اللجنة الدائمة المعنية
بتطبيق قرارات مجلس الأمن
الصادرة وفق الفصل السابع

وزارة الخارجية
MINISTRY OF FOREIGN AFFAIRS

PROLIFERATION FINANCING TYPOLOGIES AND RED FLAG INDICATORS

Permanent Committee for the Implementation of Security Council Resolutions under Chapter VII of the United Nations Charter

Ministry of Foreign Affairs, Kingdom of Saudi Arabia

Contents

Executive Summary

This paper presents a consolidated set of proliferation financing (PF) typologies and related red flag indicators, developed to support government authorities, financial institutions (FIs), and designated non-financial businesses and professions (DNFBPs) in identifying, assessing, and mitigating the risk of PF activities, particularly those linked to the Democratic People's Republic of Korea (DPRK). The typologies are grounded in authoritative, verifiable sources, including multiple reports of the United Nations Panel of Experts established pursuant to Security Council resolution 1874 (2009), as well as confirmed open-source investigations, enforcement actions, and trade data analyses.

The primary objective is to provide practitioners with a clear, operational understanding of how PF schemes are structured, the behaviors that enable them, and the transactional or logistical anomalies that can trigger suspicion. While the typologies focus on DPRK activity, many patterns have broader applicability to other sanctions contexts, including Iran and non-state actors engaged in proliferation-related procurement or financing.

Core Findings

The typologies illustrate that DPRK PF activity remains highly adaptive, operating across multiple sectors and jurisdictions despite the comprehensive nature of the UN's targeted financial sanctions (TFS) regime. Techniques range from maritime deception (e.g., ship-to-ship transfers, AIS manipulation) and front-company networks in permissive jurisdictions, to the misuse of humanitarian channels, trade misinvoicing, and phantom shipping. Several typologies reveal points of convergence between illicit procurement and other criminal economies, including bulk cash smuggling, wildlife trafficking, and cyber-enabled theft of virtual assets.

The analysis also highlights sector-specific vulnerabilities. For example:

- **Maritime transport** remains susceptible to deceptive practices such as identity laundering of vessels, falsified shipping documentation, and concealment of DPRK-linked cargo through flag-hopping.
- **Financial institutions** face persistent risk from layered transactions routed through opaque corporate structures or correspondent banks in high-risk jurisdictions.
- **DNFBPs -** including real estate agents, lawyers, accountants, and dealers in precious metals and stones, are exposed when providing services to newly formed or recently re-domiciled entities lacking legitimate commercial footprints.

Emerging Technology Risks – AI-Enabled Sanctions Evasion

A critical emerging threat identified in this study is the integration of artificial intelligence (AI) into sanctions evasion strategies. While many of the typologies rely on long-established techniques, AI is increasingly deployed to enhance deception, obscure beneficial ownership, and automate illicit tradecraft. Recent analysis by the UN Panel of Experts, blockchain analytics firms such as Chainalysis, and think tanks including the Royal United Services Institute (RUSI) indicate that DPRK-linked cyber actors are experimenting with, or operationalizing, AI capabilities in the following ways:

- **Synthetic Identities and Deepfakes:** AI-generated personas, complete with fabricated facial images and falsified identification documents, are used to pass remote customer onboarding checks and secure freelance IT contracts. This enables DPRK nationals to obtain income in foreign jurisdictions while concealing their nationality.
- **Automated Evasion in Virtual Asset Transactions**: AI-assisted transaction patterning can break expected heuristics in blockchain analytics, frustrating tracing of illicit flows from virtual asset hacks to cash-out points.
- **Trade Document Fabrication:** Large Language Models (LLMs) and AI-based design tools can generate convincing invoices, bills of lading, and end-user certificates that evade superficial scrutiny by customs and banks.
- **Enhanced Cyber Intrusion:** AI tools can accelerate reconnaissance of target systems and automate exploitation, increasing the scale and precision of cyber-enabled theft used to finance proliferation programs.

These developments do not replace traditional evasion techniques; rather, they compound existing red flags and increase detection difficulty. The inclusion of AI-specific red flag indicators in this paper reflects the need for both public and private sectors to adapt monitoring systems and investigative approaches accordingly.

Red Flag Indicators: Practical Application

Each typology in this report includes tailored red flag indicators directly linked to documented case studies. These indicators are designed to be actionable, allowing compliance officers, analysts, and investigators to distinguish between high-risk anomalies and ordinary commercial variance. They encompass behavioural, transactional, documentary, and sector-specific signals, with an emphasis on patterns that persist across multiple cases.

The final chapter consolidates cross-cutting residual indicators and incorporates new AI-focused red flags. These highlight the intersection between emerging technologies, traditional sanctions evasion tradecraft, and the need for updated compliance controls.

Policy and Compliance Implications

The typologies underscore that combating PF, particularly DPRK-related, requires a whole-of-system response, combining:

- Real-time intelligence sharing between governments, FIs, DNFBPs, and logistics sectors.
- Rigorous due diligence on high-risk goods, end-users, and trade corridors.
- Investment in AI-enabled detection to match the sophistication of evasion techniques.
- Strengthened capacity among both public and private sectors to recognise and act upon atypical patterns before goods or funds reach sanctioned programs.

Rather than offering a static checklist, this paper presents a dynamic threat picture that integrates historical lessons with forward-looking risks. The typologies, case studies, and red flag indicators are intended to equip operational actors with the situational awareness required to detect PF activity early, escalate appropriately, and disrupt the flow of funds, goods, or services to sanctioned WMD programs. The integration of AI into the PF toolkit is observable and expanding, heightening the urgency for proactive adaptation of compliance, enforcement, and policy measures.

