Proliferation Financing Typologies and Red Flags

August 2026

Isle of Man
Financial Intelligence Unit
Ellan Vannin Unnid Tushtag Argidoil

Contents

Introduction

The continued proliferation of weapons of mass destruction (WMD), together with the financing that enables it, poses a significant threat to international security and the integrity of the global financial system. The Isle of Man as an established, reputable international financial centre (IFC), presents potential vulnerabilities that could be exploited for Proliferation Financing (PF) purposes. Although the Isle of Man has minimal links to PF states, this does not mean that the Island faces little or no PF risk. By concealing illicit conduct and exploiting international commercial systems, proliferators can apply a global reach to target well-regulated jurisdictions, reinforcing the need for reporting entities to remain fully aware of their domestic and international obligations.

The Isle of Man National Risk Assessment (NRA) classifies the Island's overall residual risk of PF as **medium low**. The NRA outlines the PF risks across several sectors, notably: Financial Institutions (banking and insurance); Designated Non-Financial Businesses and Professions (TCSPs and VASPs)*; e-Gaming; Manufacturing; and Ship and Aircraft Registries.

This report consolidates intelligence, open-source information and adapted international case studies into fictitious typologies relevant to the Isle of Man. Each typology illustrates how PF can manifest across different regulated sectors, including banking, TCSPs, life assurance, online gambling, virtual assets, real estate and legal/accounting services.

The typologies provided in this report are intended to help industry identify and report suspicious activity to the Financial Intelligence Unit (FIU) in line with the Island's counter PF obligations. While not exhaustive, the typologies and red flag indicators demonstrate the wide range of ways in which PF threats can materialise.

The FIU produces typology reports in accordance with Financial Action Task Force (FATF) Recommendation 29: *to identify and raise awareness of emerging and priority financial crime threats*. This PF report builds on the findings of the Isle of Man's 2026 PF NRA and the following FATF reports:

- Guidance on Counter Proliferation Financing report (2018).
- Guidance on Proliferation Financing Risk Assessment and Mitigation report (2021).
- Complex Proliferation Financing and Sanctions Evasion Schemes report (2025).

A core function of the Isle of Man's FIU remains gathering, storing, analysing and disseminating intelligence related to the financing of proliferation of WMD. The purpose of this report is to highlight potential indicators, sector vulnerabilities and practical examples relevant to the Isle of Man's regulated sectors.

* Trust and Corporate Service Providers and Virtual Asset Service Providers.

"A typology is the study or systematic classification of types that have several characteristics or traits in common"
-ECOFEL

The Isle of Man's Risk Context?

The Isle of Man NRA concludes that the jurisdiction's risk from PF is classified as **medium low**.* While there have been no domestic or international PF investigations in the Isle of Man, the risk exposure identified in the NRA is primarily being driven by the Island's role as a well-established IFC. The vulnerabilities identified as part of this include:

- Extensive non-resident customer base.
- Multi-jurisdictional/complex ownership arrangements.
- Diversity of financial and professional services.

While the Island faces minimal direct exposure to PF states, its global connectivity facilitates legitimate cross-border financial activity that presents an opportunity for misuse by proliferators. As an IFC, the Isle of Man routinely handles inward and outward flows of significant volume and value, involving multiple jurisdictions and a variety of regulated sectors, including banking, insurance, TCSPs, VASPs, e-gaming, manufacturing and ship and aircraft registries. This creates exposure to:

- Transit of funds linked to high-risk states and states of concern.
- Evasion of sanctions through complex structures that obscure ownership.
- Layering and integration through legitimate business activity and investment.

The NRA outlines how the Isle of Man's financial system can be exploited by a malign actor's** transnational proliferation network by providing a suitable structure for PF. As such, vigilance is essential across all sectors to detect and disrupt transactions that may be intended to support proliferation overseas.

* The Isle of Man NRA uses the Royal United Services Institute (RUSI) PF Risk Assessment methodology to determine a PF score. The scale range is: High; Medium High; Medium; Medium Low; and Low.
** A malign actor is an individual, group, or state entity that deliberately engages in harmful, deceptive, or coercive actions designed to undermine laws, destabilise societies, or attack institutions.

Background: Understanding Proliferation Financing

PF, like Money Laundering (ML), relies on the obfuscation and concealment of information, often relating to beneficial ownership, payment routes and true end-users. Similarly, like Terrorism Financing (TF), PF involves a linear money trail that facilitates further illicit activities. However, despite these overlapping features with other forms of financial crime, PF is recognised as fundamentally different in its classification, presenting its own distinct risks across the global financial system.

