Excerpt from InterAgency Journal 16-2
©2026 - Simons Center

Disclaimer: The articles published in the IAJ represent the opinions of the authors and do not reflect the official views of any United States government agency, the Department of War, the Department of the Army, the U.S. Army Command and General Staff College, the Command and General Staff College Foundation and Alumni Association, the Simons Center, or any other non-government, private, public or international organization.

The Shadow Nexus:

Sanctions Evasion, Human Trafficking, and Terrorist Financing as Emerging Intelligence Collection Challenges

by Nicholas Alexander

In the years following September 11, 2001, the United States (U.S.) built a formidable financial intelligence architecture. The USA PATRIOT Act expanded the Treasury Department's surveillance authorities. FinCEN's Suspicious Activity Report system gave analysts a window into the formal financial system. The Office of Foreign Assets Control (OFAC) developed increasingly sophisticated sanctions designation capabilities. The intelligence community's financial intelligence (FININT) function matured into one of the most powerful non-kinetic instruments in the national security toolkit. That architecture produced real results: it tracked al-Qaeda financing networks, disrupted Hezbollah's money laundering operations, and helped collapse ISIS's territorial financial base.

But the threat environment has evolved faster than the collection architecture designed to monitor it. Three phenomena—sanctions evasion, human trafficking, and terrorist financing—that have historically been treated as distinct analytical and operational problems have converged into a single integrated shadow economy. Sanctioned state and non-state actors exploit the same parallel financial infrastructure. Human trafficking networks generate revenue streams that flow through the same informal value transfer systems. Terrorist organizations access the same cryptocurrency mixing services, hawala networks, and maritime evasion routes. The shadow economy created by decades of comprehensive sanctions regimes has become the operating environment for all three.

This convergence creates a collection gap that is structural, not incidental. The intelligence community's collection frameworks were built around discrete threat categories, each with its own authorities, collection tools, and analytical pipelines. FININT monitors dollar-denominated financial

Nicholas Alexander is a master of arts candidate in statecraft and strategy at the Institute of World Politics in Washington, D.C., where his research focuses on financial intelligence, transnational organized crime, illicit finance, and gray-zone statecraft. His regional expertise encompasses the People's Republic of China, the Democratic People's Republic of Korea, and Venezuela. He has served as a graduate research assistant and intern mentor through IWP's National Security Internship Program and is currently developing doctoral research on economic statecraft and sanctions effectiveness. His work has appeared in institutional research venues addressing intelligence collection, political warfare, and financial coercion.

flows. SIGINT intercepts communications. Human intelligence (HUMINT) penetrates organizations. None of these frameworks was designed to monitor an integrated shadow economy in which sanctions evasion, trafficking revenue, and terrorist financing are not separate streams but different functions of the same network.

This article examines that gap through two case studies: ISIS as the paradigmatic non-state actor that pioneered adaptive terrorist financing in the shadow economy, and Venezuela as the state-sponsored model in which sanctions evasion infrastructure became a platform for terrorist support. It then identifies the specific collection gaps these cases reveal and proposes a framework for closing them—built around AI-enabled open source monitoring, maritime domain awareness fusion, cross-domain FININT and formalized private sector integration. These are not marginal improvements to existing collection. They are structural requirements for a collection architecture adequate to the convergence that has already occurred.

The Convergence Thesis: One Shadow Economy, Three Threat Streams

The analytical foundation of this article is that sanctions evasion, human trafficking, and terrorist financing are not separate phenomena that happen to overlap—they share infrastructure, personnel, and financial architecture in ways that make them functionally components of a single system. Understanding why requires examining what comprehensive sanctions regimes actually produce in the economies they target.

When the U.S. imposes comprehensive sanctions on a state or non-state actor, it does not eliminate that actor's economic activity—it redirects it outside the formal financial system. Transactions that would otherwise flow through dollar-denominated correspondent banking, Society for Worldwide Interbank Financial Telecommunication (SWIFT) messaging, and regulated financial institutions are pushed into alternative channels: cryptocurrency exchanges, hawala networks, barter arrangements, shell company structures, and maritime evasion routes. This is the shadow economy that sanctions create as a byproduct of their design. It is a feature, not a flaw; the intent is precisely to raise the cost of operating in that shadow space. But the shadow economy that emerges is not exclusive to the sanctioned actor. It is shared infrastructure, available to any network willing to operate outside the formal financial system.