Introduction

1. Proliferation financing (PF) refers to the act of providing funds or financial services used for the development, acquisition, or transfer of weapons of mass destruction (WMD), their means of delivery, and related technologies in contravention of national or international obligations. In practice, PF often involves the deliberate or inadvertent movement of value that enables sanctioned states or entities to circumvent export controls, United Nations Security Council measures, or international embargoes. This includes the procurement of dual-use goods, concealment of end-users, deceptive shipping, and increasingly, the misuse of virtual assets and corporate structures as well as other Targeted Financial Sanctions (TFS) evasion techniques.

2. While long considered a niche issue within the broader financial crime landscape, PF has re-emerged as a critical and evolving global threat. States such as the Democratic People's Republic of Korea (DPRK) continue to finance nuclear and ballistic missile programs using sophisticated evasion tactics, while entities linked to Iran, Russia, and others exploit global trade and finance systems to acquire sensitive materials. The use of cyber-enabled theft, digital assets, and third-country intermediaries has expanded PF risk into sectors far beyond traditional banking, including real estate, shipping, insurance, legal services, and e-commerce. The Financial Action Task Force (FATF) has noted that PF threats are not only persistent but increasingly innovative[1] with significant vulnerabilities in many jurisdictions' implementation of PF-related controls under FATF Immediate Outcome 11 (IO11). PF actors deliberately target blind spots in sanctions enforcement and due diligence practices across both the public and private sectors.

3. The objective of this paper is to help financial institutions, Designated Non-Financial Businesses and Professions (DNFBPs), and relevant public authorities recognize and respond to these risks. Drawing from global and regional developments between 2021 and 2025, the paper presents a series of practitioner-focused real-world typologies that illustrate how PF is carried out in practice: from front companies and trade deception to the laundering of stolen crypto assets. Each typology is accompanied by targeted red-flag indicators observed in the case, helping readers understand not just how PF schemes work, but also how they can be detected and operationalized within risk assessment, onboarding, and monitoring workflows.

4. In addition to the typology-based indicators, a dedicated section consolidates standalone red flags drawn from recent advisories, typology reports, and regulatory reviews that do not fit neatly into the presented cases but remain operationally relevant across sectors and channels.

[1] Complex-PF-Sanctions-Evasions-Schemes.pdf.coredownload.inline.pdf

5. This paper is not intended as a legal or regulatory interpretation. Instead, it is designed to serve as a practical tool for frontline detection, awareness-raising, and institutional risk assessment, particularly within the context of Saudi Arabia’s national efforts to counter proliferation financing in line with FATF Recommendation 7 and Immediate Outcome 11. It also supports sectoral outreach, supervisory engagement, and training initiatives aimed at strengthening national implementation.

Typologies

6. The following typologies and case studies illustrate how proliferation financing and targeted financial sanctions (TFS) evasion are operationalized in practice, with a focus on activities linked to the Democratic People’s Republic of Korea (DPRK). Each typology contains two real-world or publicly reported case studies, accompanied by red flag indicators tailored to the specific evasion techniques observed. The analysis covers conduct prohibited under United Nations Security Council (UNSC) Resolutions 1718 (2006) and its successors, including but not limited to Resolutions 1874, 2087, 2094, 2270, 2321, 2356, and 2397. It also reflects activity prohibited under UNSCR 1540 (2004) in relation to non-state actors, where relevant. The patterns reflected in these cases are intended to support national efforts to identify, prevent, and disrupt financing of proliferation of weapons of mass destruction.

7. The typologies span a wide range of sectors, including finance, logistics, maritime services, virtual assets, and diplomatic channels, and are relevant to financial institutions, designated non-financial businesses and professions (DNFBPs), customs authorities, and competent authorities involved in TFS implementation. The case studies are drawn from incidents occurring between 2003 and 2025, with particular focus on methods that remain relevant to current risk environments. Older cases are included only where they illustrate techniques that remain in active use. These cases illustrate how proliferation financing risk is often obscured behind layers of misdirection, front companies, cyber obfuscation, and exploitation of legal or procedural loopholes.

8. The typologies and red flag indicators presented in this paper are compiled from a range of authoritative sources, including United Nations Panel of Experts reports, FATF typology analyses, academic research, and official national risk assessments. These sources provide a strong evidentiary basis for understanding DPRK-linked evasion activity and are consistent with FATF's typological expectations under Recommendation 7 and Immediate Outcome 11.

Key Reference Sources:

International Bodies and National Authorities

- FATF (2008). *Typologies Report on Proliferation Financing*
- FATF (2021–2024). *Mutual Evaluation Reports and Follow-Up Reports (Various Jurisdictions)*
- United States (2022). *National Proliferation Financing Risk Assessment*
- Asia/Pacific Group on Money Laundering (2024). *Typologies Report on Proliferation Financing*
- European Commission (2023). *Study on Proliferation Financing Risks in the EU Financial System*

Expert Bodies and Independent Research

- UN Security Council Panel of Experts Reports: *S/2016/157*, *S/2017/742*, *S/2018/171*, *S/2023/449*, *S/2024/234*
- RUSI (2018). *Underwriting Proliferation: Sanctions Evasion, Proliferation Finance and the Insurance Industry*
- RUSI (2024). *Detect, Disrupt and Deny: A Guide to Countering Proliferation Financing*
- Additional media, satellite imagery, and open-source investigations (2021–2025)

Typology 1 – Use of Front Companies and Third-Country Intermediaries

9. DPRK-linked proliferation networks frequently rely on front companies and foreign intermediaries to disguise the origin, destination, or purpose of transactions. These actors exploit permissive corporate registration regimes and sympathetic or complicit business environments, particularly in China, Southeast Asia, and parts of the Middle East, to create layers of obfuscation between themselves and the ultimate prohibited activity. The front companies often appear to be legitimate trading, logistics, or electronics firms, masking their underlying ties to DPRK entities subject to UN sanctions. These intermediaries handle procurement, financial transactions, and shipping arrangements on behalf of sanctioned persons or agencies. In many cases, such intermediaries operate for extended periods before detection, benefiting from weak beneficial ownership disclosure and limited cross-border information sharing.