To date, there is no universally recognised definition of proliferation or PF. However, broad working definitions of both have been provided by the FATF.[1]

> ***"WMD proliferation"*** *refers to the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both dual-use technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.*

> ***"Proliferation financing"*** *refers to the act of raising, moving, or making available funds, other assets or other economic resources, or financing, in whole or in part, to persons or entities for purposes of WMD proliferation, including the proliferation of their means of delivery or related materials (including both dual-use technologies and dual-use goods for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.*

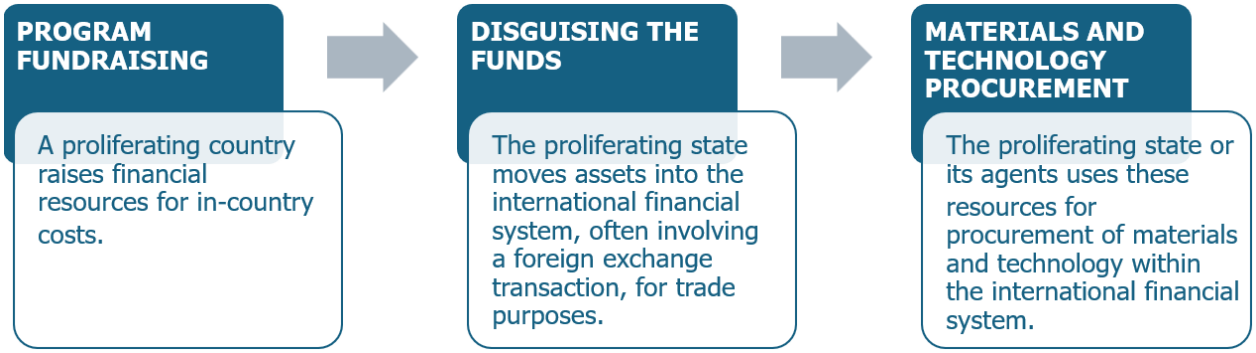
It should be noted that dual-use goods and technologies are items which can be used for both civil and military purposes. The consolidated list of strategic military and dual-use items that require export authorisation can be found on the gov.uk website. [2]

1. FATF – Guidance on Proliferation Financing Risk Assessment and Mitigation (2021).
2. https://www.gov.uk/government/publications/uk-strategic-export-control-lists-the-consolidated-list-of-strategic-military-and-dual-use-items-that-require-export-authorisation.

Background: Understanding Proliferation Financing

PF Stages

PF activities can generally be broken down into distinct stages. A report by the Centre for a New American Security has identified and documented three stages: programme fundraising; disguising the funds; and materials and technology procurement.[3] The diagram below illustrates the linear sequence of these stages, from raising funds to paying for goods and services.



While these three stages provide a useful framework for PF, it is recognised that, unlike other types of financial crime, PF remains difficult to conceptualise. RUSI's 2024 paper on the risks associated with PF addresses this and splits PF into two categories: Direct and Indirect.[4] This binary categorisation highlights how a jurisdiction's PF-related risk is not only created through their direct involvement in the proliferation supply chain, but also indirectly, via various facilitation channels.

Direct PF

Direct PF relates to the financial products and services associated with trade in proliferation-sensitive goods and technologies. While this refers to products with direct proliferation application, such as items covered by the European Union's (EU) Consolidated Control List, ambiguity exists around what qualifies goods and technologies as 'proliferation-sensitive'. This creates a challenging and continuously expanding 'below-threshold' grey area that a jurisdiction's regulated sectors must navigate.

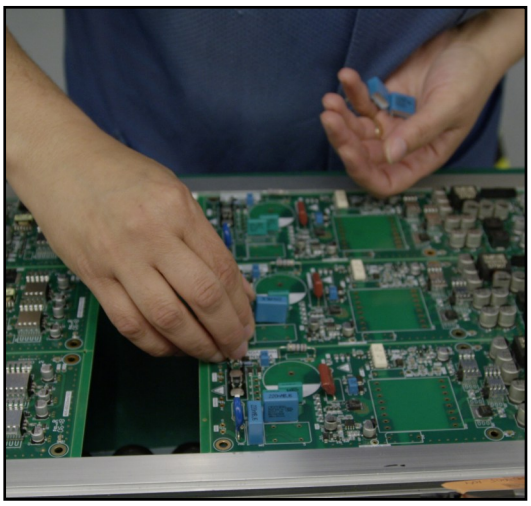
Alongside this, the difficulty of direct PF identification has only intensified as a result of the ever-changing financial products, services and strategies that are being employed to purchase these items. To date, the Isle of Man has not had any known exposure to direct PF, therefore an example has been adapted from the United Kingdom's (UK) most recent PF National Risk Assessment, published in 2021.[5]

Case Study 1: Direct Procurement of Dual-Use Items from a UK Company

This case involved a UK company that was an exporter of items that were recognised as having dual-use potential. A second company, based in a foreign jurisdiction, approached the UK exporter with the intention of purchasing these high specification dual-use items. The buyer specified that the purpose of these items was to contribute to a non-military project in an area that was local to their country's boundaries.