... the U.S. uses its centrality in global financial networks as a coercive instrument...

Farrell and Newman's framework of weaponized interdependence captures half of this dynamic: the U.S. uses its centrality in global financial networks as a coercive instrument, making access to dollar-denominated finance conditional on political behavior.[1] What their framework does not fully address is the second-order effect: every actor excluded from those networks has a structural incentive to build and use the alternative infrastructure that emerges in their place. That alternative infrastructure—the shadow economy of sanctions evasion—is precisely the environment in which human trafficking networks and terrorist financing operations thrive.

Human trafficking networks require the same infrastructure as sanctions evasion: informal value transfer, shell company structures, cash-based transactions, and corruption of officials at border crossings and financial institutions. Terrorist financing requires the same infrastructure: cryptocurrency mixing, hawala, front companies, and transactions that never touch the dollar-denominated financial system that FININT was designed to monitor.

The convergence is not accidental; it is the logical outcome of multiple actors independently optimizing for survival in the same hostile regulatory environment. The result is a shared shadow economy in which these three threat streams are not parallel but interwoven, and in which collection frameworks designed to monitor each separately are structurally inadequate to monitor the system they have collectively produced.

Stripped of oil fields and taxable populations, ISIS turned to cryptocurrency fundraising campaigns...often disguised as humanitarian appeals for Muslims in conflict zones.

ISIS: The Non-State Model

ISIS represents the most thoroughly documented case of a non-state actor building, losing, and adapting a terrorist financing architecture in the shadow economy. Its evolution across three phases illuminates both the collection successes of the current architecture and the gaps that the post-territorial adaptation exposed.

At its peak territorial expansion in 2014-2016, ISIS developed a self-financing model of unprecedented sophistication. Controlling large swaths of Iraq and Syria, it extracted revenue through oil smuggling, taxation of occupied populations, kidnapping for ransom, and seizure of state assets. Estimates placed ISIS' peak revenue at $1 million to $3 million per day from oil sales alone.[2] This territorial financing model was visible as it left physical signatures that the collection architecture was well-equipped to detect. Operation Tidal Wave II, initiated in 2015, demonstrated what integrated collection could accomplish against a physically manifest financial target. The National Geospatial-Intelligence Agency's satellite imagery identified oil infrastructure, refinery locations, and tanker convoy routes. U.S. Central Command (CENTCOM) surveillance drones tracked distribution networks in real time. OFAC used banking records, intercepted communications, and customs filings to designate the brokers, intermediaries, and buyers who connected ISIS oil to global markets. The collection architecture performed its designed function: it found a physical target and enabled its disruption.

The collection gap emerged in Phase Two, when ISIS lost its territorial base and was forced to adapt its financing into the same shadow economy infrastructure that sanctions evasion networks use. Stripped of oil fields and taxable populations, ISIS turned to cryptocurrency fundraising campaigns on Telegram, Twitter, and encrypted chat platforms, often disguised as humanitarian appeals for Muslims in conflict zones. Supporters in Western countries and the Gulf transferred value through Bitcoin wallets that had no correspondent banking relationship, generated no Suspicious Activity Reports, and left no trail in the dollar-denominated financial system that FININT was built to monitor. The 2020 Department of Justice seizure of more than 300 cryptocurrency accounts linked to ISIS, al-Qaeda, and Hamas fundraising represented a significant operational success, but it also revealed the structural inadequacy of the existing architecture. The seizures were made possible not by IC collection but by blockchain forensics firms using transaction tracing methodology that the intelligence community was not itself running at scale.[3] Private sector capability had outpaced institutional collection.