~~10.~~ By routing activity through third-country actors, DPRK entities gain indirect access to the international financial system, evade scrutiny by counterparties, and shield the end-use of sensitive or controlled goods. This method also reduces the visibility of proliferation financing risk to frontline actors such as banks, logistics firms, or DNFBPs, who may be unaware of the DPRK nexus unless conducting enhanced due diligence across complex supply chains. These arrangements often involve multiple jurisdictions, each of which may see only a fragment of the overall transaction chain, further complicating detection.

Case Study 1: Singa Supply Chain Pte Ltd and Southeast Asian Intermediation

A Singapore-based company, Singa Supply Chain Pte Ltd, was identified in a UN Panel of Experts report for its role in facilitating prohibited DPRK trade. Singa Supply Chain operated as a logistics and procurement intermediary, receiving and forwarding shipments of industrial equipment, electronics, and chemicals to sanctioned country end-users. To avoid detection, the company masked the final destination by listing other Southeast Asian countries, such as Thailand or Malaysia, as end recipients, before rerouting the goods to Pyongyang via overland transport through neighboring states or through third-party shipping agents.

In multiple instances, invoices were altered to conceal the true origin or technical specifications of the items. The company also employed falsified end-user declarations and maintained a network of counterparties who knowingly or unknowingly assisted in the evasion chain. Though based in a jurisdiction with formal export controls, Singa Supply Chain exploited gaps in enforcement and weak due diligence standards among freight forwarders and customs brokers. The firm’s directors maintained ties with DPRK nationals operating in the region under business cover.

While authorities eventually shut down the company, no formal prosecution followed. Nonetheless, the case underscored the challenges of identifying PF activity when intermediaries operate under legal facades in countries with otherwise legitimate trading profiles. This case illustrates how jurisdictional credibility can be leveraged to mask illicit activity, particularly when enforcement and awareness gaps exist in private sector gatekeepers.

Red Flag Indicators for Case Study 1:

Indicator 1: Declared shipping destinations shift post-clearance or follow indirect, illogical or circuitous trade routes inconsistent with standard commercial practice.

Indicator 2: End-user declarations are vague, unverifiable, or contradict other documentation (e.g., invoices, packing lists, or contract terms).

Indicator 3: The exporting entity is based in a jurisdiction with formal export controls but weak enforcement and limited PF awareness among freight forwarders or customs agents, or where customs declarations are routinely accepted without verification.

Indicator 4: Company directors, shareholders, or known affiliates have unexplained ties to DPRK nationals or businesses operating under commercial cover in the region.

Typology 2 - Obscuring Beneficial Ownership through Layered Corporate Structures

11. The sanctioned country -linked networks frequently conceal their involvement in companies through complex, multi-layered ownership structures to evade UN sanctions and gain indirect access to the international financial system. These structures often include nominee directors, shell companies in secrecy jurisdictions, and entities registered under the names of foreign nationals. The objective is to obscure the true beneficial owner or controlling party, typically a sanctioned country state organ or a sanctioned individual acting covertly, thereby frustrating screening and beneficial ownership verification processes.

12. These schemes exploit disparities in corporate transparency requirements across jurisdictions, as well as the limited capacity of banks, company registrars, and gatekeepers (e.g., legal or corporate service providers) to verify actual control. Once established, such companies are used to open bank accounts, sign trade contracts, receive international payments, and procure goods, including dual-use items relevant to WMD programs. The tactic is also used to reinstate sanctioned operations under new identities after prior exposure, sometimes with minimal changes to corporate names, sector profiles, or associated personnel.

13. The deliberate layering of ownership frustrates due diligence and allows the sanctioned country actors to present themselves as unrelated commercial entities in neutral jurisdictions, complicating detection by FIs and DNFBPs unless enhanced due diligence (EDD) is conducted across ownership chains and geographic links.

Case Study 2: Foreign Nationals Used to Front-Owned Companies

In a 2023 UN investigation, the sanctioned country nationals employed a network of foreign intermediaries, including Southeast Asian and African nationals, to incorporate companies on their behalf. One such firm, registered in a Gulf jurisdiction, was legally owned by a South Asian national with no commercial connection to the business. Control was exercised remotely by the sanctioned country operatives using encrypted messaging apps and proxy accounts.

The firm, presented as an electronics wholesaler, secured contracts with international suppliers to acquire dual-use telecommunications equipment. Payments were processed through accounts registered to the frontman, but operational instructions were issued by the sanctioned country actors behind the scenes.

This approach helped the network bypass beneficial ownership checks and gave the nominal owner plausible deniability, as he claimed ignorance when interviewed by authorities. The case illustrates the sanctioned country use of geographic, regulatory, and technological gaps to mask true control, and demonstrates the operational reliance on trusted intermediaries willing to act as legal fronts despite minimal business knowledge or involvement.

Red Flag Indicators for Case Study 2:

Indicator 1: The company’s beneficial owner or director resides abroad and lacks demonstrable experience in the firm’s line of business or appears to be acting as a nominee for multiple unrelated companies.

Indicator 2: Operational instructions (e.g., payments, shipping) come from individuals not listed as directors, shareholders, or authorized signatories.

Indicator 3: Core business functions are coordinated via encrypted apps (e.g., Signal, Telegram) with no supporting email or formal records.

Indicator 4: The listed beneficial owner is unable to answer basic questions about the company’s operations, contracts, or counterparties.

Typology 3 - Abuse of Remote Work and False Employment

14. The sanctioned country linked actors have developed a sophisticated scheme to generate foreign currency by embedding IT professionals within legitimate companies around the world. These operatives are trained in software development, cybersecurity,

blockchain, and web infrastructure, and pose as freelance or full-time remote workers using false or borrowed identities. They gain access to sensitive systems, earn significant salaries, and remit their earnings to the sanctioned country regime, directly undermining international sanctions and creating potential cyber intrusion vectors for the host companies.