3. https://www.cnas.org/publications/reports/the-financing-of-nuclear-and-other-weapons-of-mass-destruction-proliferation.
4. RUSI - Guide to Conducting a National Proliferation Financing Risk Assessment (2024).
5. HM Treasury: National Risk Assessment of Proliferation Financing (2021).

Background: Understanding Proliferation Financing



Customer due diligence conducted by the UK exporter revealed a complex financial structure that involved a number of overseas companies with limited trading histories. When questioned, the buyer justified this structure as being required for client/agent confidentiality and to enable the specific project to be financially ring-fenced from the customer's other business interests. While not overly common, these can be acceptable business practices, so the UK exporter opted not to investigate further. By not flagging this behaviour as suspicious, the exporter had unknowingly opened themselves up to PF risk.

This became evident only when a more detailed examination of the technical requirements of the items and the proposed transaction was conducted by His Majesty's Revenue and Customs (HMRC), which revealed the true intention of the buyer. Evidence indicated that the items were instead destined for a military project controlled by a different jurisdiction that was subject to international sanctions.

Observation: *This case highlights the importance of conducting sufficient levels of customer due diligence, particularly when it relates to foreign jurisdictions and the legitimacy of the end users.*

Themes: Dual-Use Items, Legitimate End-Users, Item End-Use, Client Confidentiality, Customer Due Diligence, Financial Structures.

Indirect PF

Indirect PF covers a broad range of activities that facilitate and/or significantly contribute to WMD proliferation. Unlike direct PF, indirect PF can be considered as activity where there is more than one step between the act of financing proliferation and the proliferator. A prevalent form of indirect PF is the act of fundraising by proliferators, or supportive parties, to generate funds for their WMD programmes. As these funds can stem from both licit and illicit activities, red flag indicators are not always present, making the prevention, suppression and disruption of indirect PF more challenging than direct PF.

Illicit Fundraising Activities	Licit Fundraising Activities
Fraud	Charitable Donations
Cybertheft	Government Funding
Arms Trafficking	Sale of Non-Nuclear Military Equipment
Illegal Wildlife Trade	Sale of Natural Resources
Drugs Smuggling	Foreign/Commercial Trade
Forgery	Legitimate Business (restaurants, construction etc.)

**Note: This list of licit and illicit PF fundraising activities is not exhaustive. More detailed breakdowns can be found in PF papers by FATF and RUSI.[6,7]*

6. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Complex-PF-Sanctions-Evasions-Schemes.pdf.coredownload.inline.pdf.
7. https://static.rusi.org/20190513_guide_to_conducting_a_national_proliferation_financing_risk_assessment_web.pdf.

Background: Understanding Proliferation Financing

The identification of proliferator involvement can be further obfuscated through the addition of intermediaries within a PF network. These will vary from individuals, such as lawyers and accountants, businesses (e.g. shell companies) and third-party jurisdictions. The larger and more complex these networks become, the greater the chance that companies fail to identify red flags and unwittingly partake in accidental indirect PF.

For the Isle of Man's regulated sectors, it is these transnational PF networks and the intermediary services within them (banking, insurance, TCSPs and VASPs) that provide the highest risk of PF exposure. A second case study, again extracted from the UK's PF National Risk assessment 2021, demonstrates how an Isle of Man company could be involved in indirect PF.[8]

Case Study 2: Indirect Exposure through the use of intermediary jurisdictions to mask the involvement of designated entities

This case involved an international bank, with a UK footprint. Its customer, the leading shipping company in its jurisdiction, attempted to transfer funds, via an intermediary bank, to a non-designated Egyptian shipping and marine supply company. The payment was in reference to services that had been provided by the Egyptian company relating to a non-designated bulk carrier. While initial assessments by the international bank had not identified above-threshold concerns, the transaction was frozen by the intermediary bank. This action was based on intelligence linking the Egyptian company to a North Korean entity. Evidence indicated the North Korean entity had, over-time, embedded employees in the Egyptian company, effectively making it a front company for the North Korean entity.

