Observatoire ARGA

Report on Sanctions and Compliance for 2025

THE EVOLUTION OF HYBRID INTELLIGENCE SERVICES IN EURASIA

Integration of Intelligence Agencies, Corporate Structures and Criminal Networks in Transnational Operations

Author:

Sergei Khrabrykh — President of ARGA, PhD

Organization: Observatoire ARGA – Sanctions and Compliance Division

Correspondence Address: 14 rue Jacques Laffitte, Bayonne, 64100

Contact: info@argaobservatory.org

Paris, 12 November 2025

Table of Contents

Executive Summary

The ARGA Observatory report documents a long-term process of mutation within the post-Soviet intelligence and security services, transforming them from classical agencies operating in the "security–counterintelligence–operational control" paradigm into complex hybrid structures that combine operational, economic, political, and criminal-financial functions.

These institutions have gradually ceased to be exclusively state security bodies. Instead, they have become institutional actors in both the economy and geopolitics, forming parallel channels of resource distribution, influence, and capital. The main trends include:

— the integration of intelligence personnel into major businesses and state monopolies;

— the formation of closed structures around export-resource industries;

— involvement in transnational operations, including the control of financial flows, crypto-assets, and foreign-trade schemes;

— the use of coercive instruments for corporate warfare, asset redistribution, and pressure on elites;

— direct cooperation with criminal networks, grey brokers, and parallel logistics chains;

— the development of cyber-operations, censorship, surveillance, and financial intelligence within a unified governance circuit.

The emerging model of Eurasian intelligence services represents a form of "coercive capitalism," in which intelligence becomes not only a tool of security but also a mechanism of access to assets, markets, people, and transit.

The boundaries between the state, major capital, and illicit activity are becoming structurally blurred.

The report focuses on:

• the interaction between intelligence agencies, state corporations, and offshore networks;

• their role in asset confiscations and international pressure on business owners;

• participation in sanctions-evasion schemes and control over grey export/import channels;

• interference in political processes in neighboring countries;

• the formation of informal channels of influence beyond national borders.

The report records the emergence of new forms of centralized power, where security structures act as brokers of technical, financial, and criminal capabilities, able to operate both domestically and abroad.

This evolution is reshaping the architecture of international security. Hybrid intelligence services are no longer merely instruments of repression but transnational mechanisms of influence, capable of triggering political crises, intervening in corporate systems of other states, creating new

channels for capital flight, disrupting economic equilibria, and exerting pressure on elites, opposition groups, and businesses.

The ARGA Observatory report aims to:

— document the architecture of hybrid intelligence services;

— identify models of their interaction with the economy and criminal networks;

— locate points of international vulnerability;

— propose systemic mechanisms of oversight and counteraction.

The hybridization of security services is becoming a defining factor of the 21st century, shaping the format of conflicts, financial flows, and political power across Eurasia.

1. Methodology

The methodological framework of this report is based on a combination of intelligence, legal, comparative-analytical, and empirical approaches.

The aim of the study is to reconstruct the transformation of intelligence agencies into hybrid coercive-economic structures, identify their key operational models, and assess their transnational implications.

The report relies on:

— OSINT data (open sources, corporate registries, investigative media, parliamentary reports, data leaks, court publications), which made it possible to map the external manifestations of intelligence agency activity;

— HUMINT materials, including testimonies from informants, former security-service personnel and affiliated actors, as well as interviews with entrepreneurs and lawyers who have faced transnational pressure;

— analysis of 110 documented intelligence-service cases, including operations involving capital transit, extradition initiatives, participation in corporate conflicts, activities within the cryptocurrency ecosystem, and raiding-type schemes;

— review of international judicial decisions (ECtHR, UN WGAD, appellate courts of France, Germany, Spain, and the United Kingdom) dealing with the persecution of entrepreneurs, officials, whistleblowers, and figures involved in politico-economic conflicts;

— data from Interpol, Europol, and SIS II, reflecting cross-border requests, international notices, and attempts by intelligence agencies to exercise extraterritorial jurisdiction;

— research on criminal networks, cryptocurrency chains, parallel-import systems, and corporate wars, enabling the identification of the economic and criminal components of hybrid structures;

— ARGA Observatory analytical materials (2020–2025), including internal legal reviews, FININT reconstructions of capital flows, classifications of raiding and politico-economic schemes, and monitoring of the evolution of intelligence-service digital tools.