Phase Three completed the convergence. As ISIS's territorial caliphate collapsed and its conventional financing dried up, the organization increasingly relied on human trafficking as both an ideological instrument and a revenue stream. The systematic enslavement of Yazidi women and girls was documented by the UN and human

rights organizations as both a war crime and a financing mechanism: captives were bought, sold, and traded through networks that used the same informal value transfer systems like cash, hawala, cryptocurrency, as ISIS's other financial operations.[4] The trafficking and terrorist financing networks were not parallel structures, they were the same network performing two functions simultaneously. Collection frameworks designed to monitor terrorist financing and human trafficking as separate phenomena had no analytical architecture for monitoring a network in which they were operationally unified.

The ISIS case yields a specific collection lesson: the current architecture is well-designed for visible, physically manifest financial targets operating in or near the formal financial system. It is structurally inadequate for adaptive networks that have migrated into the shadow economy, use cryptocurrency and informal value transfer to move funds, and integrate trafficking revenue into the same financial flows as terrorist financing. The gap is not one of effort or resources, but it is one of architectural design.

Venezuela: The State-Sponsored Model

Venezuela represents the state-actor version of the same convergence—a government that built a comprehensive sanctions evasion infrastructure as a matter of regime survival, and whose evasion architecture subsequently became a platform for supporting designated terrorist organizations. The Venezuela case adds a dimension that the ISIS case does not: the geopolitical complexity of patron substitution, in which Chinese and Russian support actively obscures financial flows from Western collection systems.

The sanctions evasion infrastructure that the Maduro government developed between 2017 and 2026 was sophisticated, multidimensional, and specifically designed to evade the collection architecture that U.S. financial intelligence relies upon. Shadow fleet operations deployed vessels under flags of convenience with obscured ownership structures and disabled Automatic Identification System transponders to transport Venezuelan crude to Asian markets outside the reach of U.S. secondary sanctions enforcement.[5] The geographic scale of these operations—loading in Venezuelan Caribbean ports, transiting the Atlantic, and delivering to Chinese refineries via the Cape of Good Hope or Suez Canal—created vast stretches of open ocean where automated information system (AIS) manipulation was difficult to detect and even harder to act upon. Oil-for-services barter arrangements with Cuba, which provided 15,000 to 25,000 security and intelligence personnel in exchange for preferential oil allocations, conducted transactions entirely outside dollar-denominated finance—invisible to FININT collection designed around SWIFT and correspondent banking.[6] The Maduro government's 2018 petro cryptocurrency experiment, though it ultimately failed as a functional currency, represented a deliberate attempt to create a sanctions-resistant financial instrument that operated outside the dollar-denominated infrastructure that U.S. collection monitored.

The sanctions evasion infrastructure that the Maduro government developed between 2017 and 2026 was sophisticated, multidimensional, and specifically designed to evade the collection architecture that U.S. financial intelligence relies upon.

The patron substitution dynamic added a geopolitical layer to the collection challenge that the ISIS case does not have. China's oil-for-loan arrangements with the Maduro government—

totaling more than $60 billion across multiple tranches—created financial flows that moved through Chinese state banking institutions largely opaque to Western intelligence collection.[7] Rosneft's role as a sanctions-evasion intermediary for Venezuelan oil sales moved transactions through Russian trading structures that partially circumvented U.S. secondary sanctions until the Treasury Department's 2020 designation of Rosneft Trading specifically targeted that conduit.[8] The collection challenge was not simply technical, it was political. Chinese and Russian patron substitution did not merely hide financial flows; it actively created alternative financial infrastructure specifically designed to be opaque to the collection systems that U.S. financial intelligence depends upon.

The shadow economy that sanctions evasion created was not compartmentalized from terrorist financing; it was the platform on which terrorist financing operated.

The terrorism financing dimension of the Venezuela case completes the convergence. The Maduro government's documented relationships with Hezbollah—including the presence of Hezbollah operatives in Venezuela, the use of Venezuelan diplomatic passports by Hezbollah-linked individuals, and the facilitation of Hezbollah financial operations through Venezuelan financial institutions—used the same sanctions evasion infrastructure that the regime had built for its own survival.[9] The shadow economy that sanctions evasion created was not compartmentalized from terrorist financing; it was the platform on which terrorist financing operated. Intelligence collection that monitored sanctions evasion and terrorist financing through separate analytical pipelines could not see the network that used both simultaneously.