If the transaction had been allowed to progress, it is possible that these funds posed a PF risk, based on the North Korean entity's link to its state of origin. The Democratic People's Republic of Korea (DPRK), an internationally recognised high-risk jurisdiction for PF and WMD development, is known to pose a critical threat to global non-proliferation efforts.

Observation: *This case highlights the effort that proliferators can make to obfuscate their involvement and the indirect PF exposure that results from this. It is crucial that companies conduct sufficient 'know your customer' actions and broader due diligence checks throughout the entire transactional pathway, ensuring that they are applied with appropriate rigour, breadth and depth.*

Themes: Sanction Evasion, Front and Shell Companies, Foreign Intermediaries, Correspondent Banking, Indirect Payment Methods, Non-Proliferating State Involvement.

8. HM Treasury: National Risk Assessment of Proliferation Financing (2021).

Countering Proliferation Financing

As described by the North Atlantic Treaty Organization (NATO), the proliferation of WMD and their delivery systems by malign actors could have incalculable consequences, making PF disruption and prevention a critical component of efforts to maintain global security and stability.[9] To accomplish this, organisations such as the United Nations (UN) Security Council and FATF have established international frameworks to counter PF.

UN Security Council Resolutions (UNSCRs): The UN has introduced three main resolutions that directly apply to proliferation.[10] The implementation of these resolutions against designated entities, individuals or those acting on their behalf, is mandatory for all UN member states. While the Isle of Man is not a UN member state, as a Crown Dependency its international relations are handled by the UK and UN obligations are therefore extended to the Island.

UNSCR 1540 (2004) requires members to prohibit any non-state actor from financing the manufacture, acquisition, possession, development, transfer or use of WMD. In addition, states must establish, develop, review and maintain appropriate controls on providing funds and services, such as financing, related to the export and transshipment of items that would contribute to WMD proliferation.

UNSCR 1718 (2006) imposes an arms embargo, assets freeze and travel ban on persons involved in the DPRK's nuclear programme. In addition, a ban on a range of imports and exports, to prohibit the DPRK from conducting nuclear tests or launching ballistic missiles.

UNSCR 2231 (2015) endorses the Joint Comprehensive Plan of Action on Iran, terminated previous sanctions measures and established a framework for monitoring and restrictions on Iran's nuclear programme.

FATF Recommendations: The FATF Recommendations are recognised as the global standard for anti-money laundering (AML), counter-terrorist financing (CTF) and counter-proliferation financing (CPF) efforts. Four of the 40 Recommendations outline the international requirements for implementing PF-Targeted Financial Sanctions (PF-TFS), which are summarised below:

Recommendation 1 requires countries, financial institutions, designated non-financial businesses and professionals, virtual asset service providers, and non-profit organisations to identify and assess the risks of potential breaches, non-implementation or evasion of PF-TFS and to take action to mitigate them.

Recommendation 2 requires countries to put in place effective cooperation and coordination of the relevant authorities to combat ML, TF and PF.

Recommendation 7 of the FATF Standards requires countries to implement PF-TFS made under UNSCRs.

Recommendation 15 requires countries to conduct a PF risk assessment and establish mitigation in respect of virtual asset activities and service providers.

9. https://www.nato.int/en/what-we-do/deterrence-and-defence/weapons-of-mass-destruction.

10. Detailed breakdowns of UNSCR 1540, 1718 and 2231 are available on the UN's website: https://main.un.org/securitycouncil/en/content/resolutions-0.

Countering Proliferation Financing

FATF Immediate Outcomes: The FATF Immediate Outcomes are a set of benchmarks that the FATF has adopted to assess the effectiveness of a jurisdiction's AML, CTF and CPF. The objective in implementing these measures is to protect financial systems and the broader economy from the threats of ML, TF and PF. Out of the 11 immediate outcomes, only one directly addresses PF:

> ***Immediate outcome 11*** dictates that persons and entities involved in the proliferation of WMD are prevented from raising, moving and using funds, consistent with the relevant UNSCRs.

Through export controls, travel bans, targeted financial sanctions, transport sanctions and recognised international standards, the UN and FATF aim to disrupt PF networks. As a result of this, they form a central part of the international framework to prevent the spread of WMD and maintain global stability. It is therefore critical that the Isle of Man remains fully aligned with these international standards.