This combination of sources allowed the authors not only to describe the phenomenon of hybrid intelligence services but also to trace how operational mechanisms migrate into the realms of economics, corporate influence, and international politics.

2. Introduction: The Nature of Hybrid Intelligence Agencies

Hybrid intelligence agencies represent a new type of coercive institution that has emerged through the fusion of traditional intelligence functions with mechanisms of political control, economic management, and criminal-financial operations.

Unlike classical security services—focused on intelligence gathering, counterintelligence, and national security—hybrid structures operate as supranational actors of influence whose sphere of interest extends far beyond the boundaries of domestic legal order.

They intervene in the private sector, shape access rules to state resources, control capital, participate in corporate wars, and construct international mechanisms of coercion. Traditional instruments of operational pressure—investigations, criminal cases, wiretapping, covert operations—are now complemented by mechanisms previously uncharacteristic of security agencies: interference in business processes, management of offshore structures, integration into cryptocurrency flows, influence over media ecosystems, and manipulation of international legal instruments.

Hybrid intelligence agencies function as a parallel system of power and asset distribution, where legal norms often play a subordinate role, while operational decisions become elements of the state's economic strategy. They operate transnationally, using Interpol channels, extradition mechanisms, international financial cooperation, and digital tools for tracking capital.

In essence, they constitute a new category of institutional actor positioned between the state, the corporate sector, and criminal networks. Their activities affect international security, investment risk profiles, digital criminology, the shadow-capital market, and the architecture of human rights. These dimensions form the analytical focus of the subsequent chapters of the ARGA Observatory report.

3. Structure and Functions of Hybrid Intelligence Agencies

Hybrid intelligence agencies operate as multilayered systems that combine political control, economic governance, coercive enforcement, international operations, as well as tools of digital intelligence and shadow criminal coordination. Below is a detailed breakdown of the key functional domains.

3.1. Political Control

Hybrid intelligence agencies become instruments for maintaining power and managing elites. Their tasks extend far beyond classical internal security and include:

— systematic suppression of political opposition, leadership groups, and media structures capable of forming alternative centers of influence;

— control over bureaucrats, business elites, and regional administrations through the threat of criminal prosecution, compromising material, and force-backed interventions;

— neutralization of whistleblowers and individuals involved in corruption schemes who possess access to sensitive information.

Here, the repressive function is not an emergency measure but a regularized tool for managing the balance of power.

3.2. Economic Governance

Security agencies become market actors, controlling key industries and the redistribution of property. Their functions manifest through:

— overseeing major privatization, nationalization, and the transfer of assets to affiliated structures;

— managing state and quasi-state sectoral holdings in oil, gas, metals, logistics, telecom, and the military–industrial complex by placing loyal top managers;

— controlling financial flows, export chains, and credit channels that sustain the revenues of ruling clans and corporate alliances.

This forms an economic vertical in which the security apparatus acts simultaneously as owner, arbiter, and moderator of the market.

3.3. International Operations

The expansion of intelligence agencies beyond national borders creates a new architecture of coercive international influence. Core instruments include:

— transnational prosecution of entrepreneurs, politicians, and individuals involved in domestic conflicts via extradition requests and MLAT mechanisms;

— using Interpol, SIS II, and diplomatic channels as tools of pressure, asset freezing, and international oversight;

— conducting operations aimed at influencing foreign courts, political processes, business structures, and diaspora networks.

Such external activity transforms intelligence agencies into an extraterritorial instrument of state policy.

3.4. Criminal Integrations

A number of hybrid intelligence agencies develop a stable symbiosis with criminal groups, providing them protection in exchange for access to shadow markets and illicit networks:

— using criminal syndicates for smuggling gold, technology, weapons, and sanctioned goods;

— participating in schemes of fiat and crypto cash-outs, illegal capital flight, and cryptocurrency operations;

— managing grey financial flows through loyal organized crime groups that carry out enforcement and debt-collection functions.