The human trafficking dimension connects Venezuela to the cartel networks that operate the northbound corridor through which seven million Venezuelan migrants have fled since 2015.[10] The Sinaloa Federation and the Jalisco New Generation Cartel are the primary operators of that corridor, and the financial infrastructure they use to move trafficking proceeds overlaps directly with the cartel financial architecture—cryptocurrency mixing, hawala, cash courier networks—that also moves drug proceeds and, through Hezbollah's documented relationships with these cartels, terrorist financing.[11] The convergence that the ISIS case established at the level of a non-state actor in the Middle East is replicated in the Western Hemisphere at the intersection of Venezuelan sanctions evasion, cartel trafficking operations, and Hezbollah's financial networks. The shadow economy is the same. The collection gap is the same.

The Collection Gap: What Current Architecture Misses

The ISIS and Venezuela cases reveal four specific structural gaps in the current intelligence collection architecture, gaps that are not artifacts of inadequate effort but of architectural design that predates the convergence they must now address.

The first is the maritime domain gap. Shadow fleet operations exploit the combination of geographic scale and AIS manipulation to move sanctioned cargo through spaces where detection is possible but interdiction is not. U.S. intelligence services maintained extensive satellite and signals surveillance of Venezuelan shadow fleet operations throughout the sanctions period, but monitoring and interdiction are different capabilities.[12] The legal and diplomatic constraints on boarding vessels in international waters, combined with the volume of maritime traffic and the sophistication of ownership-obscuring structures, meant that shadow fleet operations functioned as a durable evasion mechanism for nearly a decade. The collection

data existed; the analytical and legal architecture to act on it in real time did not. Closing this gap requires not more collection but integrated fusion of commercial satellite imagery, AIS data, Lloyd's shipping intelligence, and SIGINT into a unified maritime tracking architecture designed specifically for shadow economy detection—one that can identify AIS manipulation signatures, flag ownership structure anomalies, and connect vessel movements to financial transactions in near-real time.

The second is the cryptocurrency and decentralized finance gap. ISIS's post-territorial adaptation and Venezuelan petro experiment both demonstrate that terrorist and sanctions-evasion networks have adopted cryptocurrency infrastructure faster than the regulatory and collection frameworks designed to monitor it. The 2020 DOJ cryptocurrency seizures were a significant success, but they were made possible by blockchain forensics firms whose transaction tracing methodology the intelligence community was not running at institutional scale. Decentralized finance platforms, cryptocurrency mixing services, and peer-to-peer transfer protocols create financial flows that have no correspondent banking relationship, generate no regulatory reporting, and are architecturally designed to resist attribution. AI-enabled blockchain analytics—monitoring wallet clustering, transaction graph analysis, and exchange on-ramp and off-ramp patterns—represent the collection methodology adequate to this environment. The technology exists in the private sector. The institutional architecture to deploy it at intelligence scale does not yet exist.[13]

The third is the informal value transfer gap. Barter arrangements, hawala networks, and cash courier systems move value entirely outside the dollar-denominated financial infrastructure that FININT was designed to monitor. The Venezuelan-Cuban security-for-oil barter relationship, Hezbollah's hawala networks documented in the Lebanese Canadian Bank case, and cartel cash courier operations in the Western Hemisphere all exploit the same structural blind spot: transactions that never touch the formal financial system are invisible to collection frameworks designed around that system. Closing this gap requires HUMINT collection specifically targeted at the nodes where informal value transfer intersects with the formal economy—money exchange houses, gold dealers, real estate transactions, and the import-export businesses that provide cover for informal value transfer—combined with OSINT monitoring of the social and commercial networks in which these nodes operate.[14]

Decentralized finance platforms, cryptocurrency mixing services, and peer-to-peer transfer protocols create financial flows that have no correspondent banking relationship, generate no regulatory reporting, and are architecturally designed to resist attribution.

