiences, often outpacing local news providers in engagement. Mexico ranks among the top three countries globally consuming RT en Español online. Its digital scale has been striking: RT en Español's traffic on X in Mexico rose from 191,000 visits in 2022 to 715 million in 2023.[39]

Simultaneously, RT en Español expanded its physical presence. In October 2023, RT began broadcasting news segments in Mexico City's Metrobus stations, including videowalls with real-time news updates and QR codes directing viewers to RT content online. The campaign, endorsed by Martí Batres's local government, closely aligned with President Claudia Sheinbaum and the Morena party,[40] served as a vehicle for Kremlin messaging in one of Mexico's busiest public spaces.

Russia's media influence in Mexico is also the result of an aggressive narrative amplification. RT en Español has partnered with the state-sponsored Club de Periodistas,[41] whose biweekly journal reportedly contains 53 percent RT-produced content. Russian disinformation also sought to aggravate tensions in U.S.–Mexico relations, including through a falsified RT article attributed to President Sheinbaum threatening the U.S. with starting a war.[42] After the Mexican elections, U.S. authorities seized 32 domains linked to the Doppelgänger operation, in which the Russia *Social Design Agency and Structura National Technology* had cloned media outlets and government websites to spread anti-Ukraine narratives;[43] the Mexican branch was referred to as "Operation México No Perdona."

Another example is the operation of *Nova Resistência* in Brazil, which has promoted the writings of Aleksandr Dugin and has circulated sovereigntist, anti-Western themes aligned with the Kremlin discourse;[44] There are also links between the movement and the recruitment of Brazilian soldiers for Russia since 2014.[45]

---

[39] Abi-Habib, M., "Russian Disinformation Comes to Mexico, Seeking to Rupture US Ties", *The New York Times*, November 24, 2025.

[40] Estéves, D., "Mexicanos, víctimas de la posverdad putiniana" [Mexicans, victims of the Putinian post-truth], *Ejecentral*, May 5, 2024.

[41] Abi-Habib, M., "Russian Disinformation Comes to Mexico, Seeking to Rupture US Ties", *The New York Times*, November 24, 2025.

[42] Dean, A., "Workshops, Street Promotion and Alleged Covert Operations: Russian Propaganda in Latin America", FULCRUM, December 10, 2025.

[43] U.S. Department of Justice, "Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere", September 4, 2024.

[44] U.S. Department of State, "Exporting Pro-Kremlin Disinformation: The Case of Nova Resistência in Brazil", *Global Engagement Center*, October 19, 2023.

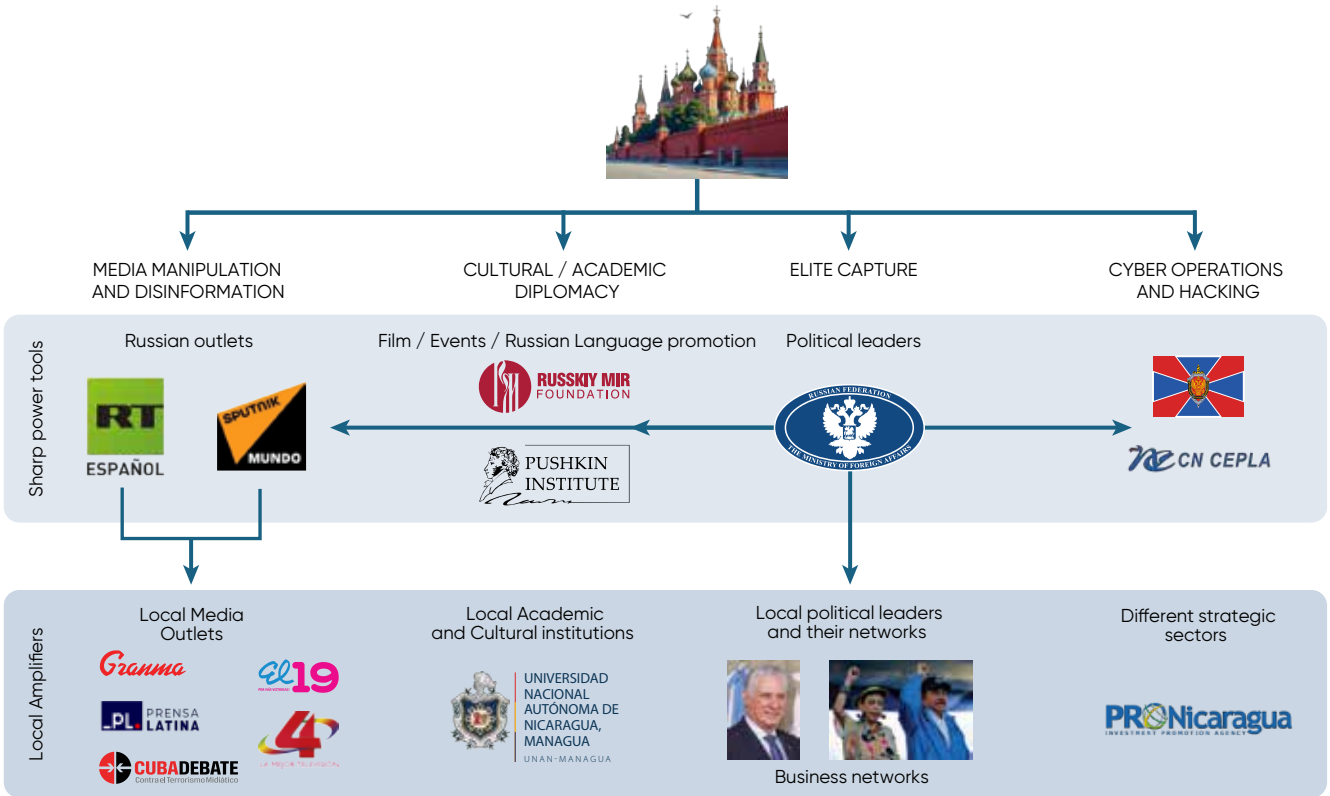
[45] Ibid.

Russia's ecosystem in Argentina has relied on the covert access to a local network of disinformation messaging platforms. One example has been the GRU-linked ring "La Compañía," tied to Project Lakhta, was operated by Russian nationals until their arrest in 2025 and was suspected of making $2,500 monthly payments to Argentine journalists to spread anti-Ukrainian disinformation.[46]

Venezuela is the clearest case of the Kremlin Playbook in the media sector. Russia's model is a tightly coordinated media-amplification circuit between TASS, RT, and Sputnik with Venezolana de Televisión, TeleSUR, and government-aligned private outlets. Statements by high-level Russian government officials are systematically reproduced in Venezuelan media, echoing the Kremlin's main narratives of anti-Americanism and anti-interventionism.

China's model is less ideological and more institutional. In Argentina, a 2022 media cooperation agreement formalized a number of content-sharing arrangements between Chinese and local news agencies. The Chinese state media, Xinhua and CGTN, circulate Beijing-aligned narratives in Argentinian outlets, and their influence is reinforced through the provision of scholarships and educational exchanges involving Argentinian journalist. This approach aims to cultivate future media elites rather than simply driving daily messaging.

Figure 4. Instruments of Sharp Power: Russia's Influence Operations in Central America



Source: CSD.

[46] Izquierdo, L. P., "La red del Kremlin que expande operaciones de desinformación en América Latina y África" [The Kremlin network that is expanding disinformation operations in Latin America and Africa], *Infobae*, March 9, 2026.

Outside cooperation on messaging between Chinese and local media outlets is also helping Latin American governments tighten their control over the media sector. The China National Electronics Import & Export Corporation has supplied software and training to the Venezuelan CANTV,[47] replicating elements of China's digital filtering model, including blocking of independent media, election-period social media restrictions, and phishing practices.

Iran's role in the Venezuelan media sector is much narrower. By 2025, HispanTV content had been cited about 500 times on TeleSUR's website, indicating only limited regional circulation[48]. The amplification of Iranian narratives has remained more thematic and indirect than the Russian model of coordinated narrative insertion.

The different approaches to influence over social structures extend into the area of **cultural diplomacy**. Russia uses culture as a supporting instrument for political influence rather than as a broad institutional ecosystem. It promotes "cultural, scientific, educational, sports, tourism and other humanitarian ties," including Rossotrudnichestvo's initiatives to establish local Russian language and educational centers[49,50].

China's cultural influence strategy has been much more visible. China has built the region's most extensive network of Confucius Institutes, academic exchanges, journalist training initiatives, and cultural programming in different countries of the region.[51] These initiatives have shaped professional, journalistic norms and have entrenched domestic media reliance on Chinese content, training, and standards. **China tends to formalize diaspora engagement through embassy-linked or United Front-adjacent channels**. In Buenos Aires, for example, the PRC embassy hosts police officers who assist with investigations involving Chinese organized crime, provide consular services, liaise with Chinese associations, and organize community meetings that reinforce loyalty to the embassy.[52] In Colombia, chambers of commerce, trade fairs, diaspora associations, and sister-city initiatives extend PRC influence into business and subnational political circles.[53] In Mexico, cultural outreach to diaspora organizations appears increasingly coordinated with Beijing's political priorities.[54]

---

47 U.S. Department of the Treasury, "Treasury Sanctions CEIEC for Supporting Venezuelan Intelligence Efforts to Undermine Venezuelan Democracy", November 20, 2020.

48 Benzoni, P., *Media Vassalage: How Venezuela's TeleSUR Acts as Russia's and China's Information Laundering Front*, German Marshall Fund, March 2025.

49 Sukhankin, S., "Will Nicaragua Become Russia's Cuba of the 21st Century", *Jamestown Foundation*, July 8, 2018.

50 The Ministry of Foreign Affairs of the Russian Federation, "Article by Foreign Minister Lavrov, Russia and Venezuela: Friendship and Partnership Spanning Years and Kilometres, dedicated to the 80th anniversary of diplomatic relations between Russia and Venezuela, for Cancilleria, a Venezuelan Foreign Ministry publication, March 14, 2025", March 14, 2025.

51 Zuppello, M., "China's Influence Operations in Latin American Media", *Diálogo Américas*, June 13, 2025.

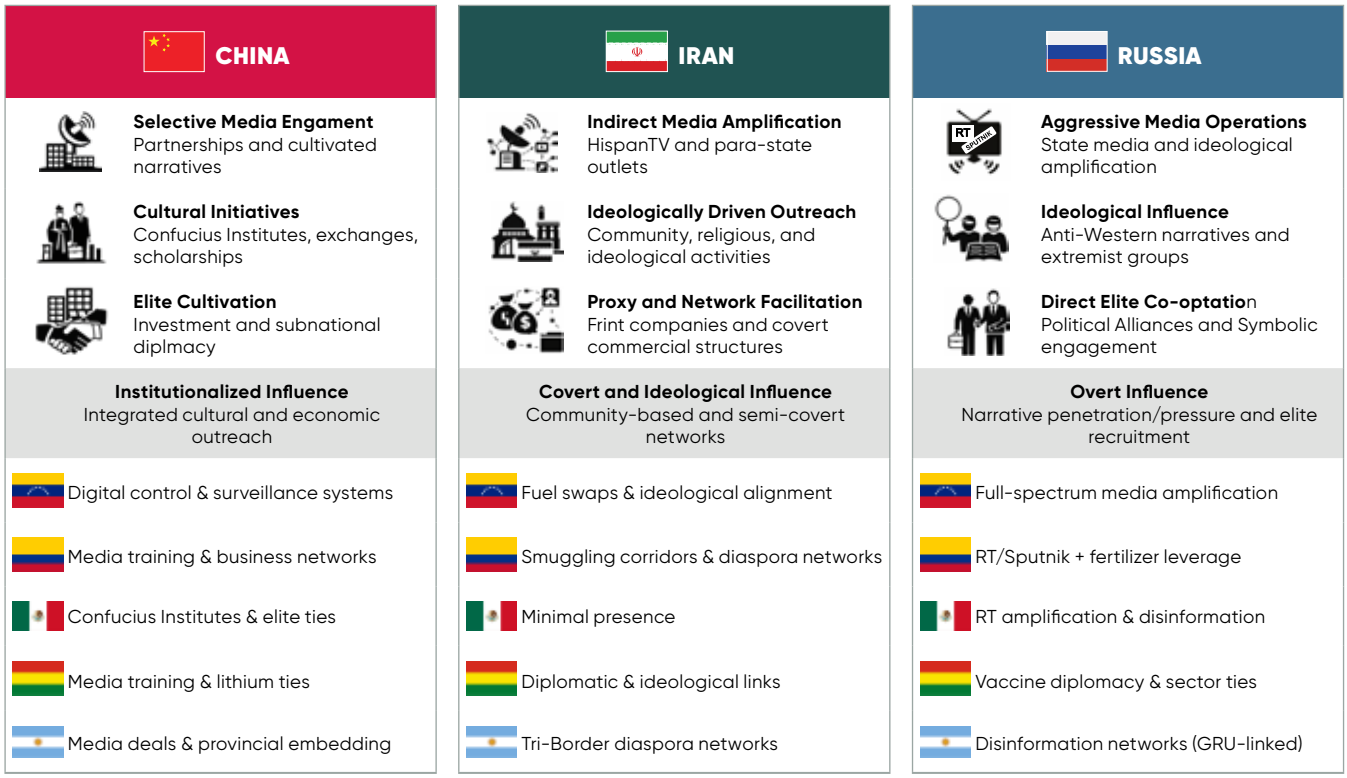
52 U.S. Army TRADOC G-2 and Foreign Military Studies Office, "Instruments of Chinese Military Influence in Argentina", August 2024.