Proliferation Financing Threat Actors

Despite comprehensive international and national sanctions, as well as strict proliferation-targeted import and export controls, some states of proliferation concern are still successfully obtaining the capital required to fund their WMD programmes.[11] This is achieved through complex procurement and revenue generation schemes, with state-sponsored or state-affiliated actors evading sanctions by virtue of a diverse range of deceptive strategies. While not an exhaustive list, these sanction evasion schemes often comprise of:

- **Intermediaries enlisted to handle components of the scheme.**
- **Multi-jurisdictional pathways to capitalise on low-regulation jurisdictions.**
- **Obscuring Beneficial Ownership Information to hide end user information.**
- **Using new technologies to avoid detection.**
- **Exploitation of maritime and shipping sectors to transport dual-use materials.**

As identified in the Isle of Man NRA, sanctions evasion that aims to hide the identity of the designated persons and entities are a common tactic employed by states engaged in, or supporting, illicit proliferation networks. While the UNSCRs formally designate the main state actors that pose PF risk as the DPRK and Iran, other states, such as Russia, China and Pakistan are commonly referenced as States of Proliferation Concern, as well as PF-enablers.[12]

The following section provides examples of how PF states, as well as some of the more notable States of Proliferation Concern, could be conducting, or contributing to, PF in an Isle of Man context.

PF States

DPRK

As part of the FATF's 2025 report that covered PF and sanctions evasion, the FATF Global Network recognised the DPRK as the most significant PF actor at the time of publication.[13] Under the leadership of their Supreme Leader, Kim Jong Un, the DPRK regime outwardly highlights its possession of nuclear weapons as an international deterrent, integral to the regime's survival. The regime has been subject to significant international sanctions since it conducted its first nuclear test in 2006.[14]

More recently, their public testing of Intercontinental Ballistic Missile capabilities in 2022 and 2023 resulted in the expansion of UN Security Council PF-TFSs.[15] These enhanced restrictions to the global financial market aimed to disrupt the DPRK's PF networks and destabilise their WMD programme. Despite this, the DPRK remains in an active state of proliferation development.

Widely considered one of the most comprehensive and strictly enforced UN sanctions regimes, the DPRK is

11. FATF - Complex Proliferation Financing and Sanctions Evasion Schemes (2025).
12. RUSI - Guide to Conducting a National Proliferation Financing Risk Assessment (2024).
13. FATF - Complex Proliferation Financing and Sanctions Evasion Schemes (2025).
14. https://www.belfercenter.org/publication/north-koreas-oct-9-nuclear-test-successful-or-failed.
15. U.S. Treasury - National Proliferation Financing Risk Assessment (2024).

increasing its use of illicit methods to fund strategic projects that include a WMD programme.[16] While the extent of this fundraising is unknown, the UN Security Council Panel of Experts estimate that between 2017 and 2023, the DPRK generated over $3 billion, primarily in cryptocurrency, through illicit cyber activities and other sanctions-evading methods.[17]

In line with the evolution of modern armed forces, it is understood that the DPRK already has considerable specialised cyber units within its military. These units employ highly sophisticated techniques to execute criminality across the cyber domain. While in no way exhaustive, techniques include:

**Note: Definitions for these techniques can be found on page 26 of this document.*

By engaging in hybrid warfare tactics, the DPRK has been able to maintain revenue generation and bypass international sanctions.

The Lazarus Group, a prolific cybercrime organisation that gained notoriety after executing some of the most consequential and high value cyber-attacks in history, is believed to be a core component of the DPRK's cyber criminality. Active since at least 2009, this group engages in illicit activity, including cyberespionage, financial theft and cyberwarfare. Its historical targets have been banks, cryptocurrency exchanges and governments worldwide that provide an opportunity for the DPRK to extract money from the global financial system.

During this extraction, a common strategy for groups like the Lazarus Group is to utilise offshore IFCs as nodes for moving stolen funds back to the regime. This is due to a perceived regulatory vulnerability of offshore IFCs, as well as their access to the global financial system and the opportunity for further layering of PF networks. It is the Isle of Man's status as an offshore IFC that exposes its regulated sectors to potential DPRK targeting for PF exploitation.

Iran

It is important to note that the international landscape surrounding Iran remains fluid, shaped by evolving legal interpretations, geopolitical tensions and recent developments in the application of UN measures. This section reflects the FIU's current understanding as at August 2026, recognising ongoing uncertainty and evolving developments, particularly in relation to Iran's possible WMD programme.

16. https://ipdefenseforum.com/2025/05/north-koreas-shadow-economy-fueled-by-illicit-activities/#:~:text=North%20Korea's%20cyber%20capabilities%20have,stolen%20funds%20through%20complex%20networks.

17. https://www.cyfirma.com/research/dprk-sanctions-violations-in-cyber-operations-post-un-panel-demise/.