The fourth and most fundamental is the cross-domain fusion gap. Sanctions evasion, human trafficking, and terrorist financing are monitored by different agencies with different authorities, different collection tools, and no unified analytical framework. Treasury's OFAC monitors sanctions violations. Homeland Security Investigations monitors trafficking. The CIA and NSA monitor terrorist financing. Each collects within its authorities and analytical mission. None has the mandate or architecture to monitor the integrated shadow economy in which all three operate as functions of the same network. The data exists in separate collection pipelines; the synthesis that would reveal the convergence does not. A dedicated cross-domain analytical cell—drawing on FININT, SIGINT, HUMINT, and OSINT simultaneously and

operating with the authority to access all four collection streams—is the structural requirement for closing this gap.[15]

Closing the Gap: Collection Approaches for a Converged Threat

Closing the collection gap that the ISIS and Venezuela cases reveal requires not more collection of the same kind but architectural changes to how collection is organized, fused, and supplemented by private sector capability. Four approaches address the specific gaps identified above. First, AI-enabled open source and social media monitoring. Trafficking networks and sanctions evasion operations generate open source signatures that systematic collection can exploit. Vessel tracking data from commercial AIS providers, social media recruitment activity by trafficking networks, cryptocurrency wallet activity on public blockchains, and shipping manifests filed with port authorities are all publicly available data streams that AI-enabled pattern recognition can monitor at scale. The analytical challenge is not acquiring the data but building the machine learning architecture to identify operationally relevant patterns within it. Investing in AI-enabled OSINT collection specifically targeted at shadow economy signatures, rather than general-purpose open source monitoring, addresses the convergence directly and at relatively low collection cost.[16]

Closing the collection gap that the ISIS and Venezuela cases reveal requires not more collection of the same kind but architectural changes...

Second, maritime domain awareness fusion. The shadow fleet gap requires integrating commercial satellite imagery providers, AIS data aggregators, Lloyd's shipping intelligence, and Port State Control inspection records into a unified analytical platform designed for shadow economy vessel detection. Several commercial providers, including Windward, Pole Star, and similar maritime intelligence firms, already offer AIS anomaly detection and vessel ownership analysis at commercial scale. A dedicated maritime domain awareness fusion cell, drawing on these commercial capabilities alongside classified collection, would provide the near-real-time detection architecture that the Venezuela shadow fleet demonstrated is currently absent. The technology exists; the institutional architecture to deploy it within the intelligence collection framework does not.[17]

Third, cross-domain financial intelligence fusion. A dedicated analytical cell that synthesizes FININT, SIGINT, HUMINT, and OSINT across the three threat streams simultaneously rather than tracking them in separate collection stovepipes. This cell would require statutory authority to access collection from Treasury, the IC, and law enforcement simultaneously, and an analytical mandate specifically defined around the convergence rather than around any single threat category. The FinCEN Exchange model, which enables voluntary intelligence sharing between government and financial institutions, provides a partial template that could be extended to include trafficking intelligence and IC collection under appropriate legal authorities.[18]

Fourth, formalized private sector integration. The 2020 DOJ cryptocurrency seizures demonstrated that blockchain forensics firms are performing collection and analysis that the IC is not running at institutional scale. Shipping intelligence companies, financial analytics platforms, and OSINT aggregators are similarly ahead of institutional collection in specific domains. Formalizing these relationships through cleared contractor arrangements, structured intelligence sharing agreements, or acquisition of commercial capability closes the gap faster than building internal capability from

scratch. The private sector's agility in adopting new analytical technologies is itself a collection asset; the institutional challenge is integrating that agility into the oversight and legal framework that classified collection requires.[19]

These four approaches are not independent recommendations, they are components of a unified collection architecture designed around the convergence. AI-enabled OSINT provides the broad monitoring layer. Maritime domain awareness fusion addresses the geographic evasion gap. Cross-domain financial intelligence fusion provides the analytical synthesis. Private sector integration supplies the technological agility. Together they constitute a collection architecture adequate to a shadow economy that the current framework was not designed to monitor.

Conclusion

The intelligence community's collection architecture was built for a threat environment in which discrete actors used identifiable financial channels to fund discrete operations. That environment has been superseded. The convergence of sanctions evasion infrastructure, human trafficking networks, and terrorist financing mechanisms into a single integrated shadow economy represents an emerging collection challenge that stove-piped, domain-specific frameworks cannot address.