15. These workers operate via freelance platforms and remote job networks, often using third parties to pass identity verification checks. Salaries are routed through intermediaries, crypto wallets, or informal channels such as cash couriers and Hawala networks. In addition to financing sanctions violations, the tactic introduces serious insider risks, including unauthorized access to source code, system credentials, and customer data and can facilitate further the sanctioned country cyber operations once access is obtained.

Case Study 3: Arizona-Based Laptop Farm Supporting IT Workers

A U.S. woman residing in Arizona facilitated employment for dozens of the sanctioned country IT workers by operating a covert infrastructure of internet-connected laptops, mobile hotspots, and online freelancer accounts. Her residence served as a physical proxy hub to simulate U.S.-based employment.

The DPRK operatives accessed the laptops remotely and used them to apply for software development and consulting positions with companies worldwide. Their identities were concealed using spoofed IP addresses, falsified documents, and third parties who posed as the job applicants during video calls and KYC checks.

The woman received a share of the profits and helped launder the proceeds through a mixture of bank accounts, crypto wallets, and overseas intermediaries. Some funds were withdrawn in cash and handed to couriers. The operation generated more than USD 800,000 in revenue for the sanctioned country linked workers.

Despite red flags such as inconsistent documentation, suspicious login activity, and communication delays, most employers failed to identify the scheme, largely due to overreliance on automated onboarding systems and insufficient manual verification of high-risk applicants.

Red Flag Indicators for Case Study 3:

Indicator 1: Freelancers evade live video verification or delegate it to third parties posing as the account holder.

Indicator 2: Multiple freelancer accounts are accessed from the same device, IP address, or browser fingerprint across unrelated profiles.

Indicator 3: Earnings are routed to bank or crypto accounts not registered to the freelancer, or withdrawn in forms inconsistent with the account's profile (e.g., frequent cash withdrawals, third-party transfers) without credible business explanation.

Typology 4 - Procurement of Dual-Use Goods via Trade-Based Evasion

16. The sanctioned country linked procurement networks routinely exploit global supply chains to acquire dual-use goods: items with both civilian and military applications, including those relevant to WMD programs. These schemes often rely on falsified trade documentation, counterfeit or misleading end-user certificates, ambiguous product descriptions, and mis declared shipping routes to circumvent export controls. Transactions are typically executed through front companies based in free trade zones or jurisdictions with weak enforcement, and are sometimes disguised within bulk commercial orders to avoid scrutiny of individual items, masking the identities of end-users and final destinations.

17. By targeting manufacturers and distributors in compliant jurisdictions, these networks exploit legitimate commerce while creating plausible deniability between exporters and ultimate recipients. Sectors at heightened risk include industrial equipment manufacturers, logistics firms, customs brokers, inspection companies, and export credit agencies. The goods sought range from machine tools and specialty metals to laboratory equipment, chemical precursors, and electronic components, many of which appear on control lists maintained under UNSCR 1718, or the Wassenaar Arrangement.

Case Study 4: Belgian Laboratory Equipment Misuse

In 2022, Belgian export control authorities intercepted a shipment of laboratory-grade vacuum pumps and precision filtration components *en route* to Jordan. These items, marketed for use in university science labs, are classified as dual-use due to potential applications in semiconductor fabrication, uranium enrichment, and chemical weapons production.

The declared end-user was a regional university's engineering department. However, export officials flagged several irregularities during due diligence: the listed contact number was inactive, the recipient email domain matched a commercial freight forwarding firm, and the academic institution's street address was linked to a known virtual office provider.

Further investigation revealed that the ordering entity had previously been associated with a sanctioned procurement agent operating on behalf of the sanctioned country. This agent had used education- and healthcare-sector covers to source sensitive items under humanitarian or academic pretenses. The procurement attempts also exploited a "low-value shipment" exemption threshold in local customs procedures, allowing the consignment to initially pass without license checks.

Although the Belgian authorities ultimately blocked the shipment, the case underscores how low-volume, high-value dual-use goods remain vulnerable to diversion - even when originating from jurisdictions with strong controls and active enforcement.

Red Flag Indicators for Case Study 4:

Indicator 1: Contact details for the stated end-user (e.g., email, phone, or physical address) are inactive, unverifiable, or resolve to unrelated commercial service providers such as freight forwarders or virtual office operators.

Indicator 2: Academic credentials, institutional affiliations, or research activities cited in end-use declarations cannot be independently verified through public or official sources.

Indicator 3: Orders for dual-use laboratory or scientific equipment are justified under vague educational or academic covers and lack supporting institutional documentation (e.g., purchase orders, grant approvals, or research project descriptions).

Indicator 4: The ordering party, or associated intermediaries, have known or prior affiliations with UN-designated entities under UNSCR 1718 (2006) or subsequent resolutions, including historical procurement agents or front companies linked to the sanctioned country programs.

Typology 5 - Maritime Sanctions Evasion and Deceptive Shipping Practices

18. Despite concerted international monitoring efforts, the maritime sector remains a critical vector for the sanctioned country to evade UN sanctions. The typology encompasses a range of deceptive practices, including disabling Automatic Identification System (AIS) transponders, conducting illicit ship-to-ship (STS) transfers, reflagging under permissive registries, and concealing ownership through shell companies. These techniques enable sanctioned entities to move commodities such as petroleum, coal, and arms with reduced risk of timely detection or interdiction.

19. Maritime evasion tactics are highly coordinated and deliberately transnational. Reflagged vessels routinely operate in the East China Sea, Gulf of Tonkin, and Yellow Sea - regions where surveillance is limited and jurisdictional enforcement is fragmented. Deceptive cargo documentation, forged bills of lading, and intermediary-owned ships further obscure the sanctioned country connection to the transaction chain. These tactics pose serious risks to flag registries, marine insurers, financial institutions, port authorities, customs officials, and vessel tracking providers.