Thus, intelligence services become the center of a criminal hub rather than a structure that opposes it.

3.5. Digital Intelligence

The digital domain is the primary control instrument of the 21st century. Operational capabilities include:

— monitoring social networks, messengers, and mapping the social graphs of elites and activists;

— cyberattacks, hacking, DDoS operations, data theft, and planting malicious modules into IT infrastructures;

— tracking cryptocurrency flows, conducting blockchain analytics, and influencing digital financial systems.

Digital intelligence transforms security services into global actors in cyber-competition, where the state, corporations, and criminal networks operate as a single integrated entity.

4. Regional Map of Hybrid Intelligence Agencies

Hybrid intelligence agencies across Eurasia are not uniform. They evolve along different trajectories but exhibit common structural traits: fusion with political elites, influence over the economy, international operational reach, and deep integration with criminal channels. Below is a systematized regional overview.

4.1. Russia — The Model of a Security–Economic Power Structure

Russia's FSB represents the most advanced example of a hybrid intelligence service. It controls strategic sectors — energy, chemicals, logistics, telecom, and the military–industrial complex — and intervenes directly in corporate conflicts.

— the FSB participates in the redistribution of assets, using criminal cases and Interpol channels as instruments of pressure on entrepreneurs;

— the security apparatus is integrated into financial operations: export hubs, commodity chains, cryptocurrency routes;

— the digital infrastructure (SORM, DPI-surveillance, cyber-operations) turns the agency into a central node for controlling information and alternative political networks;

— the service conducts transnational operations: pressure on emigrants, extradition requests, freezing of foreign assets.

Russia is the core model from which other regional states borrow mechanisms of elite and capital management.

4.2. Kazakhstan — Post-Crisis Transformation of the KNB

After the January 2022 events, the National Security Committee (KNB) underwent a power reconfiguration. The security apparatus was partially reformed but retained its economic levers.

— the KNB participates in clan-based conflicts, shaping the outcomes of corporate wars and privatization processes;

— pressure on elites is exercised through economic charges, extradition initiatives, and control over land and resource-based assets;

— the service is embedded in raw-material exports, banking channels, logistics networks, and cryptocurrency trade;

— the international dimension is expanding: Kazakhstan actively uses extradition mechanisms and MLAT channels.

The system combines a modernized state bureaucracy with a persistent informal network of influence.

4.3. Azerbaijan — A Security Apparatus with a Clan-Based Architecture

In Azerbaijan, intelligence and security services form an interconnected system of security → economy → familial–political control.

— security structures cooperate with political and oil-and-gas groups, shaping investment flows and controlling logistics routes;

— pressure on entrepreneurs and activists is accompanied by criminal cases and cross-border persecution;

— international activity includes Interpol requests, operations in Turkey, Georgia, and the EU;

— governance relies on informal decision-making centers rather than institutional rule of law.

Hybridization is expressed through the merger of security forces, corporations, and ruling family elites.

4.4. Belarus — A Totalized Security Vertical

The Belarusian model is the most rigid and monolithic in the region. Intelligence and security agencies operate as instruments of complete control over the state and the economy.

— business is managed through the threat of criminal prosecution and confiscations;

— emigration of business elites is perceived as a security threat, resulting in persecution abroad;

— the security apparatus controls access to foreign currency, state procurement, and external trade;

— digital surveillance and internal repression function as systemic, permanent mechanisms.

Belarus represents a security–state paradigm in which the economy is fully embedded into the apparatus of coercion.

4.5. Kyrgyzstan and Uzbekistan — A Hybrid of Corruption and Security-Based Corporatism

In these states, intelligence services evolve along a trajectory of criminal–clan integration.

— security bodies participate in the squeeze-out of businesses and the redistribution of resources;

— the grey sector is highly active: smuggling, cryptocurrency flows, EAEU logistics hubs;

— diasporas abroad become targets of influence: extradition attempts, threats, control of remittances;

— political instability amplifies the role of security services as economic moderators.

These models are dynamic, fluid and capable of rapid adaptation during shifts of political power.

4.6. South Caucasus (Georgia, Armenia) — Intelligence Services as Economic Moderators

In the South Caucasus, security services are less centralized but actively shape the business environment.