53 Ellis, R. E., *Colombia's Relationship with the PRC*, CSIS, November 10, 2022.

54 Ellis, R. E., "Mexico's Engagement with China and Choices for Its Future", *RevaNellis.com*, July 11, 2024.

Iran's cultural diplomacy is more localized and community-based. It operates through mosques, cultural centers, youth organizations, and diaspora spaces, especially in the Tri-Border Area between Argentina, Brazil and Paraguay,[55] where cultural and religious outreach can overlap with broader logistical and political networks. Iranian ecosystems have historically embedded themselves in segments of the wider Arab–Lebanese diaspora, estimated in about 3.5 million people in Latin America. Within that environment, segments of the Shiite community have been identified in some analyses as potential recruitment pools for Hezbollah. The system includes front companies, currency exchange offices, informal remittance channels, and facilitators such as the Barakat clan, as well as institutional touchpoints like Iran's Cultural Attaché office in Buenos Aires. Unlike China's disciplined embassy-adjacent model, Iran's network is held together less by formal hierarchy than by functional specialization in cash movement, laundering, document facilitation, and logistical support.

Figure 5. Media Manipulation, Cultural Diplomacy and Elite Capture



Source: CSD.

[55] Itzchakov, D., "Iran's Public Diplomacy in Latin America", ICT, March 16, 2025.

HYBRID INFLUENCE THROUGH ILLICIT AND COVERT NETWORKS

The transition from formal engagement to hybrid influence happens through the layering of opaque and deniable practices on top of formal economic, political and diplomatic ties. The first mechanism is **illicit finance**. Formal economic presence gives authoritarian actors access to banking relationships, corporate vehicles, commodity flows, and commercial documentation that can later support sanctions evasion, money laundering, and covert transfer systems.

Table 1. External Actors and Their Interaction with Criminal Markets in Latin America

Type of interaction	External actor	Main country / node	Examples	Strategic significance	Link to authoritarian state
Chemical precursor supply chains	China	Mexico	Chinese producers and brokers supplying fentanyl and meth precursors via Pacific ports	Enables large-scale synthetic drug production embedded in legal trade	**Indirect / structural**
Financial laundering networks	China	Mexico / transnational	Underground banking, trade-based laundering, crypto channels linked to cartel proceeds	Facilitates rapid cross-border movement of illicit funds	**Indirect / structural**
Offshore opacity and sanctions-evasion finance	Russia	Venezuela / Caribbean / Panama	Shell companies, offshore entities, oil-linked financial structures	Enables capital concealment and sanctions evasion	**Direct / state-linked**
Proxy financial and logistical networks	Iran / Hezbollah	Tri-Border Area; Venezuela; Panama	Money laundering, remittance systems, document facilitation	Sustains sanctions resilience and deniable operational reach	**Direct (proxy-based)**
Arms–narcotics hybrid flows	Iran / Hezbollah-linked	Venezuela / Colombia / Brazil	Cocaine-for-weapons exchanges; links to FARC dissidents and PCC	Integrates trafficking, arms flows, and geopolitical networks	**Direct (proxy-based)**
Resource extraction and illicit commodities	Russia-linked actors	Venezuela (Orinoco)	Gold extraction linked to security actors and informal networks	Generates off-book revenue and supports regime resilience	**Mixed (state-enabled)**
Permissive logistical environments	All (China / Russia / Iran)	Panama; TBA; Mexico; Venezuela	Ports, FTZs, customs gaps, shipping routes	Enables overlap of licit and illicit flows	**Indirect / enabling**
Opportunistic foreign criminal actors	Russia-linked	Mexico / Colombia	Fraud, cybercrime, recruitment intermediaries	Limited on their own; relevant in hybrid contexts	**Weak / unclear**
Localized procurement networks	Iran / Hezbollah-linked	Panama / Bolivia	Sourcing of explosives, intermediaries, front companies	Expands operational capacity within local markets	**Direct (proxy-based)**

Source: CSD.

Illicit economies function as instruments of strategy, which provide financial resilience, logistical flexibility, and deniable channels through which states can sustain influence under constraints. The durability of hybrid influence tactics can be explained by the existence of the right enabling conditions such as logistical infrastructure, governance gaps in security systems, financial opacity, permissive border regimes, digital tools, and political alignment. These factors allow illicit and covert activities to function with resilience over time by reducing visibility and limiting the risk of disruption.

Sanctions Evasion and Shadow Finance

Sanctions evasion and shadow financial systems constitute **one of the most consistent mechanisms through which illicit economies are operationalized**. These systems rely on the integration of trade-based laundering, offshore corporate structures, and informal or digital financial channels. Russia has developed one of the most structured and state-integrated models of sanctions evasion and shadow finance, combining trade-based laundering, offshore corporate architectures, and alternative payment systems.

Trade-based money laundering (TBML) links organized crime, proxy financing, and hybrid geopolitical influence. By embedding illicit financial flows within legitimate trade and commercial transactions, TBML allows actors to obscure the origin, movement, and destination of funds while maintaining plausible deniability. Across Latin America, TMBML occurs through intermediaries, including casinos, currency exchange offices, front companies, shipping firms, and informal remittance networks, which all create complex financial architectures that connect narcotics trafficking, commodity flows, and geopolitical influence. In Venezuela, for example, oil shipments evading sanctions have been routed through intermediaries and disguised through falsified documentation and maritime practices such as AIS manipulation, reflagging, and cargo relabeling.[56] These practices allow sanctioned crude to enter global markets under alternative identities, often with the involvement of transnational brokers and facilitators.

Corporate opacity further reinforces these systems. Russian-controlled financial networks provide one of the clearest examples: of 269 Russian-owned entities in Latin America and the Caribbean, 65% are registered in offshore jurisdictions, including 115 in the British Virgin Islands, 15 in the Cayman Islands, and 13 in Belize, with an estimated $70 billion in assets routed through Caribbean financial centers.[57] Panama alone hosts 726 Russian-owned companies,[58] illustrating how formal corporate structures can be repurposed into vehicles for capital concealment and sanctions evasion.

---

[56] Childs, N., *Russia's 'Shadow Fleet' and Sanctions Evasion: What Is To Be Done?*, IISS, January, 2025.

[57] Bureau van Dijk, *Orbis* database. CSD analysis of companies with Russian global ultimate owners registered in Latin America and the Caribbean. Data update no. 381007, exported March 13, 2026.

[58] Center for the Study of Democracy, *Countering Kremlin's Global Influence in Latin America*, Policy Brief No. 153 December, 2024.

Russia has sought to provide **alternative transaction channels for sanctioned partners**, including the use of state-owned banks such as Gazprombank and the expansion of the Mir payment system in Venezuela, reducing reliance on dollar-based settlement systems.[59] After the Venezuelan state-owned oil and gas company, PDVSA lost access to SWIFT,[60] smaller and less globally exposed financial institutions began to process Venezuelan oil payments through triangulated transactions involving front companies in **low-tax jurisdictions**. Among them are **Evrofinance Mosnarbank** and **Novikombank**, which routed transactions linked to Venezuelan oil exports through layered intermediary structures. The use of such institutions allowed Russian-linked actors to reduce exposure to Western enforcement while maintaining access to international financial channels under sanctions pressure. Another example of shadow finance is the deployment of the **ruble-backed A7A5 token**, which has facilitated large-scale international transactions for the Venezuelan energy sector.[61] Prior to being targeted by U.S. and EU sanctions in August 2025, the token reportedly processed approximately $100 billion,[62] illustrating the scale at which state-linked digital financial instruments can operate within sanctions-evasion ecosystems.

Iran's model is more decentralized but equally dependent on shadow finance. Lacking access to formal banking systems, it relies on barter arrangements, front companies, and informal remittance networks. The Alex Saab network[63] exemplifies how these systems operate across jurisdictions, linking Venezuelan oil flows with the siphoning of public funds to offshore accounts in Europe and the Caribbean. The IRGC are estimated to control up to 50% of Iran's crypto ecosystem, and have moved illicit funds through USDT-based transactions[64] and OTC exchange groups operating via Telegram and based out of Venezuelan cities.

This decentralized architecture extends into the **aviation sector**, an important logistical layer within Iran's sanctions-resilience model. The Venezuelan airline company CONVIASA and its cargo subsidiary EMTRASUR have partnered with sanctioned Iranian carriers, particularly Mahan Air, to facilitate IRGC logistical operations.[65]

---

[59] Institute for the Study of War, "Russia in Review: Russia's Venezuela Intervention", April 5, 2019; The Ministry of Foreign Affairs of the Russian Federation, "Article by Foreign Minister Lavrov, Russia and Venezuela: Friendship and Partnership Spanning Years and Kilometres, dedicated to the 80th anniversary of diplomatic relations between Russia and Venezuela, for Cancilleria, a Venezuelan Foreign Ministry publication, March 14, 2025", March 14, 2025.

[60] Shipowners, "Venezuela — U.S. sanctions imposed on PdVSA", March 20, 2019.

[61] Ambaye, M., "Russia-Linked Stablecoin's Transactions Top $100 Billion in Year", *Bloomberg*, January 22, 2026.

[62] Elliptic, "A7A5: The ruble-backed stablecoin crosses $100 billion in transactions", January 22, 2026; Transparencia Venezuela, *Nuevas formas de corrupción y lavado de dinero, El uso de las criptomonedas en Venezuela en la era de Nicolás Maduro*, 2025; Transparencia Venezuela, *PDVSA-Crypto, An Unprecedented Fraud with Tremendous Economic and Social Impact*, 2023.

[63] Cohen. L., and Ulmer, A., "Explainer: Who is Maduro ally Alex Saab, who was granted clemency in prisoner swap?", *Reuters*, June 5, 2020.

[64] The Washington Post, "Iran's Revolutionary Guard used crypto to evade sanctions, reports finds", January 13, 2026.

[65] Motamendi, M., "US seizes plane that Iran sold to Venezuela", *AlJazeera*, February 13, 2024; Giambertoni, M., *Hezbollah's Networks in Latin America*, Expert Insights, March, 2025.

A notable case involved a Boeing 747 cargo aircraft, **transferred from Mahan Air to EMTRASUR through the Dubai-based intermediary** Lance Tech General Trading Company LLC, without required authorization, and subsequently used on routes between Venezuela, Iran, and Russia.[66] The aircraft was detained in Argentina in 2022, carrying 14 Venezuelan and 5 Iranian crew members,[67] including Gholamreza Ghasemi, identified in multiple reports as part of the IRGC-affiliated aviation structures.[68] Civilian aviation assets function as dual-use logistical platforms, enabling the movement of personnel, equipment, and potentially sensitive cargo under the cover of commercial operations, while exploiting regulatory gaps and uneven enforcement across jurisdictions.