Case Study 5: Ocean Maritime Management (OMM) Fleet Activity (2022–2024)

Between 2022 and 2024, multiple vessels operated by Ocean Maritime Management Company Ltd. continued to engage in prohibited maritime activity despite their designation under UN sanctions. Several OMM-linked ships carried out STS transfers of petroleum in international waters, particularly in the East China Sea and adjacent high-risk maritime corridors, while AIS transponders were disabled for extended periods. These transfers often involved vessels flying flags of convenience registered in jurisdictions with minimal maritime compliance enforcement.

After conducting STS transfers, vessels frequently re-emerged on AIS with different names, altered IMO numbers, or changes in flag state. These identity changes obscured their ownership lineage and frustrated due diligence efforts by marine insurers, port authorities, and financial institutions. Investigations traced many of the vessels to shell companies based in Hong Kong and the British Virgin Islands, with nominee directors and opaque beneficial ownership structures.

Further complicating detection, bunkering payments and insurance premiums were often routed through third-party entities unrelated to the registered owners. These payment chains were deliberately disconnected from the ships' actual operators and allowed designated vessels to continue accessing fuel, insurance, and port services across the region.

Red Flag Indicators for Case Study 5:

Indicator 1: Extended AIS disablement near known STS transfer zones, followed by reactivation under a changed vessel identity (e.g., altered name, IMO number, or flag state).

Indicator 2: STS transfers of petroleum or other restricted cargo occur in international waters without clear commercial rationale, public scheduling, or identified end-user.

Indicator 3: Vessel ownership or control is linked to shell companies recently incorporated in jurisdictions lacking effective beneficial ownership transparency.

Indicator 4: Payments for maritime services (e.g., insurance premiums, bunkering, port fees) are made by third parties with no verifiable link to the registered owner or operator.

Indicator 5: The vessel, its operator, or associated entities are UN-designated and have a documented history of sanctions evasion or related maritime offenses.

Typology 6 - Exploitation of Free Trade Zones and Transshipment Hubs

20. The sanctioned country -linked proliferation financing networks have repeatedly exploited Free Trade Zones (FTZs), bonded warehouses, and transshipment hubs to obscure the movement of sensitive goods and avoid detection by customs and financial authorities. These environments are often marked by relaxed inspection regimes, opaque ownership structures, and fragmented oversight, and provide an attractive cover for the misdirection, repackaging, or misdeclaration of dual-use goods.

21. Routing patterns are often structured to appear commercially plausible while deliberately masking any link to sanctioned actors. Front companies operating in jurisdictions with weak export control enforcement play a key role, as do complicit logistics providers and intermediaries in nearby financial centers. Forged end-user certificates and mislabeled documentation are common, with some goods disassembled, re-coded under generic HS codes, and shipped in parts before final assembly in the sanctioned country**.**

22. This typology is particularly relevant for customs agencies, shipping firms, freight forwarders, warehouse operators, and financial institutions involved in trade finance or remittance services. It also underscores the need for cross-border intelligence coordination and robust export control screening by national authorities.

Case Study 6: Smuggling of Industrial Equipment via UAE Free Zone

Between 2022 and 2023, a sanctioned country -linked procurement network sourced restricted industrial components, including pressure transducers, vacuum pumps, and power capacitors, from European suppliers. The shipments were routed through the Jebel Ali Free Zone in the United Arab Emirates, where the goods were repackaged for re-export to East Asia. Although initially declared as destined for Gulf-based clients, investigators later found that the end-use had been falsified.

The operation relied on several front companies registered in Hong Kong and the UAE, posing as HVAC and electronics wholesalers. These firms leveraged bonded storage and re-export services within the FTZ, allowing goods to bypass standard customs checks. Payments were fragmented across several unrelated trading companies and processed via third-party remittance agents, creating multiple disjointed financial trails that obscured any direct link to sanctioned country.

Once in East Asia, primarily Shenzhen and Dalian, the items were declared as general-purpose electronics or spare parts. Shipping manifests omitted final delivery destinations or cited fictitious Chinese importers. European exporters had received end-user declarations that were later proven to be forged, with contact information linked to dormant or non-existent companies.

Red Flag Indicators for Case Study 6:

Indicator 1: Trade activity involves free trade zones (FTZs) or bonded warehouses known for re-export services and limited customs oversight.

Indicator 2: Payments originate from third-party entities not commercially linked to the shipment, including use of remittance agents or unrelated trading firms.

Indicator 3: Shipping documentation omits final destination details or lists fictitious or untraceable importers.

Indicator 4: End-user declarations submitted to suppliers contain unverifiable company details, inactive contact information, or shell addresses.

Indicator 5: Goods are repackaged or relabeled in-transit at logistics hubs or FTZs, particularly when re-labelling obscures HS codes, technical specifications, or original manufacturers.

Case Study 7: Routing of Dual-Use Valves Through Southeast Asia

In late 2023, authorities intercepted a shipment of cryogenic valves and seals - components with potential missile applications – *en route* to a sanctioned country -linked entity. The goods were legally procured in Japan by a trading company that posed as an automotive parts supplier. The shipment then transited through Shanghai and was held briefly at a bonded warehouse in Port Klang, Malaysia, before being re-exported to an entity in Dandong previously identified in the sanctioned country procurement efforts.

The cargo passed through at least three freight forwarders. At each stage, bills of lading were altered—describing the contents alternately as “automotive spares” or “HVAC equipment.” In Port Klang, customs authorities noted that the shipment had been subdivided and merged with unrelated goods to obscure its nature.

Financial flows were equally opaque. A Thai-based remittance company routed payment to a Singaporean shell entity with no commercial footprint. Despite one freight forwarder flagging inconsistencies in the shipment documentation, the matter was not escalated to regulators, reflecting an enforcement gap in maritime and trade finance oversight.

Red Flag Indicators for Case Study 7:

Indicator 1: Shipment involves multiple freight forwarders, with cargo descriptions altered at each stage (e.g., changing from “cryogenic valves” to “automotive parts” or “HVAC equipment”).