— intervention in corporate conflicts and redistribution of assets;

— control over digital financial flows, exchanges, and OTC markets;

— cross-border persecution operations, particularly targeting business emigration;

— use of intelligence bodies as instruments of influence over diasporas.

The South Caucasus serves as a key transit hub where intelligence agencies act as de facto economic regulators operating outside parliamentary oversight.

5. Case Studies

Case analysis reveals how hybrid intelligence services operate not as isolated security bodies, but as integrated centers of control over the economy, information flows, and criminal-legal mechanisms. The three cases below illustrate the most characteristic patterns.

Case 1 — A Transnational Operation Against an Entrepreneur

A political–financial conflict deployed through international mechanisms.

In this scenario, security services initiate a criminal case (typically under economic charges: fraud, tax evasion, formation of an "organized group"), after which an artificial evidentiary base is constructed — testimony obtained under pressure, unaudited financial documents, rulings issued in closed courts.

The subsequent mechanism includes:

— issuing an INTERPOL notice to restrict the individual's mobility;

— sending requests to foreign banks to freeze accounts and block assets;

— attempts at extradition using an INTERPOL Red Notice combined with proceedings before the national courts of a partner state;

— parallel pressure on family members and business partners to force the transfer of ownership stakes.

Such a mechanism is frequently used not for justice, but for the forcible seizure of assets and the exclusion of an entrepreneur from international capital-management chains.

Case 2 — Intelligence Service Participation in a Corporate War

The security apparatus as a direct actor in an economic conflict.

In this type of case, the intelligence service becomes an active side in a corporate confrontation, supporting one elite group against another. Typical elements include:

— initiation of criminal cases to pressure a competitor and change ownership structures;

— security-backed raids, asset seizures, interference in M&A transactions;

— information campaigns — leaks, media operations, engineered reputational damage;

— use of international channels (INTERPOL, MLAT, FATF-related notices) to legitimize coercive actions.

As a result, the state apparatus functions as a private corporate instrument, undermining investment security and destroying judicial predictability.

Case 3 — A Hybrid Operation Through Digital Networks

An information-cyber attack as a political-economic weapon.

The modern format of hybrid intelligence services includes full-scale digital operations aimed at discrediting and subordinating the target:

— hacking of correspondence, cloud storage, and corporate servers;

— publication of compromising materials through controlled Telegram/YouTube/media channels;

— involvement of criminal networks to conduct DDoS attacks, extortion, and crypto-blackmail;

— digital pressure accompanied by attempts to construct a legal basis for criminal prosecution.

At the final stage, international search mechanisms and financial freezes are activated, turning an IT-attack into a multi-layered coercive operation targeting both property and reputation.

6. Institutional Implications for International Security

Hybrid intelligence services in Eurasia — combining functions of intelligence, economic governance, criminal networks, and transnational persecution — generate a new model of international risk. The implications extend far beyond regional politics, shaping threats to global legal order, investment security, financial stability, and refugee protection systems. Each of the following points reflects a systemic shift in the global security architecture.

1. Blurring of Boundaries Between the State and Organized Crime

Hybrid intelligence services operate simultaneously as state authorities and as actors within the shadow economy. They control capital transit, facilitate illicit transactions, cooperate with criminal brokers, and build "parallel governance models."

As a result:

— state prosecution becomes indistinguishable from criminal intimidation;

— a grey layer of power emerges, unaccountable to courts or parliaments;

— international law enforcement loses the ability to distinguish between lawful authority and sovereign criminal machinery.

This undermines the foundations of political–legal sovereignty and creates a model of a *"state as a criminal consortium."*

2. Weakening of the Rule of Law at the International Level

When politically motivated criminal cases are pushed through INTERPOL, MLAT channels, SIS II, or bilateral treaties, the independence of international legal mechanisms is put at risk.

Manifestations include:

— INTERPOL, the CCF, and national courts are forced to evaluate requests that disguise corporate coercion as "criminal prosecution";

— judicial systems of the EU must filter thousands of politicized requests;

— international law becomes overloaded with cases that are not criminal in nature but driven by coercive economic and political motives.

This leads to an erosion of trust in legal institutions that underpin international security.