Proliferation Financing Threat Actors

Currently, ultimate authority in Iran rests with the Supreme Leader, with the Islamic Revolutionary Guard Corps (IRGC) acting as a highly influential force within the state that ensures regime survival. While there is no evidence of Iran or the IRGC possessing operationally ready WMD, there is considerable speculation around their intent and the timeline required to achieve the capability. In order to prevent this, the United States, the UN , the EU and several Western allies have placed region specific sanctions on Iran. These are intended to restrict Iran in their suspected proliferating activities.

In response, Iran has adopted a range of mechanisms to bypass these sanctions, including the creation of 'co-operation channels' with other states. These trade channels with willing partners, such as China, ensure that Iran maintains access to the global financial system. Through the purchase of Iranian exports, funds are generated and distributed across the regime's strategic projects, which could include WMD programmes.

The Iranian shadow fleet is a critical enabler for such illegal trade by providing discreet access to global shipping networks and foreign markets, particularly in regard to the transportation of Iran's petroleum and petroleum-related products. The fleet is comprised of a group of opaquely owned vessels that are used by Iran to circumvent many of its international sanctions. It is possible that vessels in this fleet have been, or will be, used for the exportation of sanctioned products to generate funds for proliferation development, or in the importation of sanctioned dual-use goods and technologies back into Iran

Recently, the region has experienced ongoing volatility. In June 2025, the 12-day war between Israel and Iran resulted in the US intervening via Operation MIDNIGHT HAMMER. Several Iranian nuclear sites were struck, after which a ceasefire was brokered. This endured until February 2026, when the US and Israel pre-emptively struck Iran. The primary justification for this new operation (Operation EPIC FURY) was that Iran was suspected of re-developing its WMD arsenal.

The Strait of Hormuz, a natural chokepoint linking the Persian Gulf to global energy markets, became a focal point for this conflict, particularly as approximately 20% of both global petroleum liquids and liquefied natural gas travel through this waterway.[18,19] Iran's tactical disruption of this trade route therefore has had a significant impact on international markets and supply chains, placing considerable pressure on Western allies domestically.

During the crisis, global demand for oil persisted despite a significant reduction in supply. This scarcity heightened concerns that restricted crude from exporters like Iran and Russia would

18. https://www.eia.gov/international/analysis/special-topics/World_Oil_Transit_Chokepoints.
19. https://www.eia.gov/todayinenergy/detail.php?id=65584.

seep into global markets and gain wider acceptance among desperate buyers. Driven by supply pressures and operational necessity, firms faced an elevated risk of inadvertently facilitating PF.

In addition to this, Iran's imposition of a safe-passage toll on vessels that were transiting through the Strait of Hormuz, payable via cryptocurrency, demonstrated a growing level of technical sophistication and a more overt use of digital assets by the IRGC.[20] This development further highlights the potential threat posed by Iran's exploitation of emerging financial technologies for sanctions evasion and revenue generation.

Despite ongoing efforts to restore a broken truce, the full implication of this conflict remains ambiguous as events continue to unfold. While the Isle of Man has had no criminal investigations linked to Iran, its position as an IFC and global maritime hub remains the most likely risk exposure to Iranian sanction evasion efforts.

States of Proliferation Concern

While North Korea and Iran have the status of PF states, other jurisdictions, such as Russia, China and Pakistan, also pose proliferation threats. States of Proliferation Concern is a broader geopolitical classification than PF States that is used to label countries suspected or known to be attempting to acquire, develop or transfer WMD. As the Isle of Man regulated sectors are more commonly exposed to Russia and China, it is these jurisdictions that have been covered below. However, vigilance across all activity concerning any States of Proliferation Concern is paramount in order to maintain the integrity of the Isle of Man's financial system.

Russia

It is internationally recognised that Russia maintains the largest and most capable nuclear weapons stockpile in the world.[21] To date, there is no evidence to suggest that Russia has, or intends to, slow down its WMD development and the modernisation of its capabilities.

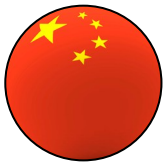
While Russia has not conducted a full-scale nuclear explosion since 1990, it has recently prepared its Novaya Zemlya test site for potential future tests.[22] Alongside this domestic investment in proliferation infrastructure, Russia has also stepped back from or halted its involvement in various international arms control and WMD mechanisms. This includes treaties such as the Comprehensive Nuclear-Test-Ban Treaty (CTBT), which Russia revoked its ratification of in 2023.[23] The CTBT prohibits any testing of nuclear explosive devices and acts as a foundational component of the global effort to prevent nuclear proliferation.