ISIS demonstrated that a non-state actor could build a self-financing territorial empire, lose it, and adapt its financing into a shadow economy that outpaced the collection architecture designed to monitor it—integrating cryptocurrency fundraising, informal value transfer, and human trafficking revenue into financial flows that traditional FININT was structurally unable to see. Venezuela demonstrated that a state actor could build a comprehensive sanctions evasion infrastructure that subsequently became a platform for terrorist support, using the same shadow economy nodes, shadow fleet operations, barter arrangements, cryptocurrency experiments, that cartel networks use to move trafficking proceeds and drug revenues through the same Western Hemisphere corridor.

The collection gaps these cases reveal are not failures of effort or resources. They are architectural—products of a collection framework designed around discrete threat categories that no longer map onto a threat environment defined by convergence. Closing them requires the maritime domain awareness fusion that shadow fleet operations demand, the AI-enabled blockchain analytics that cryptocurrency evasion requires, the cross-domain financial intelligence synthesis that the integrated shadow economy makes necessary, and the private sector integration that the pace of technological adaptation in the shadow economy makes urgent.

The shadow economy that has emerged at the intersection of sanctions evasion, human trafficking, and terrorist financing is not a future threat. It is the operating environment of adversaries who are already inside it. Building the collection architecture to monitor it is not an optional enhancement to current capability; it is a structural requirement for the intelligence mission to remain adequate to the threat it is designed to address.[20] ***IAJ***

Notes

1 Henry Farrell and Abraham L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion," International Security 44, no. 1 (2019), 42-79.

2 David S. Cohen, "Attacking ISIS's Financial Foundation," U.S. Department of the Treasury, October 23, 2014, https://home.treasury.gov/news/press-releases/jl2672.

3 U.S. Department of Justice, "Global Disruption of Three Terror Finance Cyber-Enabled Campaigns," August 13, 2020, https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns.

4 United Nations Human Rights Council, Report of the Independent International Commission of Inquiry on the Syrian Arab Republic (Geneva: UN Human Rights Council, 2016).

5 Nicholas Alexander, "Pipelines and Patrons: How Venezuela's Geographic and Resource Endowments Enabled Sanctions Evasion Through Chinese and Russian Patronage," IWP 634, Geography and Strategy (Institute of World Politics, 2026).

6 Javier Corrales and Michael Penfold, Dragon in the Tropics: Hugo Chávez and the Political Economy of Revolution in Venezuela (Washington, D.C.: Brookings Institution Press, 2011), 142-148.

7 Kevin P. Gallagher and Margaret Myers, China-Latin America Finance Database (Washington, D.C., Inter-American Dialogue, 2020).

8 James Henderson and Tatiana Mitrova, "Implications of the Global Energy Transition on Russia," Energy Research & Social Science, 64 (2020), 1014-1044.

9 Matthew Levitt, Hezbollah: The Global Footprint of Lebanon's Party of God (Washington, D.C., Georgetown University Press, 2013), 87-92.

10 United Nations Human Rights Council, Report of the Special Rapporteur on the Negative Impact of Unilateral Coercive Measures on the Enjoyment of Human Rights: Mission to Venezuela (Geneva: UN Human Rights Council, 2020).

11 Levitt, Hezbollah, 201, 207.

12 Mark M. Lowenthal, Intelligence: From Secrets to Policy, 7th ed. (Washington, D.C., CQ Press, 2019), 134–138.

13 Juan C. Zarate, Treasury's War: The Unleashing of a New Era of Financial Warfare (New York, PublicAffairs, 2013), 318-324.

14 U.S. Department of Justice, "Global Disruption," supra note 3.

15 Corrales and Penfold, Dragon in the Tropics, 156-162.

16 Farrell and Newman, "Weaponized Interdependence," 58-62.

17 Levitt, Hezbollah, 214-219.

18 Nicholas Alexander, "Economic Warfare, Sanctions, and Strategic Outcomes in Venezuela," IWP 732, International Trade and Globalization (Institute of World Politics, 2026).

19 Zarate, Treasury's War, 302-308.

20 Lowenthal, Intelligence: From Secrets to Policy, 198-202.