3. Heightened Threats to Refugees, Elites, and Whistleblowers Abroad

High-level individuals and witnesses of corruption schemes face continued persecution even after receiving asylum.

Risks include:

— attempts at physical pressure through diasporas and covert operatives;

— criminal cases initiated against relatives in the home country;

— surveillance, attacks on assets, attempts at extradition;

— death threats and blackmail through kompromat.

As a result, asylum ceases to provide genuine safety — threats become transnational.

4. Infiltration of Financial Systems in the EU, UAE, Turkey, and Singapore

Hybrid intelligence services actively employ offshore networks, crypto OTC channels, shell law firms, and mirror-payment schemes to control and repatriate capital.

Consequences:

— erosion of global AML barriers;

— growth of illicit transfers, pseudo-loans, and trust structures;

— penetration of security actors into the compliance architecture of banks.

Mechanisms intended to protect the global financial system increasingly serve the operational interests of authoritarian security structures.

5. Growth of INTERPOL Abuse as a Tool of Geopolitical Pressure

International criminal notices are used for:

— corporate raiding,

— political coercion,

— asset seizure,

— forced return of individuals,

— destruction of reputations.

The rise in abuses leads to increased appeals to the CCF, more extradition refusals, the creation of EU-level filtering systems, and declining trust in INTERPOL as a neutral cooperation mechanism.

7. Forecast 2025–2027

1. Deepening of the "security–economic" functions of intelligence services

In the coming years, intelligence agencies in several Eurasian states will increasingly act not only as political-repressive bodies but also as economic power centers. This will include:

— expanding their role in privatization and re-privatization processes;

— exercising direct influence over the allocation of state contracts, access to natural resources, infrastructure projects, and financial flows;

— institutionalizing "security supervision" of major deals and corporate conflicts.

Intelligence services will not merely "protect state interests" but operate as independent economic actors competing with other clans and ministries. This will further blur the boundaries between politics, business, and security structures, solidifying a model in which major business cannot function without informal approval from security agencies.

2. Intensification of transnational operations against elites and business figures

Cross-border pressure on entrepreneurs, former officials, top managers, witnesses, and whistleblowers will become the norm rather than the exception. Expected developments include:

— growth in INTERPOL submissions, MLAT requests, and extradition initiatives;

— active use of foreign asset freezes (bank accounts, real estate, corporate shares);

— closer coordination among Eurasian security agencies, especially within regional alliances and informal networks.

Those most at risk are individuals holding key information on corruption, privatization schemes, sanctions-evasion mechanisms, and shadow financial routes. Their legal status will remain unstable even in "safe" jurisdictions, increasing demand for comprehensive international protection strategies (legal + media + compliance + secure asset structuring).

3. Expansion of cyber-operations in Europe and the United States

Hybrid intelligence agencies will increasingly shift activity into the digital domain, targeting infrastructures and key actors in the EU, UK, and US. Anticipated trends:

— growth in targeted cyberattacks on politicians, businesspeople, lawyers, journalists, and research institutions involved in corruption or illicit-finance investigations;

— combining cyber-operations with information warfare (leaks, discreditation, fake investigations targeting victims of political or corporate conflicts);

— using cryptocurrencies and anonymous digital services for payments, coordination, and operational masking.

This will increase pressure on Western cybersecurity systems and likely lead to the formal recognition of "hybrid intelligence agencies" as a specific threat category in NATO, EU, and specialized analytical frameworks—distinct from classic cybercrime and military intelligence.

4. Rise of corporate wars orchestrated by intelligence agencies

Corporate conflicts will increasingly function not as causes but as *instruments* of political strategy. Intelligence services will:

— initiate or support criminal cases against owners and executives to facilitate redistribution of assets;

— supervise media outlets, "investigative" platforms, and lobbying structures targeting specific business groups;

— use international legal mechanisms (INTERPOL, foreign courts, asset freezes) to pressure individuals who have already left the country.

Some of these corporate wars will become fully transnational: one side relying on foreign legal protection, the other—on hybrid intelligence tools and international pressure framed as "economic" prosecutions. This will intensify the clash between investment-protection principles and the "anti-corruption" narratives of authoritarian regimes.