China's role in shadow finance is to facilitate **organized criminal activities**. China-linked money laundering networks (CMLNs) have become k**ey service providers for Mexican drug trafficking organizations**, particularly within the fentanyl economy.[69] Large-scale legal trade systems are financial camouflage, allowing illicit flows to be absorbed into ordinary commercial activity.

The scale of these financial flows is considerable. Between January 2020 and December 2024, U.S. financial intelligence identified approximately $312 billion in suspicious transactions linked to Chinese money laundering networks, based on more than 137,000 filings.[70] This volume underscores the systemic role of these networks in facilitating cross-border illicit finance.

In a typical model, cartel operatives in the United States provide U.S. dollars to Chinese brokers, who deliver equivalent amounts in pesos to cartel affiliates in Mexico. The dollars are then sold to Chinese clients seeking to circumvent capital controls, who transfer renminbi to accounts controlled by the network in China. This creates a circular financial loop that simultaneously launders narcotics proceeds and facilitates capital flight.[71]

Specific cases further illustrate the operational structure of these systems. **The Li Xizhi network**, a Hokkien-speaking triad operating in Mexico, has functioned as an **intermediary linking cartel-generated cash in the United States with Chinese financial channels**.[72] The network enabled the rapid conversion and redistribution of illicit proceeds, demonstrating how criminal and commercial financial infrastructures can become tightly integrated across jurisdictions. Beyond cash movement, these networks employ **daigou**

---

[66] U.S. Department of Justice, "*Former Iranian-Owned Boeing Aircraft Successfully Returned to the United States*", (February 12th, 2024).

[67] Chambers, B., "Last 5 crew members of detained Venezuelan plane leave Argentina", AA, October 18, 2022.

[68] Montaruli, F., "The Mystery Venezuelan Plane Carrying IRGC Officers Grounded in Argentina", *IranWire*, June 13, 2022.

[69] U.S. Treasury, "FinCEN Issues Advisory and Financial Trend Analysis on Chinese Money Laundering Networks", August 28, 2025.

[70] Financial Crimes Enforcement Network, *Chinese Money Laundering Networks: 2020-2024 Threat Pattern & Trend Information*, Financial Trend Analysis, August 28, 2025; Rosen, L. W., *Chinese Money Laundering Networks*, Congressional Research Service Report R48786, January 8, 2026.

[71] Corporate Finance Institute, "Hawala", 2025; AML Square Experts, "What Is Hawala Money Laundering? How to Prevent it", *AML Square Blog*, July 22, 2025.

[72] Rotella, S., and Berg, K., "How a Chinese American Gangster Transformed Money Laundering for Drug Cartels", *ProPublica*, October 11, 2022.

(代購) purchasing systems, in which consumer goods are acquired abroad and exported to transfer value into China, as well as highly compartmentalized, trust-based organizational structures that complicate attribution.

While these dynamics demonstrate **deep operational integration between Chinese-linked networks and Mexican criminal organizations,** available evidence suggests that these relationships are privately-driven rather than directed by the Chinese state. Nevertheless, they highlight how global financial structures can sustain large-scale illicit economies and indirectly shape broader strategic dynamics.

Box 2. Chinese Chemical Precursors and the Synthetic Drug Supply Chain in Mexico

China's role in Mexico's synthetic drug economy is best understood through its position within the global commercial and logistical systems that underpin precursor supply chains. Synthetic drug production increasingly depends on industrial chemical inputs sourced through transnational supply chains that connect Chinese producers and brokers to Mexican manufacturing and distribution networks.

These supply chains have evolved significantly. Earlier patterns (2010–2017) centered on bulk methamphetamine precursors such as monomethylamine, whereas more recent trends (2018–2025) show a shift toward fentanyl and increasingly complex precursor and pre-precursor substances, including NPP, ANPP, and 1-boc-4-piperidone.[73] These synthetic drug precursors depend on globally sourced industrial inputs coordinated through commercially structured illicit supply chains.

The flow of these dual-use goods depends on **maritime routes linking Asia to Mexico's Pacific coast**. The ports of Manzanillo, Lázaro Cárdenas, and Ensenada, function as critical gateways between Chinese supply chains and Mexican criminal organizations.[74] To reduce detection risks and obscure origin, shipments are often routed through intermediary jurisdictions, including European transit points, and increasingly combine large commercial consignments with smaller, fragmented deliveries arranged through international shipping services and online procurement platforms.[75] Mexican criminal organizations rely on supply chains, dominated by Chinese producers, brokers, and intermediaries even as regulatory controls and enforcement patterns evolve.

There are **several major China-based precursor networks,** including the **Du Changgen**, the **Anhui Hefei**, the **Hubei Aoks Bio Tech**, the **Amarvel**, and the **Guangzhou Tengyue clusters**. These networks operate through legally registered chemical companies that perform differentiated roles across production, sales, logistics, and financial processing. In some cases, they exhibit features of vertically integrated consortium models, combining multiple firms and intermediaries into coordinated supply structures.

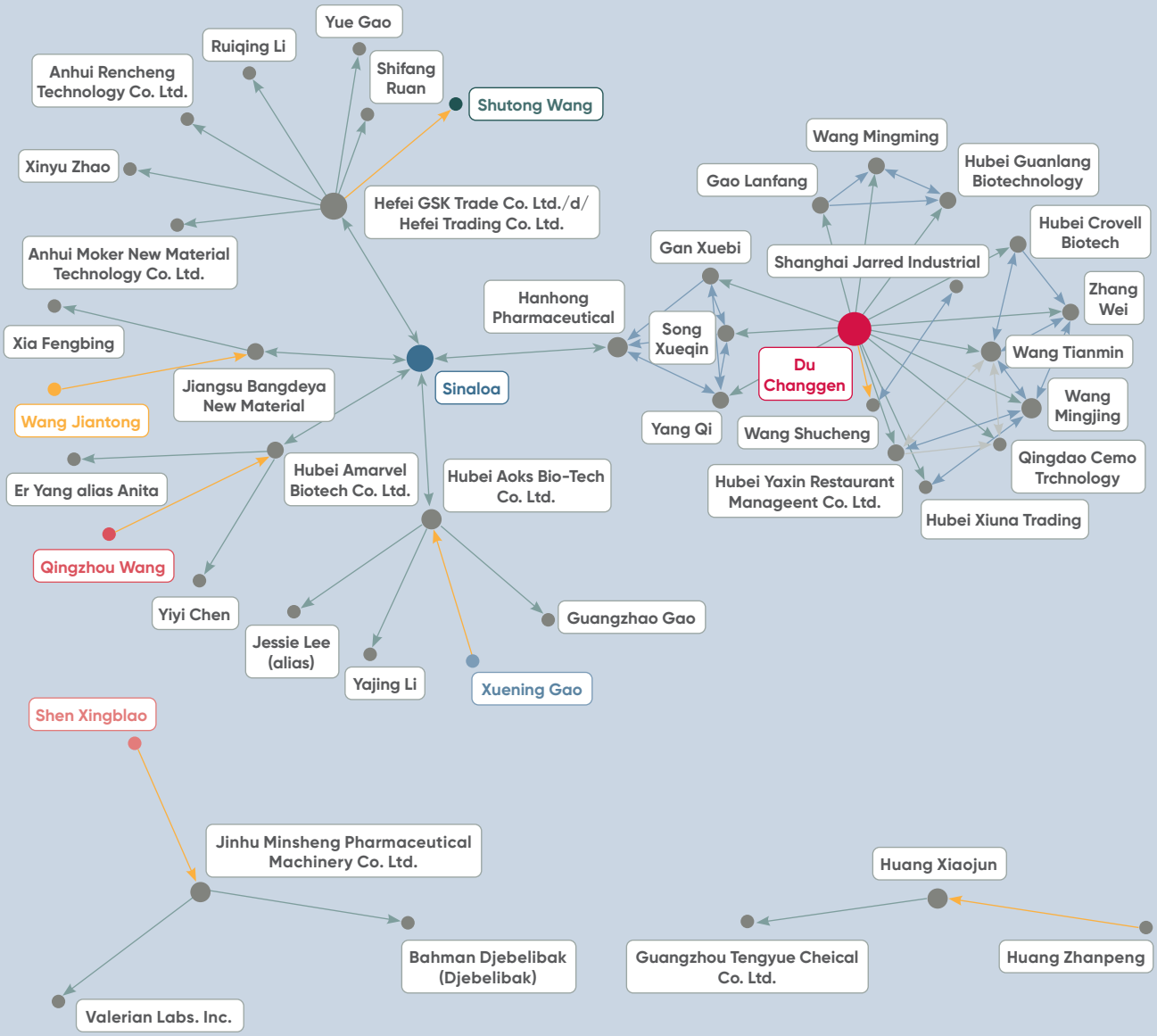
---

[73] Dudley, S., "How Fentanyl Is Synthesized in Mexico", *InSight Crime*, May 9, 2023; Garcia, S., "Beyond China: Other Countries Providing Precursor Chemicals to Mexico", *InSight Crime*, February 28, 2024; Garcia, S., "China's New Fentanyl Controls May Impact Production in Mexico", *InSight Crime*, November 29, 2023.

[74] Jorgic, D., Gottesdiener, L, and Eisenhammer, S., "The shadowy 'brokers' helping Mexico's cartels smuggle fentanyl chemicals from China", *Reuters*, December 18, 2024; Dudley, S., Dittmar, V., and García, S., *The Flow of Precursor Chemicals for Synthetic Drug Production in Mexico*, InSight Crime, May 2023.

[75] Kinnee, K., "Illicit Drug Precursor Shipments from China: A Growing Concern", *Kpler*, July 10, 2024.

Figure 6. Network Analysis of the Links Between China and Mexican Cartels



Source: CSD based on U.S. DOJ, DEA, FinCEN, and Treasury reports (2023–2025); OFAC sanctions notices; Reuters, NPR investigations; and Tianyancha corporate data.

Among these, the **Du Changgen network stands out for its complexity** by combining precursor supply, pill-press equipment, and financial coordination across multiple jurisdictions supplying to commercial partners, associated with both the Sinaloa Cartel and the **Jalisco New Generation Cartel.** In 2025, the U.S. Treasury sanctioned the Guangzhou Tengyue Chemical Co., Ltd. and associated individuals, including Huang Xiaojun and Huang Zhanpeng, for delivering synthetic opioids, precursor substances, and production equipment.

The synthetic drug economy is not concentrated in a single territory, but distributed across many ports, processing zones, manufacturing hubs, and transit corridors. Colima, anchored by the port of Manzanillo, serves as a major maritime entry point and has been associated with at least four transnational criminal

organizations in relation to bulk precursor chemicals and contraband tobacco.[76] Michoacán functions as both an entry and processing zone for fentanyl and methamphetamine precursors.[77] Sinaloa plays a central role in production and procurement, particularly for substances such as 1-boc-4-piperidone and other pre-precursors.[78] Jalisco appears as a key supply-chain node for fentanyl analogues and precursor substances,[79] while Baja California operates primarily as a transit corridor for NPP, ANPP, and fentanyl precursors.[80] More recently, Mexico State emerged in 2025 as an air and logistics hub, linked to the handling of chemicals such as (2-Bromoethyl) benzene.