Since Russia's invasion of Ukraine in February 2022, Russia has struggled to increase its arms production, resulting in the significant shrinkage of their conventional arms stockpiles.[24] As an attempted counter measure, Russia has increased engagement with close partners, such as the DPRK and Iran, to replenish

20. https://www.ft.com/content/02aefac4-ea62-48db-9326-c0da373b11b8?syn-25a6b1a6=1.
21. U.S. Treasury - National Proliferation Financing Risk Assessment (2024).
22. https://www.csis.org/analysis/russias-latest-nuclear-saber-rattling-nuclear-testing.
23. https://press.un.org/en/2023/sgsm22022.doc.htm.
24. https://cepa.org/article/russias-year-of-truth-the-missing-military-hardware/.

its stocks.[25] It has been suggested that, in return for these conventional weapons systems, nuclear weapon material or expertise could be being transferred back to these states.[26] As the war in Ukraine continues and Russian arms stockpiles continue to be depleted, it is possible that Russian efforts to enable PF will accelerate.

This course of action heightens the risk of the Isle of Man's regulated sectors being unknowingly involved within a PF-related transactional chain. While no cases linking Isle of Man to Russian-enabled PF are currently known, other jurisdictions have identified attempted exploitation. Commonly, this manifests as sanctions evasion and the leveraging of front and shell companies to finance or place orders for dual-use good and technologies.[27]



China

Over the course of the last 5 years, China has been conducting its largest nuclear buildup in history. Between 2020 and 2025, reports estimate that their nuclear arsenal has approximately doubled, from 300 to 600 warheads, making it the third largest nuclear power after Russia and the US.[28]

This places China in a position of authority on the world stage that, combined with its status as a major economic power, underpins a global attitude that is growing in confidence. With this, comes an evolving level of independence and perceived superiority that motivates China to disregard international treaties, sanctions and obligations that it deems non-beneficial to the state.

While being demonstrated in a number of ways, one manifestation of this growing defiance is the trade with known PF states. In respect to Iran, published papers indicate that China has long been the primary purchaser of Iranian oil,[29,30] purchasing between 80-90% of Tehran's oil exports in 2025.[31] This relationship was formalised in 2021, when the Iran-China 25-year cooperation agreement was signed. By establishing Iran as a critical energy source to China, the flow of Chinese funds back into Iran acts as an economic lifeline for the IRGC. Despite China breaching no UN sanctions through this agreement, it is highly likely that the money generated through the sale of Iran's oil is contributing to the IRGC's defence budget which is suspected to include a WMD programme.

25. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/09/pub25-094-tracking-the-components-of-missiles-and-uavs-used-by-russia-in-ukraine.pdf.
26. https://platform.opennuclear.org/thoughtroom/external-contributions/russia-the-iran-nuclear-programme-and-the-degradation-of-non-proliferation-norms-and-tools.
27. https://finance.ec.europa.eu/document/download/ae2e63e2-4c4d-4f77-9757-c408ddbcede1_en?filename=240924-preventing-russian-export-control-sanctions-evasion%20.pdf.
28. https://www.csis.org/analysis/parading-chinas-nuclear-arsenal-out-shadows.
29. https://www.researchgate.net/publication/345436280_Sino-Iranian_Oil_Investment_Current_Status_Analysis_and_Countermeasure_Research.
30. https://www.uscc.gov/sites/default/files/2026-03/China-Iran_Fact_Sheet_A_Short_Primer_on_the_Relationship.pdf.
31. https://www.bruegel.org/analysis/what-war-iran-means-china.

Chinese trade has also been documented with the highly sanctioned DPRK.[32] This is perhaps not surprising given the shared border, unified opposition to Western global dominance and China's willingness to breach international export/import control regimes. The border itself runs along the Yalu River, with a number of port cities positioned along its shores. Cities such as Dandong, China and Sinuiju, North Korea operate as trading nodes for these nations to engage with each other while shielded from the surveillance of others. Unlike the Iran-China agreement, trade with the DPRK is widely sanctioned by the UN, resulting in China, a permanent member of the UN, actively violating its binding international legal obligations.

Published articles indicate that the importation of raw materials, such as coal and sand,[33,34] by China from North Korea, is a core fund raising pathway for the DPRK, that is likely diverted to the funding of WMD and defence programmes. Alongside this, it is also possible that this border provides a valuable entry point for dual-use items and intellectual know-how into the DPRK, using China as both a supplier, as well as a country of diversion to facilitate sanction breaching from other jurisdictions.[35]

Critically, exposure to China's trade with PF states poses a rare but realistic risk to firms on the Isle of Man. The US treasury reported that shell companies have been set up and used in the UK by China-North Korean cross-border traders, to act on the behalf of North Korean proliferators and help them launder tens of millions of dollars, as well as procure items for their WMD programme. It is possible these traders could look to exploit Isle of Man firms in a similar payment architecture.