5. Emergence of a new architecture for international monitoring of intelligence services

In response to the rise of hybrid intelligence agencies, a new layer of international oversight will gradually form. Likely developments include:

— expanding the mandates of existing mechanisms (Council of Europe, UN, EU) to monitor intelligence-agency abuse in extradition, economic cases, corporate conflicts, and cyber-operations;

— progressive creation of informal "risk registries" of jurisdictions whose intelligence services systematically weaponize international cooperation mechanisms for political-economic coercion;

— strengthening the role of the CCF, national courts in the EU, and specialized NGOs and research institutes documenting and conceptualizing hybrid-intelligence practices.

In the long term, a new field of international law and political science is likely to emerge—*"security governance & hybrid intelligence studies"*—treating these actors not as anomalies but as key variables in the global security landscape.

8. ARGA Observatory Recommendations

The recommendations aim to build a resilient global security architecture capable of countering the expansion of hybrid intelligence agencies, their penetration into the economy, and their transnational coercive practices.

1) International Institutions (UN, EU, Council of Europe, OECD, OSCE)

A structural shift is required in how the international community approaches authoritarian-type intelligence agencies — moving from diplomatic caution to analytical and legal oversight. ARGA Observatory recommends:

— establishing an International Index of "Security–Economic Pressure" — a rating of countries whose intelligence services engage in corporate conflicts, asset recovery campaigns, extradition-driven prosecutions, and politically motivated cross-border operations;

— launching a monitoring system for transnational operations of intelligence services, gathering data on the persecution of entrepreneurs, whistleblowers, former officials, top managers, lawyers, and politically exposed individuals;

— strengthening protection mechanisms for refugees and persons at risk of coercive persecution, including simplified asylum procedures, expanded Witness Protection programs, and the creation of international emergency-protection mechanisms.

These measures would create a legal barrier that reduces the effectiveness of coercive pressure as a tool of political and economic struggle.

2) Interpol and Europol

The digital environment and modern financial channels have enabled state pressure without physical jurisdiction. Interpol and Europol must adapt and update their screening mechanisms:

— enhance the scrutiny and filtering of Red Notices and Diffusions originating from jurisdictions where intelligence services are involved in corporate wars, economic prosecutions, and asset confiscations;

— introduce an Interpol Abuse Monitoring Protocol, documenting refusal rates, repeated submissions, CCF-reviewed notices, and the longitudinal history of persecution of specific individuals;

— create a high-risk jurisdiction list, whose requests must be accompanied by a comprehensive evidentiary package proving the absence of political motivation, family pressure, fabricated materials, or economic interest.

In the long term, this may lead to the development of a sanctions mechanism against states that systematically abuse international law enforcement channels.

3) Law Schools, Think Tanks, and Research Institutes

The academic sector must begin to study hybrid intelligence agencies as a *new class of global political actors*, rather than as part of the traditional "state security" model.

— develop intelligence-service studies as a distinct interdisciplinary field, combining criminology, political sociology, international law, and political economy;

— build comprehensive case databases on hybrid intelligence agencies — including extraditions, Interpol persecutions, corporate wars, asset confiscations, cyber-operations, pressure on businesses, and persecution of whistleblowers;

— develop indicators of security-service influence on the economy, covering control over privatization processes, shadow financial networks, crypto-operations, and capital flight.

A robust, evidence-based academic foundation is the key resource for future reforms. Without large-scale documentation of cases, it is impossible to establish international legal barriers against coercive state pressure.

9. Conclusion

The hybridization of intelligence agencies in Eurasia is neither a marginal phenomenon nor a temporary anomaly. What we observe is a long-term institutional transformation in which security and intelligence services cease to function solely as instruments of national security and instead become autonomous actors in global politics, finance, and the shadow economy. Their functions are no longer limited to intelligence gathering, counterintelligence, or counter-extremism: they participate in corporate conflicts, control capital flows, oversee privatization processes, manage digital networks, and intervene in the international operations of private businesses.

In effect, intelligence agencies are becoming a new type of power operating outside constitutional frameworks, outside judicial oversight, and outside classical accountability models. In several countries, they form a parallel governance system — a “state within a state” — where decisions are made not in parliament or government, but within a narrow security elite aligned with financial, corporate, and clan-based interests. This fundamentally transforms the nature of the economy: competition is replaced by loyalty, private property becomes contingent, and law becomes a tool of operational expediency.