Figure 7. TOC Presence in Mexico's Synthetic Drug Supply Chains

State	Transnational Organized Crime groups (TOCs)	Years Active	Role in TOC	Top Commodities
Sinaloa	3	2022, 2024, 2025	Production and Procurement	1-boc-4-piperidone, Pre-precursors
Colima	4	2011, 2021, 2024	Major Maritime Entry	Contraband tobacco, bulk precursors
Michoacán	4	2019, 2021, 2023, 2024	Entry and Processing	Fentanyl, Meth precursors
Jalisco	3	2022, 2023, 2024	Supply Chain Node	Fentanyl analogs, Precursors
Baja California	2	2020, 2023	Port Transit	NPP, ANPP, Fentanyl precursors
Mexico State	1	2025	Air/Logistics Hub	(2-Bromoethyl) Benzene

[76] U.S. Department of the Treasury, "Treasury Works with Government of Mexico to Sanction CJNG Members Operating Through the Port of Manzanillo", October 6, 2021; Wilson, M., "US Sanctions Reveal CJNG's Grip on Mexico Port To Move Fentanyl", *InSight Crime*, October 8, 2021.

[77] Asmann, P., "China Fentanyl Ban Yet to Hamper Mexico's Crime Groups", *InSight Crime*, September 4, 2019.

[78] El Reporte, "Desde 2018 la mafia rusa y china producen fentanilo en México: el Cártel de Sinaloa pasó de comprador a productor," *Reporte Maya*, January 8, 2025.

[79] U.S. Drug Enforcement Administration (DEA), *National Drug Threat Assessment 2024*.

[80] Dudley, "How Fentanyl Is Synthesized in Mexico", *InSight Crime*, May 9, 2023; Dittmar, V., and Ríos, P., "How Fentanyl Producers in Mexico Are Adapting to a Challenging Market", *InSight Crime*, January 22, 2025.

Concealment practices are central to the success of this system. Precursor chemicals are frequently hidden within legitimate cargo, and transported through commercial channels. This overlap exploits weak customs controls, and use the scale of legitimate trade as camouflage. Some of the same routes and nodes connected to precursor flows are also used for contraband tobacco, firearms trafficking, and other smuggling activities.

These logistical systems are **closely linked to parallel financial infrastructures**. Chinese underground banking networks have become key facilitators for Mexican criminal organizations, enabling the movement of proceeds generated by synthetic drug production through trade-based laundering, informal value transfer systems, and cryptocurrency.[81]

Available evidence does not indicate direct coordination between the Chinese state and these criminal activities. China's role is better understood as structural rather than operational. Its vast chemical industry, deep integration into global trade, and centrality to shipping and manufacturing networks create the logistical and commercial conditions in which illicit flows can move alongside legitimate commerce.

Strategic Commodities and Extractives

Strategic commodities represent a second key interface between licit and illicit economies. The distinction between legal and illegal activity is often blurred, as state-linked actors, private firms, and criminal networks intersect around high-value resource flows.

Oil remains central to sanctions evasion and geopolitical alignment. In Venezuela, cooperation with Russia, China and Iran has enabled the continued export and processing of crude despite international restrictions. Russian financial support to PDVSA, estimated at up to $17 billion in loans,[82] has been directly tied to oil-backed arrangements that facilitate both formal production and opaque distribution channels. Iran's role complements this system through fuel shipments, condensate swaps, and refinery rehabilitation, embedded in agreements exceeding $15 billion,[83] allowing Venezuela to sustain output while bypassing U.S. sanctions. Between 2000 and 2023, China committed over $100 billion in loans to Venezuela, with roughly $95 billion structured as oil-backed repayments. These agreements, primarily from the China Development Bank, allowed Venezuela to service debt with oil shipments rather than cash. This strategic partnership made China the biggest purchaser of Venezuelan crude despite U.S. sanctions and even after the arrest of Nicolas Maduro.

Gold and illegal mining provide another critical channel. Gold has become an **alternative payment mechanism** when access to formal banking is restricted. In Venezuela, illegal gold extraction in the Orinoco Mining Arc, has generated an estimated $2.2 billion annually.[84] Russia's role has been to facilitate the marketing of the gold via intermediary networks involving Russian-linked

[81] U.S. Department of Justice, "Federal Indictment Alleges Alliance Between Sinaloa Cartel and Money Launderers Linked to Chinese Underground Banking", June 18, 2024.

[82] De la Cruz, A., "Rosneft's Withdrawal amid U.S. Sanctions Contributes to Venezuela's Isolation", CSIS, April 10, 2020.

[83] Johnson, *Iran's Influence in the Americas*, CSIS, 2012.

[84] U.S. Department of State, *Report to Congress on The State-Sponsored Extraction and Sale of Gold from Venezuela's Orinoco Mining Arc, and from National Reserves in Venezuela such as Canaima National Park*, June 5, 2025.

buyers, and the Dubai-based jewelry industry.[85] **Russian paramilitary units**, including the **Wagner group**, have been involved also in the illegal mining operations.[86]

Box 3. Russia's Oil Sanctions Evasion Network in Latin America

Within the broader oil-based system of sanctions circumvention, Russia has developed parallel illicit trading and financial infrastructures that further entrench its role as a key enabler of Venezuela's shadow energy economy. A sophisticated sanctions evasion network linking Russian operatives, Venezuelan intermediaries, and the global financial network, operating through a Germany-based front company, facilitated the smuggling of millions of barrels of Venezuelan oil to Russian and Chinese buyers, including entities connected to sanctioned oligarchs[87].

The scheme relied on a combination of shell companies, falsified shipping documentation, and covert maritime practices such as disabling tanker tracking systems to obscure the origin of oil shipments. Financial transactions were routed through complex international banking structures, including high-risk jurisdictions, and supplemented by cryptocurrency transfers and bulk cash movements to evade detection.

Beyond oil trading, the same network was involved in procuring sensitive Western technologies for Russia's military-industrial complex, illustrating the convergence of sanctions evasion, illicit finance, and strategic procurement.

Under sanctions pressure, **Iran has incorporated Venezuelan gold into barter-like exchanges** tied to the delivery of refined products and the technical maintenance of oil facilities. The gold trade has also been part of a 20-year cooperation agreement, signed in 2022, which stipulated that networks linked to the **IRGC and Hezbollah** can facilitate the acquisition, transport, and resale of gold through intermediaries and routes in Türkiye and the wider Middle East.[88]

China has also played a significant role in the illegal gold mining. Rather than using gold as an instrument for the evasion of financial sanctions, Chinese actors have been embedded in **illegal extraction and brokerage networks** in

[85] Farah. D., and Babineau, K., "A Strategic Overview of Latin America: Identifying New Convergence Centers, Forgotten Territories, and Vital Hubs for Transnational Organized Crime", p.18, *INSS Strategic Perspectives*, January, 2019.

[86] Ellis, R. E., "Venezuela: Understanding Political, External, and Criminal Actors in an Authoritarian State", *Small Wars Journal*, January 14, 2022.

[87] DOJ, "Five Russian Nationals and Two Oil Traders Charged in Global Sanctions Evasion and Money Laundering Scheme", October 19, 2022.

[88] Rousselle, A., "Hezbollah's Latin American Networks: Stablecoins, Smuggling, and Sanctions Evasion", *Global Network on Extremism and Technology*, July 21, 2025.

Peru and Ecuador,[89] while China's large gold refining capacity and destination market have helped absorb the large volumes of illegal gold whose origins have been obscured through the use of intermediaries, falsified documents, or blended supply chains.[90]

Logistics and Trade Corridors

The control over logistics and trade corridors is a critical enabling mechanism for the shadow cooperation between states and transnational organized crime networks. Ports, free trade zones, shipping registries, and customs systems provide the infrastructure through which both licit and illicit activities circulate. It can support hybrid warfare activities by securing the movement of money, commodities, and personnel across borders while obscuring origin and destination.

These dynamics are particularly visible in **trafficking corridors across South America**. Key routes include the Bolivia–Paraguay–Argentina corridor feeding into Atlantic export points, the Paraná–Rosario–Montevideo waterway linking inland production zones to global markets, and routes connecting the Tri-Border Area to Buenos Aires and onward to Europe and Africa. The strategic relevance of these corridors is reinforced by the scale of the global narcotics economy. At an estimated wholesale value of roughly $25,000 per kilogram, the global cocaine market has reached approximately $66.6 billion, around 37% of which comes from Colombia.[91]

Russia's use of maritime logistics illustrates how intergovernmental agreements can buttress these hybrid transport systems. Following a 2022 maritime cooperation agreement with Venezuela (in force from December 2024),[92] Russian-linked networks expanded the use of "shadow fleets" to move sanctioned oil in the Caribbean basin. The use of flag registries such as Panama, which hosts around half of Russia's shadow fleet, further enhances flexibility and deniability. By 2023, this fleet had grown from approximately 600 vessels to between 1,100 and 1,400–around 16% of the global tanker fleet.[93] Since December 2025, at least seven tankers have been seized by U.S. authorities[94].

Russia-linked shadow oil shipping intersects with narcotics trafficking corridors. In 2022, Estonian authorities seized 3.5 tons of Latin American cocaine at the port of Muuga from a Russia-bound vessel originating in **Ecuador**.[95] A more direct case occurred in **Argentina** between 2016 and 2018,

---

89 Felbab-Brown, V., "How Chinese criminal networks fuel illicit markets across the Americas", *Brookings*, December 9, 2025.

90 Dialogo Americas, "China and the Amazon's Illegal Gold: The Plot Behind Clandestine Mining", March 16, 2026.

91 McDermott, J., and Dudley, S., "GameChangers 2024: Global Cocaine Networks and Trump 2", *InSight Crime*, January 6, 2025.

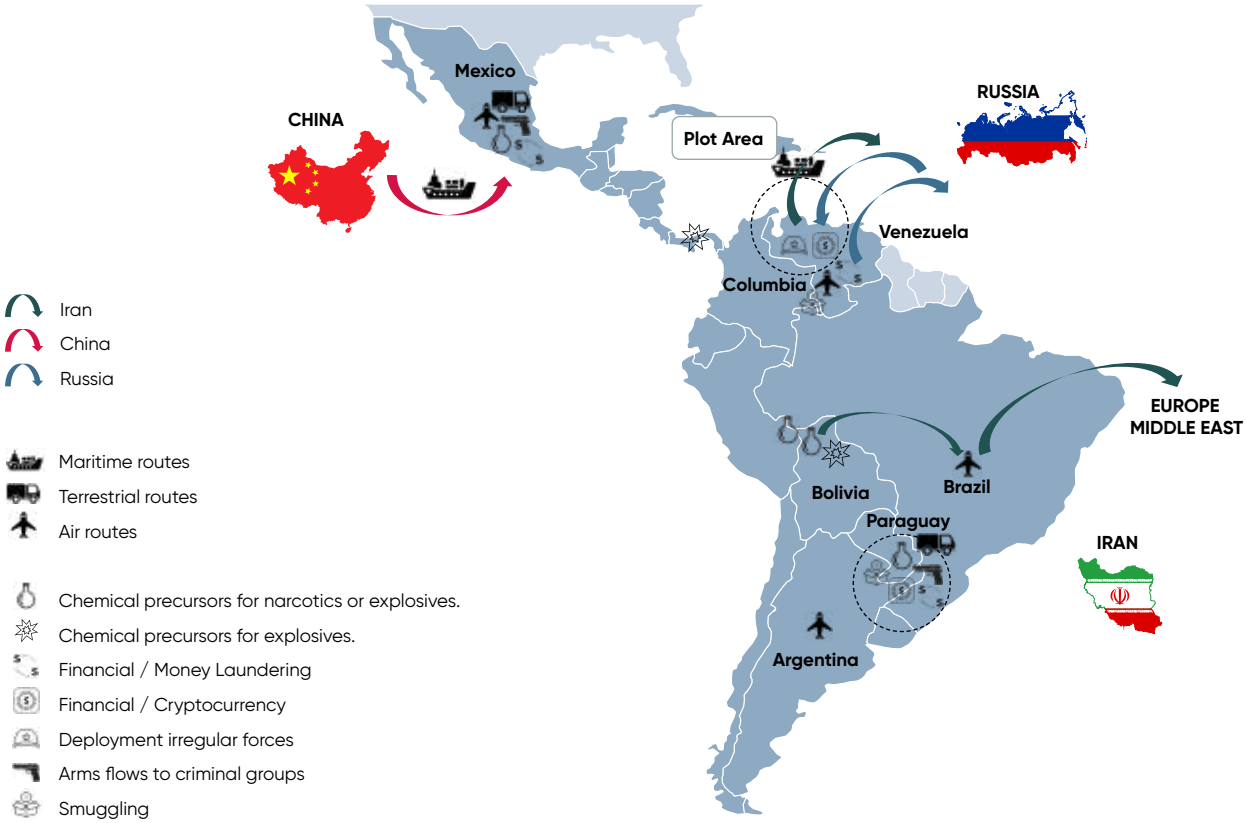
92 Interfax, "Russian, Venezuelan maritime transport cooperation agreement goes into effect", February 11, 2025.