Indicator 2: Goods are subdivided or co-loaded with unrelated items at bonded warehouses or transshipment hubs, obscuring original contents or quantity.

Indicator 3: Payment is routed through shell companies or remittance services based in jurisdictions with weak AML/CFT oversight, often lacking a clear link to the buyer or consignee.

Indicator 4: Internal red flags (e.g., documentation discrepancies or transit anomalies) are noted by logistics or compliance staff but not reported to relevant authorities.

Indicator 5: Dual-use goods sourced from credible jurisdictions are shipped via circuitous or commercially unjustified trade routes, especially through known the sanctioned country -linked transit points.

Typology 7 - Facilitation by Professional Service Providers

23. The sanctioned country -linked networks often rely on foreign professional service providers to mask sanctions evasion, either through willful facilitation or negligent due diligence. Lawyers, accountants, company formation agents, and technical consultants may be exploited to provide access to legal structures, financial systems, or specialist knowledge that would otherwise be inaccessible to the sanctioned country -linked entities or operatives.

24. These professionals may play a role in incorporating front companies, opening bank or VASP accounts, drafting technical documentation, advising on regulatory navigation, or enabling the cross-border movement of funds and goods. While some service providers are directly recruited or compensated for their role, others are misled through falsified documents or concealment of the sanctioned country nexus.

25. This typology is highly relevant for lawyers, notaries, corporate service providers, accountants, technical consultants (particularly in IT and telecom sectors), and financial institutions or VASPs servicing corporate clients.

Case Study 8: Malaysian Corporate Service Providers and the sanctioned country Front Companies

Between 2017 and 2019, UN Panel of Experts investigations revealed that corporate secretarial firms in Malaysia had played a central role in incorporating and administering front companies linked to the DPRK. These included entities such as International Golden Services and International Global Systems, which operated as cover for Glocom, a **sanctioned country** -controlled arms exporter run by the Reconnaissance General Bureau (RGB).

While some service providers may have lacked full awareness of **the sanctioned country** nexus, the Panel found several red flags were ignored, including inconsistencies in director information, use of **sanctioned country** nationals as beneficial owners, and business activities unrelated to declared corporate purposes. In one instance, onboarding documentation filed with a Malaysian bank clearly identified a **sanctioned country** citizen as the account holder and stated that the funds originated from **the sanctioned country**.

Despite these warning signs, the companies were able to open multiple personal and business accounts, facilitating the movement of funds tied to arms procurement. The failure of company formation agents and banking intermediaries to escalate obvious sanctions risks or conduct enhanced due diligence enabled the misuse of Malaysia’s corporate and financial ecosystem for **the sanctioned country** sanctions evasion.

Red Flag Indicators for Case Study 8:

Indicator 1: Company formation or administration involving **the sanctioned country** nationals as beneficial owners, directors, or authorized signatories, especially where nationality is disclosed in registration or account-opening documents.

Indicator 2: Use of the same nominee director, formation agent, or corporate address across multiple companies with opaque or unverifiable business purposes.

Indicator 3: Onboarding documents referencing **the sanctioned country** -linked individuals, institutions, or fund origin, accepted without appropriate escalation, verification, or risk-based assessment.

Indicator 4: Corporate registration forms or declarations feature implausible or contradictory business activity, (e.g., references to arms-related activity under the guise of IT or consultancy services).

Indicator 5: Company service providers or intermediaries proceed with incorporation or account setup despite visible inconsistencies in KYC data or red flags related to sanctioned jurisdictions.

Indicator 6: Repeated corporate registrations or account openings by entities later linked to sanctioned networks, with no evidence of retrospective review or reporting.

Typology 8 - Abuse of Charities and Non-Profits to Procure Dual-Use Items

26. The sanctioned country has repeatedly exploited charitable organisations and non-profit entities (NPOs) to procure sensitive dual-use goods and technologies under the guise of humanitarian aid or scientific collaboration. These operations typically involve front charities or research entities requesting items with plausible civilian uses, such as agricultural drones, laboratory equipment, or water treatment systems, which also have well-documented proliferation-related applications. In some cases, these goods have been directly integrated into sanctioned weapons programs.

27. This approach allows the sanctioned country -linked actors to circumvent commercial scrutiny by appealing to goodwill or invoking humanitarian exemptions, particularly in jurisdictions granting expedited customs clearance for NPO consignments. According to FATF and UN reporting, these vulnerabilities are especially pronounced in jurisdictions with limited oversight of cross-border aid shipments or scientific cooperation agreements. Charitable branding can also deter due diligence by logistics providers and financial institutions, which may be reluctant to apply enhanced scrutiny to ostensibly altruistic activity.

28. This typology is relevant for freight forwarders, customs officials, exporters of dual-use goods, and financial institutions that provide services to humanitarian or academic organisations. It has also been cited in FATF guidance (including Recommendation 8) as a growing vector of abuse in relation to UN-sanctioned jurisdictions and has specific implications for legal and accounting professionals involved in NPO formation and cross-border donations.

Case Study 9: Agricultural and Health NGOs Used for Dual-Use Procurement

Between 2016 and 2022, several UN Panel of Experts reports documented repeated misuse of foreign charities by DPRK-linked actors. These non-profits, often operating through Southeast Asia, China, or Africa, submitted import requests for items labelled as "agricultural aid" or "medical assistance." These included multispectral imaging drones for crop monitoring, laboratory-grade centrifuges for soil or blood analysis, gamma irradiators for pest control or sterilization, and water purification systems with radionuclide filters. Although ostensibly intended for humanitarian use, many of these goods appeared on international export control lists due to their dual-use nature. In one case, a Southeast Asia-based charity procured agricultural drones with payload capacity and imaging capabilities matching restricted military specifications. The end-user was misdeclared, and supporting documentation omitted sensitive technical features to avoid triggering export licensing thresholds. Subsequent investigation linked the end-user to a DPRK-affiliated agricultural research body under national sanctions.