The international dimension of this transformation manifests in its most dangerous form. Intelligence agencies increasingly operate beyond their national borders, using mechanisms such as Interpol, extradition systems, financial monitoring, asset-freeze requests, and—more recently—digital channels including cryptocurrency OTC networks, cyber-operations, infrastructure attacks, and disinformation campaigns. This means that a citizen or entrepreneur can be targeted not only in their home country but also in third countries, undermining the fundamental principle of political asylum and threatening the global human rights protection system.

For Eurasia, this leads to the emergence of a new model of “security-driven political economy,” where control over capital and corporations is exercised not through markets and institutions but through coercive leverage. For the world, it results in rising transnational pressure, the politicization of Interpol, the criminalization of the digital economy, and the proliferation of networks where the state and organized crime operate as partners.

The ARGA Observatory report demonstrates that counteracting this process is only possible through the creation of systemic monitoring of intelligence operations, the development of international risk indices, the strengthening of legal protection mechanisms, and the establishment of a global regulatory framework capable of preventing abuses before they produce legal consequences. Without such reforms, the world risks not merely the entrenchment of authoritarian regimes but the emergence of a new form of global coercive economy in which security, property, and freedom of movement depend not on institutions but on the interests of security factions.

This is why researching and documenting hybrid intelligence agencies is not an academic task, but a strategic one. It is a necessary step for preserving international legal order, financial transparency, and the fundamental principles of human rights protection in the 21st century.

Sources

1. Niklas Nilsson, Mikael Weissmann, Björn Palmertz, Hybrid Threats and the Intelligence Community : Priming for a Volatile Age, 27 January 2025, https://www.tandfonline.com/doi/full/10.1080/08850607.2024.2435265#abstract.
2. TraCCC, Yulia Krylova, Spotlight on a Critical Threat : The Abuse and Exploitation of Red Notices, Interpol and the U.S. Judicial Process by Russia qnd Other Authoritarian States, Conference Report, 28 November 2018, https://traccc.gmu.edu/wp-content/uploads/2020/09/Final-Red-Notices-Conference-Report-Bright-Red.pdf.
3. Global Initiative Against Transnational Organized Crime, Annual Report 2024, https://globalinitiative.net/wp-content/uploads/2025/01/Annual-Report-2024.v2.pdf.
4. European Parliament, Misuse of Interpol's Red Notices and impact on human rights – recent developments, January 2019, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/603472/EXPO_STU%282019%29603472_EN.pdf.
5. CSCE, Countering Authoritarian Abuse of Interpol, October 29, 2024, https://www.csce.gov/briefings/countering-authoritarian-abuse-of-interpol/.
6. New Lines Institute, Ted R. Bromund, How the Abuse of Interpol Contributes to Transnational Repression, July 2025, https://newlinesinstitute.org/wp-content/uploads/20250715-Interpol-Abuse_policy-report-nlisap.pdf.
7. TraCCC, S4D Working Group, Kleptocracy & Illicit Finance Dialogue II : Investigating and Prosecuting Kleptocrats and Complicit Enablers, March 2023, https://traccc.gmu.edu/wp-content/uploads/2023/03/S4D-WG-Kleptocracy-and-Illicit-Finance-Dialogue-2023-FINAL-REPORT-2-MARCH-2023.pdf.
8. UNODC, Regional Programme for South-Eastern Europe 2024-2029, https://www.unodc.org/rosee/uploads/documents/Overview/RPSEE_24-29_-_Public_Version_v3.0.pdf.
9. Amnesty International, Report 2022/2023, The state of the world's human rights, 2023, https://www.amnesty.org/en/wp-content/uploads/2023/04/POL1056702023ENGLISH.pdf.
10. Parliamentary Assembly, Transnational repression as a growing threat to the rule of law and human rights, 5 June 2023, https://rm.coe.int/transnational-repression-as-a-growing-threat-to-the-rule-of-law-and-hu/1680ab5b07?utm_source=chatgpt.com.