93 Menjón, D. M., "Russia's Shadow Fleet: A Maritime Network to Evade Sanctions, its Operations, Destinations, and Comparison with the Fleets of Iran and Venezuela", *Hermes Kalamos*, August 12, 2025.

94 Matza, M., "US boards second tanker in Indian Ocean after tracking it from Caribbean", *BBC News*, February 15, 2026.

95 Konrad, J., "Estonia Clears Russia-Bound Ship After Drug Raid", *gCaptain*, February 5, 2026.

Figure 8. Logistics and Trade Corridors for Hybrid Use in Latin America



	CHINA	IRAN	RUSSIA
Primary Focus	Chemical supply chains and financial infrastructure	Proxy networks (including chemical precursors for explosives), crypto laundering and transregional finance and facilitations	State-linked logistics, sanction evasions, and strategic access
Main Corridors	China → Mexico → U.S.A. (Precursos chemicals and drugs)	Caribbean coast, tri-border Area, South America → Middle East	Russia-Venezuela oil route, Argentina cocaine/ diplomatic route, Mexico arms and migration corridors
Relationships to Crime	Commercial supply enabler	Embedded through proxy and facilitator networks	Hybrid and state-adjacent often operationally involved

Source: CSD.

when a cocaine-trafficking network operating within the Russian embassy in Buenos Aires shipped approximately 400 kilograms of cocaine to Moscow via diplomatic pouches. The operation was led by the Russian national Andrei Kovalchuk, with embassy staff member Ali Abyanov sealing the shipments. Argentine authorities photographed a plane associated with the Security Council Chief Nikolai Patrushev transporting the cargo.[96]

[96] Kirilenko, A., "Ministry of strange affairs: How the Russian foreign ministry and secret services help smuggle cocaine into the country", *The Insider*, October 13, 2020.

Investigations further indicated that the **cocaine shipments were sourced through Argentine criminal networks**, including groups such as Los Monos and the Alvarado clan,[97] highlighting the extent of the embedding of formal Russian state actors within organized crime networks. This results in a more institutionally blurred boundary between official and illicit activity.

The Russian links to the Latin American drug markets go beyond smuggling activities and into the technical assistance of the illegal substance production. In 2018, Mexican authorities arrested the Russian national **Anton Petrov Kulkini in Mexicali**[98] for alleged involvement in fentanyl production. Investigations linked him to the **Sinaloa Cartel** and suggested he was providing technical expertise for synthetic drug production.

Historical precedents reinforce this pattern. In the late 1990s and early 2000s, a "guns-for-drugs" network involving **Russian mafia figures, corrupt officials, and FARC traffickers** established a template for the interaction between Russian actors and insurgent criminal organizations.[99] The Russian state's willingness to protect such individuals is illustrated by the **Pravfond foundation**, a state-backed legal defense entity that financed the defense of Viktor Bout, who was convicted in the United States for conspiring to supply weapons to the FARC.[100]

Box 4. The Shadow Presence: Russian Espionage and Intersection with Organized Crime in Mexico

Since the start of the war between Russia and Ukraine in 2022, Mexico has become a strategic hub for Russian intelligence operations in the Americas. The country's geographic proximity to the U.S., its bilateral relations with Washington, weak counterintelligence capabilities, and Mexico's noninterventionist foreign policy have made it an ideal base for Russian operations, run by the GRU (Russian military intelligence) and the SVR (foreign intelligence service).[101]

The number of Russian diplomats in Mexico increased by about 60% to 86 accredited officials.[102] This expansion coincided with the mass expulsion of Russian diplomats from Europe, many of whom were redeployed to Latin America, with Mexico as a key destination. The increase goes far beyond the needs of diplomatic functions, and many of these individuals are believed to be GRU operatives and disinformation agents.[103]

---

97 Ibid.

98 El Reporte, "Desde 2018 la mafia rusa y china producen fentanilo en México: el Cártel de Sinaloa pasó de comprador a productor," *Reporte Maya*, January 8, 2025.

99 Schrimp, J., "Post-Demobilization of the FARC: Predictions for Colombia's Future Crime space," *The International Affairs Review*, June 15, 2025; Parkinson, C., "US-Colombia Operations Uncovers FARC, ELN Link to Russian Mafia," *Insight Crime*, February 17, 2014.

100 Lozovsky, I., and Laine, M., "Russian Foundation Aimed at Helping 'Compatriots' Abroad, Supports Spies, Criminals and Propagandists", OCCRP, May 21, 2025.

101 Vladimirov, M., and Galvez, S., *The Kremlin Playbook in Mexico: Asymmetric Influence*, Sofia: Center for the Study of Democracy,2025.

102 Ibid.

103 Luce, D., and Hayes, O., "Back to the Cold War: Russia uses Mexico as a hub for spying on the U.S.", *NBC News*, September 21, 2024.

According to General Glen VanHerck, former Commander of U.S. Northern Command[104] "the largest concentration of Russian intelligence personnel in the world is in Mexico", tasked with collecting intelligence on the United States.[105]

Russia may have used the tourism hotspot of Cancún as a key hub for Russian migration, and possibly infiltration, into the region. Between January 2022 and April 2024, over 166,000 Russian citizens entered Mexico (90% of the post2022 Russian arrivals in Mexico), with at least 73,000 then crossing illegally into the U.S.[106] Some investigations revealed that at least 13 identified GRU agents infiltrated these migration flows,[107] often traveling via the Moscow– Istanbul–Cancún route. U.S. Customs and Border Protection (CBP) has documented a sharp rise in Russian nationals attempting to cross the U.S.–Mexico border, with many relying on smuggling operations coordinated through Telegram.

These channels distribute detailed instructions on illegal crossings and connect migrants with facilitators, creating a well-organized underground pipeline. Some of these migrant flows may also serve as cover for intelligence operatives or as a means to recruit local intermediaries for espionage and sabotage. These concerns have gained some credibility in January 2025, when Timur Praliev, a self-proclaimed former member of the Wagner Group, was apprehended near Roma, Texas, after crossing the Rio Grande from Mexico. Brought before a federal judge in McAllen, Texas, his capture raised further questions about the possibility that Russian paramilitary elements may be using Mexican territory as a transit zone or staging area for intelligence related operations targeting the United States.

Former President López Obrador downplayed U.S. warnings about Russian espionage, stating that "Mexico does not spy on anyone, nor does it allow spying". Concurrently, the Foreign Ministry authorized an expansion of Russia's diplomatic presence, while the U.S. Drug Enforcement Administration has reported bureaucratic delays in accrediting its agents in Mexico.[108] Further concern arose when the newly-elected President Claudia Sheinbaum invited Vladimir Putin to her inauguration, reinforcing the perceptions of a foreign policy more tolerant of Moscow.

---

[104] Mongue, Y., and Camhaji, E., "US General: Russia has more spies deployed in Mexico than in any other country", *El Pais English*, March 26, 2022.

[105] Marginedas, M., "México se convierte en la plataforma del espionaje ruso en el continente Americano" [Mexico becomes the platform for Russian espionage in the Americas], *El Periodico*, August 7, 2024.

[106] Ibid.

[107] Mironova, V., "*Russian FSB is trying to illegally enter US from Mexico*", *Conflict Field Notes*, March 9, 2023.

[108] Arginedas, M., "México se convierte en la plataforma del espionaje ruso en el continente Americano", *El Periodico*, August 7, 2024.

Russian security services have been deployed to support local armed groups to facilitate grey-zone operations across Latin America. It is believed that the Russian Colonel Roman Frolenko, also **chief of the Russia–Venezuela Chamber of Commerce**, has been cooperating with Valentin Santana, the **leader of the armed colectivo La Piedrita,** involved in the crushing of the Venezuelan opposition.[109]

Russian intermediaries have operated across multiple domains simultaneously in Venezuela. Prior to 2023, Wagner personnel were reportedly involved in protecting the Maduro regime, securing gold mining operations in the Orinoco region, and training pro-government militias, including colectivos, in repression techniques.[110] Following the Wagner mutiny, many of these functions appear to have been absorbed into more formal Russian state structures, establishing a more direct form of state involvement.

Russia-linked criminal actors maintain also **physical presence in certain regional organized crime hubs**. In Santa Cruz de la Sierra, Bolivia, the Russian mafia boss Igor Gorelkin was assassinated in 2011, and the El Dorado casino was identified as a Russia-controlled money laundering hub.[111] More recently, Russian and other Eastern European criminal organizations have expanded their presence in Santa Cruz as Bolivia has become an increasingly important coca-producing country and node within the cocaine supply chain.[112]

Leaked Mexican military intelligence documents have also alleged that Antonio Rullán Dichter, the **Honorary Russian Consul in Acapulco**, has maintained a **working relationship with Los Rusos**, a local organized crime group operating within the Beltrán Leyva network.[113]

Similarly, the case of Vladimir Lyubishin Sr. and Jr., arrested in Hungary during a DEA sting operation for an alleged **weapons deal with Mexican cartels**. Russia submitted a competing extradition request and maintained repeated consular engagement with the detainees; after their return to Russia, charges were reportedly dropped.[114]

---

[109] Barráez, S., "Un coronel ruso inauguró un mausoleo en Caracas junto al más temido colectivo de civiles armados", *Infobae*, May 13, 2025.

[110] Ellis, R. E., "Venezuela: Understanding Political, External, and Criminal Actors in an Authoritarian State", *Small Wars Journal*, January 14, 2022.

[111] Redacción de la Prensa, "Jefe policial advierte presencia de mafia rusa en Bolivia", *La Prensa*, December 2, 2011.

[112] Urgente.bo, "Mafias del este de Europa tienen presencia en Santa Cruz, segun criminologo", September 5, 2025; Redaccion de la Prensa, "Jefe policial advierte presencia de mafia rusa en Bolivia", *La Prensa*, December 2, 2011.

[113] Zerega, G., "El cónsul honorario de Rusia que se vinculó al crimen organizado en Acapulco", *El País*, November 14, 2022.

[114] Panyi, S., "Russian arms dealer busted by U.S. agents in Hungary now out of jail after extradition", *Direkt36*, March 7, 2019.

Iran moves goods and money through a loose, decentralized web of personal and business connections rather than a central organization. A key hub for this is the Colón Free Trade Zone in Panama, where investigations have uncovered financial and shipping activity managed by Hezbollah. Two primary examples illustrate this model: first, the **Ayman Joumaa network**, which used various shipping companies and offshore bank accounts to move illegal funds across borders;[115] and second, the **Barakat clan**, whose operations show how this works in practice. In the Barakat model, cocaine produced in Bolivia is moved through Paraguay (Ciudad del Este) and Argentina (Buenos Aires) before being shipped across the ocean to markets in Lebanon and Syria, with the profits feeding back into the network.[116]

Box 5. Joumaa, Barakat and Omairi Networks: Nodes within the Hezbollah-Linked Transnational Illicit Ecosystem

The Joumaa, Barakat, and Omairi networks are part of a broader Hezbollah-linked transnational illicit ecosystem spanning Latin America, West Africa, and the Middle East. These networks operate as **functionally differentiated nodes that collectively enable narcotics trafficking, financial laundering, and cross-border logistics**.