UNSCR 1718 implementation reports and related Panel findings also noted that such shipments were often cleared without adequate documentation due to exemptions applied to charitable or academic consignments. The shipment was routed through a third country. Payment was made in hard currency via a Hong Kong-based intermediary, and when challenged, the charity produced a forged end-use certificate and a reference letter from a sympathetic academic partner to obscure its links to DPRK-affiliated ministries.

Red Flag Indicators for Case Study 9:

Indicator 1: Charitable organization procures drones, laboratory equipment, or irradiators inconsistent with its stated humanitarian mandate or operational footprint.

Indicator 2: Shipping or customs documentation omits or downplays technical specifications that would otherwise require export authorization.

Indicator 3: End-use declarations reference unverifiable entities, display signs of fabrication, or conceal links to DPRK state ministries or research bodies.

Indicator 4: Payments are issued by third parties in unrelated jurisdictions, with no documented link to the charity or stated project.

Case Study 10: Misuse of Scientific Collaboration Frameworks for Sensitive Imports

In its 2019–2023 watchlist advisories, the UN Security Council 1718 Sanctions Committee highlighted the misuse of scientific exchange and cultural cooperation initiatives to mask DPRK-linked procurement. These schemes often involved DPRK-affiliated universities or medical institutes registering as educational NPOs abroad.

In one example, a Europe-based research NGO entered into a bilateral academic partnership with a North Korean medical science institute. Over three years, the arrangement was used to import advanced diagnostic imaging software applicable to missile telemetry, microfluidic lab devices for field testing that were classified as dual-use under EU controls, and super-resolution microscopes subject to Wassenaar Arrangement restrictions. These items were declared as inputs for joint medical research and public health diagnostics.

However, the DPRK counterpart was affiliated with a research complex suspected of WMD development. The NGO had no scientific publications, opaque governance, and no evident funding sources - all clear anomalies that intermediaries failed to examine. The freight forwarder handling the shipments had limited documentation and no visibility into the true end-user. This case illustrates how academic collaboration can be used as a cover to transfer sensitive technology to sanctioned programs.

Red Flag Indicators for Case Study 10:

Indicator 1: Non-profit or research organization engages in academic partnerships involving controlled technology without verifiable research activity or institutional oversight.

Indicator 2: Declared DPRK partner is linked to sanctioned entities, military research centers, or known proliferation actors.

Indicator 3: Dual-use or Wassenaar-controlled goods are misdeclared as intended for civilian or humanitarian purposes.

Indicator 4: Organization lacks transparent governance, scientific outputs, or complete shipment documentation consistent with legitimate research.

Typology 9 - Trade Misinvoicing and Financial Manipulation

29. Trade misinvoicing and financial manipulation remain core methods by which the Democratic People’s Republic of Korea (DPRK) moves value across borders in violation of targeted financial sanctions. These schemes involve falsified invoices, over- or under-invoiced contracts, phantom shipments, and misrepresented goods classifications, allowing sanctioned actors to justify illicit payments or obscure the true origin, quantity, or value of traded items.

30. While formal trade channels into the DPRK are increasingly constrained, many transactions continue under the guise of barter trade, humanitarian exchanges, or commercial shipments with artificially inflated or suppressed values. According to multiple UN Panel of Experts reports, such practices enable the DPRK to obtain restricted goods, launder proceeds of sanctioned exports, and maintain foreign currency reserves that support its proliferation financing activities. Such manipulation also facilitates settlement through third-country clearing accounts and enables sanctioned entities to accumulate foreign currency earnings later channeled into proliferation programs.

31. This typology is particularly relevant to financial institutions handling trade finance instruments, customs authorities, freight forwarders, DPMSs handling collateralized trade, and DNFBPs engaged in invoice review or business formation services.

Case Study 11: DPRK Fertilizer-for-Coal Barter Scheme via Chinese Intermediaries

Between 2019 and 2021, multiple UN Panel of Experts reports documented a barter arrangement in which fertilizer shipments from China were exchanged for coal originating from the DPRK. On paper, the trades appeared legitimate, but customs records and maritime tracking data revealed major inconsistencies in declared volumes, cargo manifests, and payment structures. Fertilizer consignments were routinely invoiced at highly inflated values, in some cases as much as USD 950 per metric ton compared to the prevailing market rate of USD 350–450. Conversely, matching coal shipments from the DPRK were recorded at implausibly low prices or without any corresponding financial documentation, pointing to off-book barter rather than conventional trade.

The scheme relied on third-party trading firms incorporated in Hong Kong and Dalian, which issued back-to-back contracts designed to mask the identities of DPRK counterparties. Settlement took place through a complex network of front companies and currency exchange intermediaries operating in Macau and Southeast Asia. Notably, one of the trading companies involved had previously been linked to sanctioned arms transfers, suggesting the persistence and adaptability of its illicit networks.

This misinvoicing structure allowed prohibited DPRK coal exports, banned under UNSCR 2371 (2017), to continue under the radar, with fertilizer serving as the nominal countervalue. The barter not only obscured the underlying financial flows from banking and shipping scrutiny but also introduced proliferation concerns, as some fertilizer components, such as ammonium nitrate, are considered dual-use and potentially applicable to weapons programs.

Red Flag Indicators for Case Study 11:

Indicator 1: Invoices or shipping documentation for fertilizer or coal showing prices or volumes that significantly deviate from market benchmarks without credible justification.

Indicator 2: Trade involving prohibited DPRK-origin goods disguised as humanitarian aid or structured as barter to avoid financial scrutiny.

Indicator 3: Settlement routed through multiple front companies, shell entities, or informal remittance agents in jurisdictions with limited AML/CFT supervision.

Indicator 4: Barter transactions involving dual-use goods without verifiable end-use declarations or appropriate export licensing.