The **Ayman Joumaa network**, dismantled in 2011,[117] represents the most expansive and financially significant of these structures. Operating across Lebanon, Colombia, Panama, and West Africa, it reportedly laundered up to $200 million per month through a combination of cocaine trafficking and trade-based money laundering (TBML).[118] The network linked Latin American cocaine production to global markets, including Europe and the Middle East, and maintained **direct connections with Mexico's Los Zetas cartel**. Its infrastructure included shipping companies, currency exchange houses in Lebanon, front businesses in Panama and Colombia, and bulk cash smuggling operations.[119] **Financial flows were routed through institutions such as the Lebanese Canadian Bank**, which was later designated by U.S. authorities for its role in laundering narcotics proceeds.

[115] Giambertoni, M., "Hezbollah's Networks in Latin America", *Expert Insights*, March, 2025.

[116] U.S. Department of the Treasury, "Treasury Designates Islamic Extremist, Two Companies Supporting Hizballah in Tri-Border Area", June 10, 2004.

[117] Giambertoni, M., "Hezbollah's Networks in Latin America", *Expert Insights*, March, 2025.

[118] US Department of the Treasury, "Treasury Targets Major Lebanese-Based Drug Trafficking and Money Laundering Network", January 26, 2011.

[119] Ryan, J., "Lebanese Drug Lord Charged in US: Links to Zetas and Hezbollah", *ABC News*, December 14, 2011.

The **Barakat network**, active since the 1990s and partially disrupted between 2018 and 2021, functions as a regional financial and logistical hub centered in the Tri-Border Area (Argentina–Brazil–Paraguay). Led by Assad Ahmad Barakat, the network has combined multiple illicit revenue streams, including casino-based money laundering, import-export businesses, contraband trade (cigarettes, electronics, counterfeit goods), and cocaine trafficking routes linking Bolivia to Buenos Aires and onward to the Middle East. Investigations identified at least $11.7 million in fictitious casino "winnings" between 2015 and 2018 used to legitimize illicit cash. The network relied heavily on hawala-type remittance systems and exchange houses to transfer funds to Lebanon, and U.S. authorities have described Barakat as one of Hezbollah's principal fundraisers in Latin America. The Tri-Border Area, with its porous borders and dense commercial activity, provides the permissive environment that sustains this model.

The **Omairi network**, also operating within the Tri-Border ecosystem, represents a more localized system. Associated with Farouk Omairi, the network has specialized in the trafficking of narcotics, funds, and people through decentralized methods, particularly the use of human couriers ("mules") traveling on commercial flights. Cocaine sourced from Bolivia and Peru is transported via the São Paulo International Airport to destinations in Europe and the Middle East, especially Jordan.[120] The network has leveraged a travel and exchange agency to provide integrated logistical support, including ticketing, documentation, accommodation, and financial transfers. Reporting indicates that the network operated under Hezbollah-linked direction and maintained connections to Mohsen Rabbani, an Iranian-linked intermediary associated with Lebanese diplomatic networks.[121]

The **current operational status of these networks varies**. The Joumaa network was formally disrupted in 2011,[122] but its model persists in successor and parallel structures. The Barakat network has been partially dismantled through enforcement actions between 2018 and 2021, although some elements of its infrastructure and associated networks remain active. The Omairi network reflects an ongoing pattern of decentralized facilitation that is more difficult to disrupt due to its reliance on small-scale, distributed operations.

[120] UNICRI, *The Nexus between Transnational Organized Crime and Terrorism in Latin America*, June, 2024.

[121] Ibid.

[122] US Department of the Treasury, "Treasury Targets Major Lebanese-Based Drug Trafficking and Money Laundering Network", January 26, 2011.

Cyber and Digital Crime

Digital ecosystems represent an emerging layer of illicit economic activity, particularly in enabling financial transfers, information manipulation, and operational coordination. **Digital payment systems** have expanded the capacity for sanctions evasion and illicit transactions. These instruments are often coordinated through encrypted messaging platforms such as Telegram, allowing actors to move funds across borders with minimal regulatory oversight.

Digital infrastructure itself can be repurposed for broader influence operations. In Venezuela, Chinese-supported tools delivered by the China National Electronics Import & Export Corporation (CEIEC) have contributed to the development of state-controlled digital environments, including surveillance and real-time content manipulation.[123] At the same time, emerging evidence shows the use of generative artificial intelligence to produce Spanish-language media content aligned with Chinese narratives, which is then disseminated through Latin American outlets, sometimes as sponsored material.[124]

Russian-language cybercrime has historically played a central role in shaping illicit digital markets, including the **Hydra darknet marketplace**, dismantled in 2022 and described by the U.S. Treasury as the world's largest illicit online platform for narcotics, hacking tools, and cryptocurrency-based laundering services.[125] While Latin American actors have not controlled these infrastructures, they have operated within them, benefitting from the global services they have enabled.

Mexican authorities have identified Russian hacker groups, ZOMBiE and Hell Knights Crew to be linked to large-scale banking fraud targeting institutions including Banco Azteca and Banco Santander.[126] More recently, the dismantling of the "La Compañía" network[127] in Argentina in 2025 revealed the Russia-controlled Project Lakhta ecosystem, in which disinformation operations were directly connected to cryptocurrency wallets enabling financial fraud, money laundering, and arms smuggling. In parallel, as sanctions pressure has increased, Russia-connected actors have expanded the use of "digital shielding" mechanisms designed to obscure blockchain traceability and reduce exposure to monitoring.[128]

---

[123] U.S. Department of the Treasury, "Treasury Sanctions CEIEC for Supporting Venezuelan Intelligence Efforts to Undermine Venezuelan Democracy", November 30, 2020.

[124] Tong, A., "OpenAI removes users in China, North Korea suspected of malicious activities", *Reuters*, February 21, 2025.

[125] U.S. Department of the Treasury, "Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex", April 5, 2022.

[126] Mendez, A., "Hacker rusos operan en Mexico desde cinco años", *La Jornada*, June 18, 2008; Mongue, Y., and Elias Camhaji, "US General: Russia has more spies deployed in Mexico than in any other country", *El Pais English*, March 26, 2022.

[127] U.S. Department of State, "Exporting Pro-Kremlin Disinformation: The Case of Nova Resistencia in Brazil", *Global Engagement Center*, October 19, 2023.

[128] Acuna, O., "Elliptic flags Russia-linked crypto platforms' ongoing sanctions evasion", *CoinDesk*, February 23, 2026.

Box 6. Terrorism and Latent Operational Capabilities

State-supported violence and terrorism represent an uneven but strategically significant dimension of hybrid influence. A key insight is that **the absence of frequent attacks does not imply the absence of capability**. The preservation of operational networks, logistical systems, and preparatory activities sustains a latent capacity for violence that can be activated when strategically advantageous, reinforcing broader patterns of hybrid influence across Latin America.

Iran's approach is the most clearly organized around terrorism as a strategic tool, primarily through its long-standing relationship with Hezbollah. The financial and logistical systems that sustain Hezbollah including money laundering, the issue of travel documents, and the facilitation of cross-border logistics form the backbone of an operational ecosystem. These infrastructures support Hezbollah's role within Iran's "Axis of Resistance,"[129] enabling both sustained fundraising and the maintenance of latent operational capabilities that could be activated during periods of escalation.

Argentina provides the clearest and most historically significant case of this state–proxy nexus. The country experienced two major attacks: the 1992 bombing of the Israeli Embassy, which killed 29 people,[130] and the 1994 attack on the AMIA Jewish community center, which killed 85.[131] These attacks are linked to enduring Hezbollah infrastructure and Iran-associated diplomatic and operational networks. Leading figures such as Mohsen Rabbani have been connected to **the Iranian embassy in Buenos Aires** and the Omairi network.[132] Additional operatives, such as Samuel Salman El Reda, have been accused of coordinating Hezbollah's Islamic Jihad Organization activities across multiple regions since the early 1990s, pointing to long-standing transregional connections between Latin America and the Middle East.[133]

---

[129] Mansour, R., Al-Shakeri, H., and Haid, H., "The shape-shifting 'axis of resistance'. How Iran and its networks adapt to external pressures", March, 2025.

[130] WJC, "20 years after bombing of Israel's Embassy in Argentina: WJC leaders call for justice", March 16, 2012.

[131] Oyekalin, O., "Terrorists Attack Israeli Embassy and Jewish Center in Argentina", EBSCO, 2023.

[132] UNICRI, *The Nexus between Transnational Organized Crime and Terrorism in Latin America*, June, 2024.

[133] U.S. Justice Department, "United States District Court Southern District of New York sealed indictment on Samuel Salman El Reda", December 20, 2023.

Operationally, **Hezbollah activity in the region** can be understood as a pipeline consisting of surveillance of potential targets, sourcing of explosives, and staging of terror attacks. Evidence of preparatory stages includes attempts to source explosive precursors in Panama and the seizure of explosives in Bolivia.[134] In November 2023, Brazilian authorities, with Israeli intelligence support, detained suspected Hezbollah operatives allegedly planning attacks against Jewish targets in South America.[135] Additional reports have pointed to surveillance activities in Peru, while in Colombia there were allegations involving monitoring Israeli diplomatic delegations and a potential assassination plot targeting a former diplomat.[136]

These patterns are consistent with Iran's broader global operational model. Hezbollah-directed activity in Latin America overlaps with criminal networks, including those associated with Brazil's Primeiro Comando da Capital (PCC) and, to a lesser extent, Comando Vermelho, through shared logistical systems.

[134] Giambertoni, M., "Hezbollah's Networks in Latin America", *Expert Insights*, March, 2025.

[135] Reuters, "Brazilian police arrest third man suspected of links to Hezbollah", November 13, 2023.

[136] AP, "Peru arrests an Iranian man accused of planning an attack on an Israeli citizen", March 9, 2024; El Tiempo, "The search for Hezbollah's hidden plans in Bogotá", November 11, 2021.

SECURITY AND MILITARY SPILLOVERS INTO ILLICIT NETWORKS

While economic and criminal networks form the backbone of hybrid warfare, **security and military actors play a critical enabling role** where governance is weak or regimes face internal and external pressure. These actors leverage the illicit delivery infrastructure in ways that provide protection, operational capacity, and/or coercive reinforcement, allowing illicit networks to function more effectively while advancing broader geopolitical objectives. Formal military cooperation often serves as the initial entry point into these dynamics, creating institutional access, technical dependencies, and political alignment that can later be leveraged for opaquer forms of influence.

One of the clearest manifestations of this dynamic is the **use of paramilitary and quasi-state actors to secure strategic assets and stabilize allied regimes**. Russia stands out as the most active external actor in deploying irregular forces through private military contractors such as the Wagner Group. Until the 2023 mutiny, Wagner functioned as an indirect state proxy through the personal ties between Yevgeny Prigozhin and President Vladimir Putin. Following the mutiny, its repression, and Prigozhin's death, the organization was progressively absorbed into Russia's formal military command under the label "Africa Corps," making its activities more directly attributable to the Kremlin.[137] While Russia still preserves deniability at the operational level, its irregular forces have become more structurally embedded within formal military hierarchies than in the past, distinguishing them both from Iran's more diffuse proxy networks. In Venezuela, Wagner and its successor formations have been deployed to secure key infrastructure and resource extraction zones, including gold mining areas in the Orinoco region.[138] **Wagner** has been also involved in training pro-government militias (colectivos) in repression techniques later used against civilian demonstrators.[139]

Paramilitary actors operate as extensions of a broader system that links regime protection, resource control, and hybrid influence under conditions of sanctions and political pressure. By providing protection for state assets, logistical corridors, and extractive operations, these actors indirectly sustain illicit revenue streams that can be monetized outside formal financial systems. This convergence extends to the strengthening of internal regime security.[140]

---

[137] Pannegeon, E., "From Wagner to the Africa Corps: Changing Presence of Russian on the African Continent in 2025", *Black Sea Security Journal*, No. 1, 2026, pp. 101-107.

[138] Ellis, R. E., "Venezuela: Understanding Political, External, and Criminal Actors in an Authoritarian State", *Small Wars Journal*, January 14, 2022.

[139] Barnett, Lerner, Karsen, Zobec, P.A., "Russian Mercenaries on the Move in Latin America," *injuredoverseas.com*, accessed February 18, 2026.

[140] Russian-linked contractors have reportedly provided training not only to Venezuelan military units but also to pro-government militias, known as colectivos, in areas such as crowd control, counter-protest tactics, and the use of modern weaponry. These irregular groups—armed, state-aligned paramilitaries embedded in urban and peri-urban areas—have played a central role in the repression of anti-government demonstrations, contributing to hundreds of civilian casualties and thousands of arrests in recent protest cycles.

The connection between external paramilitary training and domestic coercive enforcement highlights a key feature of Russia's model: the integration of irregular security actors into regime survival strategies. Rather than relying exclusively on formal military institutions, this approach distributes coercive capacity across both state and semi-state actors, increasing flexibility while maintaining plausible deniability.

This reliance on irregularity is reinforced by recruitment that gives Russia access to foreign manpower beyond its formal military apparatus. It is estimated that more than 5,000 Cuban contractors have been recruited through Wagner to fight for the Russian armed forces in Ukraine. Reports also indicate that Wagner established central bases on the island from which elements of its leadership operate.[141]

In Colombia, Global Qowa Al Basheria S.A.S., a Bogotá-based company established in 2012, has become a central intermediary in recruiting former **Colombian military personnel for participation in the war in Ukraine on the Russian side**.[142] Evidence based on documents, communications, and testimony from at least twenty-one families indicates that this network combined a formal corporate façade with informal brokerage functions, including passport processing, travel logistics, accommodation, payment coordination, and digital communication. Recruitment activity has been concentrated in Bogotá's Chapinero district, where candidates were initially approached with offers of private security work in third countries before being redirected to Russia. The network was managed by retired Colombian colonels.[143] Colombian nationals have become one of the largest groups of foreign fighters killed in Ukraine by February 2026.[144]

The Russian paramilitary presence is embedded within a broader **long-term military partnership.** Between 2001 and 2013, the Russian state-owned defense company, Rosoboronexport facilitated approximately $11 billion in loans to Caracas,[145] to be used specifically for Russian arms purchases.[146] Based on the agreement Russia has supplied more than $4 billion in military equipment, including Su-30MK2 fighter jets, Mi-35M helicopters, armored vehicles, and advanced air defence systems such as the S-300VM and Pantsir-S1.[147] These systems require continuous maintenance, training, and technical support, **creating sustained operational dependence on Russian expertise.**

---

[141] Analyzy CBAP, "Russian Private Military Contractors' Presence in Latin America: Covert Russian Influence in the Western Hemisphere", CBAP, March 16, 2025.

[142] El Espectador, "La empresa de dos coroneles (r): así reclutan a exmilitares en Bogotá para ir a Rusia", February 22, 2026.

[143] Pardo, J., "Así funcionaría la red de reclutamiento de exmilitares colombianos para combatir en Rusia: dos coroneles serían los dueños del 'negocio'", *Infobae*, February 22, 2026.

[144] Ibid.

[145] Vladimirov, Rueda, and Osipova, *Global Reach*, CSD, 2024.

[146] Reuters, "Russia lends Venezuela $2.2 bln to buy weapons", September 14, 2009.

[147] Interfax, "Russia completes Venezuelan contracts on military purpose goods exports – agency", May 20, 2017.

Even in contexts where defense ties are more limited, such as Mexico, Russian equipment transfers, including Mi-17 helicopters,[148] have created maintenance and training dependencies that bind local security forces to Russian technical systems over time. Similar patterns are visible in Colombia, where Russian-origin equipment and servicing arrangements[149] have generated long-term reliance on spare parts and maintenance infrastructure.

The arms supply dependence on Russia has been reinforced with industry-level cooperation. In 2025, a Kalashnikov ammunition factory built by Russia's state arms exporter Rosoboronexport was inaugurated in Venezuela, with an annual production capacity of up to 70 million cartridges.[150] Rosoboronexport invested $474 million in the construction of the factory, a deal that has raised concern that this is an elaborate money laundering scheme aiming to siphon funds to the Venezuelan military junta.[151] Russia's military presence in Venezuela is complemented by the installation of S-300 air defense systems, the presence of at least 100 military instructors and technicians.[152]

More recently, in November 2024, two new strategic agreements were signed to strengthen military-technical cooperation and counterintelligence ties,[153] indicating the deepening and institutionalizing the bilateral security ties despite U.S. sanctions and diplomatic pressure. At the same time, these developments highlight both the depth and the limits of Russia's security model, as extensive military support and embedded defense infrastructure did not necessarily translate into effective regime protection under conditions of external intervention.

In **Nicaragua**, the Russian Ministry of the Interior established in 2014 training centers, expanded in 2017 to provide local police forces with surveillance and crowd-control capabilities.[154] The goal has been to not only strengthen the capacity of the Ortega regime for internal repression but to also provide Russian security services with a semi-permanent operational foothold in the region. In addition, since 2007, Moscow has supplied military equipment and infrastructure through the creation of an Anti-Narcotics Training Center.

Notably, this center is managed entirely by Moscow on its own terms, giving the Russians complete autonomy to operate as they wish. The two countries have also signed an agreement, allowing Russian warships to use Nicaraguan ports as part of a 2015 deal. In late 2025, they also signed a more comprehensive military cooperation agreement, focusing on intelligence sharing, training, and strategic partnerships.

---

[148] Vladimirov, and Galvez, *The Kremlin Playbook in Mexico*, CSD, 2025, p. 28.

[149] TASS, "Russia's arms deliveries to Colombia hit $500 mln over 20 years", December 4, 2017.

[150] Militar, G., "Venezuela recurre a Rusia en busca de misiles balíticos capaces de alcanzar objetivos estadounidenses si la crisis se agrava", 2025.

[151] Vladimirov, Rueda, and Osipova, *Global Reach*, CSD, 2024.

[152] The U.S. military operation to capture Maduro included jamming of S-300 radars, which blunted the Venezuelan response.

[153] The Moscow Times, "Russia Signs Security, Energy Deals With Venezuela", November 8, 2024.

[154] Farah, D., and Richardson, M., *Dangerous Alliances: Russia's Strategic Inroads in Latin America*, INSS, Strategic Perspectives, No. 41, 2022; Vladimirov, and Gálvez, *Authoritarian Shadows*, CSD, 2025.

In **Mexico**, there has been a visible increase in the **penetration of military-grade Russian weaponry into cartel arsenals**. Between 2022 and 2024, Russian-origin arms reportedly accounted for approximately 60 per cent of the weapons seized from Mexican cartels,[155] reflecting both the wider circulation of surplus military equipment following the war in Ukraine and its diversion through transnational criminal networks. This trend was underscored in 2026, when Russian-made rocket-propelled grenade launchers were identified in the arsenal of the Jalisco New Generation Cartel following the death of its leader.[156] While it is unlikely that there is direct control by the Kremlin over the arms procurement process for the cartels, the pattern shows that Russia-linked supply channels can strengthen local criminal actors in ways consistent with Moscow's broader grey-zone model of credible deniability.

The **shipment of arms and dual-use goods** overlaps with the flows of illicit goods. Military equipment, surveillance technologies, and technical components supplied through formal agreements can circulate beyond their intended use, particularly in contexts where oversight is limited. This dynamic is particularly evident in the export of **Russian surveillance architecture**. Systems based on **SORM** (System for Operative-Investigative Activities), which enable the interception and monitoring of telecommunications, internet traffic, and digital communications, have been deployed in allied states including Venezuela, Nicaragua, and Cuba.[157] These systems can provide authorities with direct access to communications data, often bypassing traditional oversight mechanisms.

Access to **SORM-like capabilities** is extending beyond state actors, reaching criminal organizations such as the Sinaloa Cartel or Los Zetas[158]. Cooperation agreements with Russia and Iran have often included not only defense equipment but also technologies linked to **drone systems and counter-drone capabilities**[159]. These technologies, while formally part of state-to-state cooperation, contribute to a broader security environment in which irregular actors and illicit networks can operate with enhanced protection and capacity.

Russia has also engaged in strategic defense investments such as the installation of the GLONASS (an alternative GPS system) ground station in 2017, operated by Roscosmos. Despite its civilian label, the GLONASS ground station has raised concerns about dual-use intelligence activities.[160] The agreement has been led by the Chilean-based Russian National Committee for the Promotion of Economic Trade with Countries of Latin America (NK SESLA). On the surface, it promotes Russian trade in Latin America and the Caribbean, within Russia's broader strategy to diversify and reorient its foreign trade

---

[155] Muñiz, E., "Cárteles mexicanos reciben armas y municiones rusas de alto poder", *ABC Noticias*, August 14, 2025.

[156] Fisher, S., "Inside El Mencho's arsenal: high-powered weapons, 400 gunmen, drones and land mines", *Los Angeles Times*, February 24, 2026.

[157] Farrah, and Richardson, *Dangerous Alliances*, INSS, Strategic Perspectives No. 41, 2022.

[158] Ibid.

[159] Globovisión, "Maduro thanks Russia, China, and Iran for their support in drone system technology", July 6, 2024.

[160] Tlis, F., "Russian Military Politician: Tracking Station in Nicaragua Does Not Spy on US", *VoaNews.com*, April 12, 2017.

in response to Western sanctions.[161] In fact, it has emerged as an unofficial group of intelligence and surveillance companies and organizations. They are involved in cyber intelligence, cryptology, and surveillance.[162] NK SESLA has promoted Russia's GLONASS also in Brazil and Chile.

Another dimension of the security cooperation with authoritarian states includes the deployment of foreign **surveillance and internal security systems**. In Venezuela, the state-owned China National Electronics Import & Export Corporation (CEIEC) has supplied software, equipment, and training that support digital monitoring, communications control, and information filtering.[163] Systems such as the carnet de la patria, which integrates identity, welfare distribution, and political monitoring, illustrate how technological infrastructure can reinforce regime control.[164] Bolivia provides another example. The previous government, dominated by the far-left *Movimiento al Socialismo* obtained Chinese-supported surveillance systems such as BOL-110, which integrate cameras, command systems, and data processing into national security systems and was financed through a RMB 350 million concessional loan from China Eximbank in 2018.[165]

In addition**,** Bolivia's Túpac Katari (TKSAT-1) satellite, financed, built, and launched by China,[166] has illustrated how technological dependence can even operate at the level of sovereign communications systems. Although presented domestically as a symbol of technological autonomy, its operational architecture–including software, maintenance, and technical support–remains closely tied to Chinese providers, creating long-term structural reliance.

Argentina has also doubled down on Chinese information security technology. A 2012 bilateral agreement enabled the construction of a Chinese-operated deep-space station in Neuquén, managed by the China Satellite Launch and Tracking Control General (CLTC), an entity linked to the People's Liberation Army Strategic Support Force. The facility, covering approximately 200 hectares under a 50-year agreement, includes a 35-metre antenna capable of satellite tracking and data transmission to Chinese networks. Limited Argentine oversight and confidentiality provisions have raised concerns regarding transparency, data sovereignty, and potential dual-use applications.

China's technological footprint extends on **local level**. In Argentina's Jujuy province, a $30 million contract awarded to ZTE in 2019 introduced surveillance cameras, monitoring centers, and emergency response systems.[167]

---

[161] Ternovsky, V., "América Latina y el Caribe se consolidan como una de las prioridades del comercio exterior ruso" [Latin America and the Caribbean consolidate as one of Russia's foreign trade priorities], *Sputnik*, June 23, 2025.

[162] Farrah, and Richardson, *Dangerous Alliances*, INSS, Strategic Perspectives No. 41, 2022.

[163] U.S. Department of the Treasury, "Treasury Sanctions CEIEC for Supporting Venezuelan Intelligence Efforts to Undermine Venezuelan Democracy", August 19, 2020.