Typology 10 - State-Controlled Criminal Enterprises

32. The sanctioned country–has long operated criminal enterprises directly or indirectly controlled by state institutions, generating hard currency to finance its sanctioned weapons programs. These enterprises encompass narcotics trafficking, counterfeiting of consumer goods and currencies, and illicit trade in commodities such as tobacco and wildlife products. Unlike ordinary organized crime, these operations carry the explicit backing of the state, often orchestrated by intelligence services or military-linked trading companies acting under government direction.

33. In the absence of access to formal financial channels, these illicit ventures form a durable alternative stream of foreign exchange. Proceeds are frequently funneled through informal remittance networks, diplomatic channels, or regionally embedded front companies. The funds ultimately support procurement activities, cyber operations, or weapons development. Such operations frequently intersect with formal-sector actors, including logistics providers, DNFBPs, and informal money transfer operators, who may be unaware that they are facilitating the laundering and reinvestment of criminal proceeds.

34. This typology presents significant proliferation financing (PF) risk because it operates almost entirely outside formal oversight frameworks. The activities often involve high-risk or dual-use commodities, take place in jurisdictions with weak enforcement capacity, and rely on layered deception strategies to obscure beneficial ownership.

Case Study 12: *Pong Su* Heroin Trafficking Operation

A landmark example of the sanctioned country use of state resources for organised criminal activity is the 2003 Pong Su incident off the coast of Australia. The sanctioned country--flagged cargo vessel covertly delivered 125 kilograms of high-grade heroin, worth over AUD 160 million, via a clandestine beach landing in Victoria. Australian authorities intercepted the offload, arresting several participants, including senior members of the vessel's crew.

Subsequent investigations confirmed that the Pong Su was operated by sanctioned country state-owned trading company and carried official diplomatic documentation. The use of a government-owned vessel for narcotics smuggling demonstrated the regime's willingness to blur the line between state operations and criminal enterprise. Although the event occurred over two decades ago, it remains a reference point in UN and think-tank analysis due to its clarity in illustrating_the sanctioned country criminal-financing architecture.

The case also revealed how the sanctioned country–institutions have both the logistical capability and the political will to conduct transnational trafficking, leveraging sovereign cover to shield operatives and recover assets. Such characteristics: state involvement, use of official status, and high-risk commodities, remain hallmarks of current PF risk assessments.

Red Flag Indicators for Case Study 12:

Indicator 1: Deployment of state-affiliated or diplomatically registered vessels in commercial transactions lacking a clear economic purpose or market justification.

Indicator 2: Declared cargo inconsistent with the vessel's build, itinerary, or flag registry, particularly for voyages originating from the sanctioned country-ports.

Indicator 3: Evidence of criminal activity involving vessels operated by entities with sovereign, diplomatic, or state-affiliated ties.

Indicator 4: Invocation of diplomatic immunity or political pressure following interdictions involving serious transnational crimes.

Emerging AI-Enabled Behaviors and Associated Red Flag Indicators

35. Artificial intelligence (AI) is transforming the mechanics of sanctions evasion and proliferation financing. For the sanctioned countries and other high-risk actors, AI tools now amplify familiar tactics : identity fraud, document forgery, cyber theft, by increasing their realism, scale, and speed.

36. These indicators are designed to capture cross-cutting AI-enabled behaviours that can appear across multiple typologies, particularly where traditional red flags manifest with unusual precision or persistence.

AI-Generated Identities and Deepfakes

UN Panel of Experts reporting and law enforcement advisories have documented DPRK-linked IT workers using AI-based face-swapping during live video calls to impersonate legitimate contractors. These techniques can bypass facial recognition and image verification in remote onboarding, enabling sanctioned nationals to secure income under false identities.

Red flag: Subtle video anomalies (e.g., lip-sync delays, unnatural blinking) during KYC; profile images with no verifiable online history.

Generative AI-Fabricated Documentation

AI tools can produce forged trade documents, bank statements, and corporate profiles that are visually credible but entirely fictitious. the sanctioned country -linked actors have used such capabilities to create tailored CVs and corporate histories that pass superficial screening.

Red flag: Documents from different purported issuers that share suspiciously identical formatting or metadata; “perfect” paperwork from unverifiable sources.

Synthetic Identity and Shell Company Networks at Scale

AI can rapidly generate hundreds of synthetic personas and corporate entities with coherent but false digital trails, overwhelming traditional due diligence processes.

Red flag: Clusters of newly incorporated companies in multiple jurisdictions that share repeating design elements (email syntax, web templates) with no plausible commercial linkages.

AI-Enhanced Social Engineering

Large language models can produce phishing or payment instruction requests that precisely mimic internal communications, while deepfake audio or video can replicate executives' voices or likenesses to authorize illicit transfers.

Red flag: Requests from senior officials that are uncharacteristically perfect and resist independent voice or identity verification.

High-Tempo, Multi-Channel Coordination

AI-assisted operations can sustain round-the-clock activity across multiple languages and platforms, adapting instantly to detection or countermeasures.

Red flag: Intermediaries engaging continuously in complex transactions without downtime; frequent, rapid payment instruction changes optimized to avoid detection.

37. These behaviors do not replace established PF red flags: they amplify and conceal them. Compliance teams should focus on the *combination* of classic anomalies with signs of algorithmic consistency or "uncanny" precision. Detecting such patterns requires both upgraded human review and the deployment of counter-AI tools, including deepfake detection, metadata analysis, and multi-source verification.

38. While regulatory typologies for AI-enabled evasion are still evolving, they are no longer hypothetical. Evidence from UN Panel of Experts reports, cybersecurity and blockchain analytics firms (e.g., Chainalysis), and specialist think tanks (e.g., RUSI) shows that these tactics are already in use. Proactive monitoring and escalation will be critical to mitigating the next phase of the sanctioned country and other high-risk actors' proliferation financing strategies.