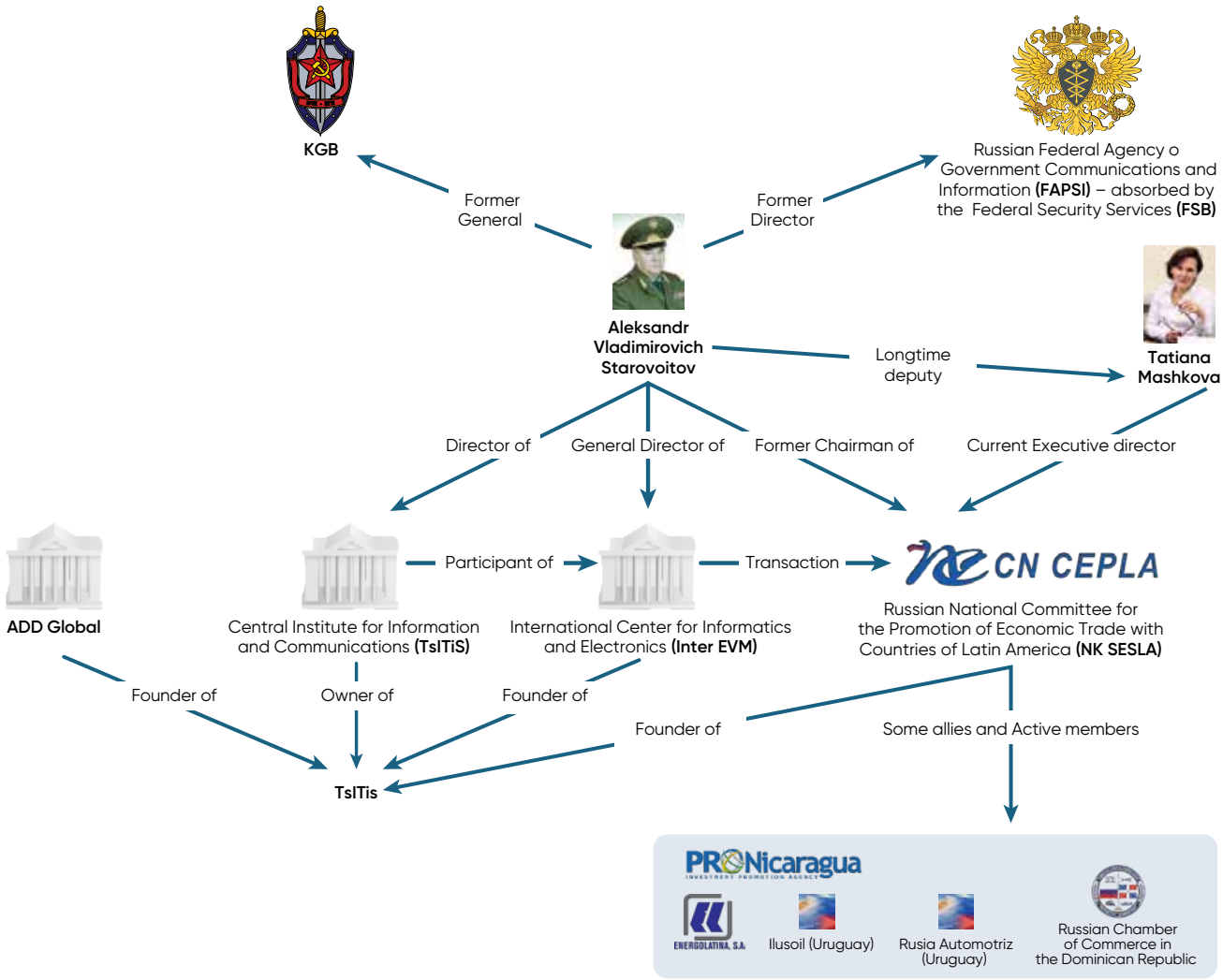
[164] Berwick, A., "How ZTE Helps Venezuela Create China-Style Social Control", *Reuters Special Report*, November 14, 2018.

[165] AIDDATA, "China Eximbank provides RMB 350 million government concessional loan for Phase I of BOL-110 Command and Control System for Citizen Security Project (Linked to Record ID#54577)".

[166] American Security Project, "China's Footprint in Bolivian Space", August 18, 2023.

[167] Ellis, R. E., "The Evolution of Chinese Engagement in Argentina under Javier Milei", Center for Strategic and International Studies Analysis, June 5, 2024.

Figure 9. NK SESLA: A Russian Intelligence-Linked Network in Latin America



Source: CSD based on Farah, D., and Richardson, M., *Dangerous Alliances: Russia's Strategic Inroads in Latin America*, Washington D.C.: Institute for National Strategic Studies, Strategic Perspectives, No. 41, 2022.

In countries with strong security ties to the US, such as Mexico and Colombia, China's defense engagement remains limited to training exchanges, professional education programs, and modest equipment transfers[168] rather than comprehensive formal military agreements. Beijing maintains a foothold through **low-visibility institutional engagement**.

Even so, in Colombia, by 2016, more than 200 Chinese personnel had reportedly completed training at Colombia's elite Lanceros course at the Tolemaida air base, while Colombian officers have attended defense education programs in China.[169] China maintains a defense attaché in Bogotá, and cooperation has gradually expanded into areas such as space-related training for Colombian Air Force personnel and academic exchanges involving defense institutions.[170]

[168] AIDDATA, "China donates 2 Harbin Y-12 aircraft to Satena, Colombian national airline".

[169] Ellis, R. E. *Colombia's Relationship with the PRC*, CSIS, November 10, 2022.

[170] Ibid.

RESPONDING TO HYBRID INFLUENCE

Latin America has become a permissive environment for a new form of external influence in which economic engagement, political leverage, and illicit networks are increasingly interconnected. China, Russia, and Iran operate through different entry points, but their activities converge into layered systems that combine formal statecraft with informal and covert mechanisms. Over time, these systems generate durable influence that is embedded in institutions, markets, and security structures rather than exercised through overt pressure.

Influence in this model accumulates through interaction across sectors. Trade, infrastructure, finance, media, and logistics are not isolated channels. They reinforce one another and create cumulative leverage. Infrastructure projects provide access to strategic nodes; financial arrangements reduce transparency and increase dependency; media and political networks shape the local environment in which economic decisions are made. Once established, these layers are difficult to disentangle because they are integrated into the normal functioning of state and market systems.

A central feature of this model is the functional role of organized crime. Criminal networks provide logistics, financial channels, and access to informal economies that are difficult to replicate through formal mechanisms. External actors engage these networks selectively, relying on their capabilities without requiring direct control. This produces flexible arrangements that can adapt to regulatory pressure, sanctions, or political change. The absence of a formal hierarchy makes these systems harder to trace and disrupt.

The three principal actors follow distinct operating logics. **China** builds influence through scale and continuity, anchoring its presence in trade, infrastructure, finance, and technology. **Russia** concentrates on strategic sectors and combines economic ties with political and informational instruments, supported by opaque corporate and financial structures. **Iran** operates through decentralized networks shaped by sanctions pressure, relying on intermediaries, informal finance, and proxy-linked ecosystems. These approaches differ in visibility and structure, but they rely on the same enabling conditions: regulatory gaps, fragmented oversight, and the overlap between licit and illicit activity.

Formal engagement provides the foundation for more complex forms of influence. Access to ports, energy systems, mining operations, financial institutions, and digital infrastructure creates opportunities that extend beyond the initial economic relationship. Over time, these channels can support sanctions evasion, trade-based money laundering, covert logistics, or surveillance and information control. **The shift from formal to hybrid activity is gradual** and often takes place within the same institutional and commercial frameworks.

Latin America's institutional diversity and uneven enforcement create opportunities for external actors to operate across jurisdictions. Financial flows, trade routes, and criminal networks connect multiple countries, while regulatory responses remain largely national. This mismatch allows influence mechanisms to shift location, exploit weaker nodes, and reconfigure when pressure increases in a specific country.

Responding to hybrid influence in Latin America requires a shift in how states organise their security and governance frameworks. The convergence between foreign influence and organized crime cuts across institutional mandates that are typically separated–counterintelligence, financial supervision, anti-corruption enforcement, and organized crime policing. As the European experience shows, fragmentation between these domains creates operational blind spots that external actors can exploit.

A first priority is therefore **institutional integration**. In most Latin American countries, counter-organized crime units, financial intelligence authorities, and national security services operate in parallel rather than as part of a unified threat assessment system. This limits the ability to detect how illicit financial flows, criminal logistics, and foreign influence operations interact. More effective responses require joint analytical capabilities that bring together intelligence, law enforcement, and financial oversight. In practice, this means developing integrated task forces or fusion mechanisms at the national level that treat hybrid influence as a single operational problem rather than a set of disconnected risks.

This integration needs to extend beyond national borders. Hybrid influence networks operate regionally, moving across jurisdictions through trade corridors, financial systems, and criminal supply chains. Yet cooperation in Latin America remains uneven and often reactive. **Strengthening regional intelligence-sharing frameworks**, whether through existing platforms such as Ameripol, financial intelligence networks, or ad hoc bilateral arrangements, would improve visibility over cross-border activities. The European debate on building joint intelligence capacities reflects a recognition that fragmented responses reduce deterrence and slow reaction times; similar logic applies in Latin America, where coordination gaps are even more pronounced.

Targeting financial and commercial infrastructures is equally critical. Hybrid influence depends on the ability to move funds, commodities, and services through a mix of legal and illicit channels. Trade-based money laundering, shell companies, and informal financial systems provide the backbone of these operations. Disrupting them requires more than traditional anti-money laundering frameworks. It calls for a stronger focus on high-risk sectors and supply chains, including energy exports, extractives, logistics hubs, and free trade zones, where large volumes and weak oversight create opportunities for illicit activity. European experience shows that following financial flows and tightening control over intermediary structures can significantly constrain the operational space of hybrid networks.

At the same time, **enforcement efforts need to reflect the evolving role of organized crime**. Criminal networks are no longer peripheral actors; they function as service providers within broader systems of influence, enabling sanctions evasion, smuggling, cyber operations, and covert logistics. Treating organized crime solely as a domestic law enforcement issue underestimates its strategic role. Recognizing its integration into foreign influence operations should lead to a reprioritization of resources, investigative mandates, and analytical frameworks. As highlighted in the European case, acknowledging the use of criminal actors as instruments of statecraft is a prerequisite for mobilizing an effective response.

Another critical area is **economic security governance**. Many of the vulnerabilities identified in this report originate in strategic sectors where foreign investment, weak regulation, and political discretion intersect. Infrastructure projects, energy systems, and extractive industries provide entry points that can later support hybrid activities. Strengthening oversight of these sectors–through **investment screening, procurement transparency, and regulatory enforcement**–can reduce exposure to opaque arrangements and limit the conversion of economic presence into political leverage. This does not imply restricting foreign investment, but rather ensuring that it operates within transparent and enforceable frameworks.

Greater transparency and accountability across intermediary networks are also essential. Influence is often exercised through local actors such as business elites, political figures, corporate entities, and service providers, who operate within the legal economy while facilitating grey-zone activities. **Improving oversight of political financing, lobbying, and public–private partnerships** can reduce the ability of these intermediaries to act as conduits for external influence. This is particularly relevant in environments where state capture risks are already high and where informal practices are embedded in institutional processes.

Finally, responses need to **address the systemic nature of hybrid influence** rather than its individual manifestations. Efforts focused narrowly on specific actors, transactions, or sectors tend to produce displacement effects, with activities shifting to less regulated areas or jurisdictions. More durable impact depends on strengthening the underlying resilience of governance systems, **improving regulatory capacity, reducing informality**, and enhancing coordination across institutions and borders. This is a longer-term process, but without it, short-term enforcement measures are likely to have limited effect.

The European experience demonstrates that hybrid threats thrive in fragmented systems, where institutional silos, regulatory gaps, and uneven cooperation create space for complex networks to operate. Latin America faces similar conditions, often in more acute form. Addressing the convergence of foreign influence and organized crime will therefore depend less on the introduction of new instruments and more on the ability to connect existing ones into coherent, coordinated responses.