Non-State Actors

It is important to note that non-state actors, such as terrorist organisations, also pose a proliferation threat, although their involvement in PF remains comparatively limited. While groups such as ISIL, Aum Shinrikyo and al-Qaeda have demonstrated intent through the limited use of chemical agents,[36] terrorist entities typically pursue objectives distinct from state militaries, including generating fear to convey ideological or political messages. Such objectives can often be achieved without WMD, through smaller-scale, less sophisticated attacks that generate psychological impact and unrest within a population.

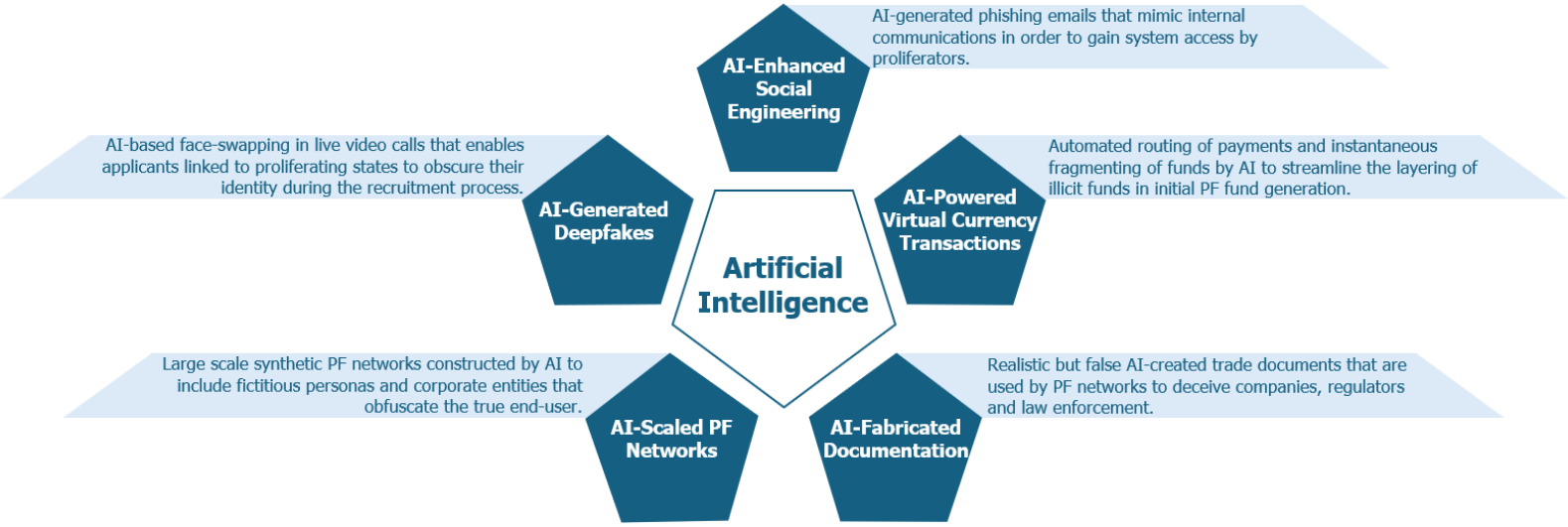
Unlike states, terrorist organisations lack territorial sovereignty, freedom from prosecution and jurisdictional protection, which severely constrain their ability to develop, conceal or sustain large-scale clandestine WMD programmes. As a result, while non-state actors may participate in PF-related activity or feature within proliferation networks, the lower applicability and practical feasibility of WMD to their objectives makes such activity less common than state -sponsored proliferation.

32. https://www.kcl.ac.uk/news/north-koreas-proliferation-illicit-procurement-apparatus-within-china.
33. https://undocs.org/S/2021/211.
34. https://c4ads.org/blogposts/against-the-grain.
35. https://publications.parliament.uk/pa/cm201919/cmselect/cmfaff/109/109.pdf .
36. ISIL: https://news.un.org/en/story/2023/06/1137492.
Aum Shinrikyo: https://www.cwccoalition.org/events/anniversaries/tokyosubwaysarinattack30th/.
Al-Qaeda: https://ctc.westpoint.edu/reevaluating-al-qaidas-weapons-of-mass-destruction-capabilities/.

Emerging Proliferation Financing Methods & Risks

Internationally, cyber-enabled PF has been identified as an area of considerable and growing risk to global CPF efforts.[37] Proliferators, with the DPRK at the forefront, are capitalising on the dynamic and fast-evolving capabilities of technology to continuously evade sanctions and generate revenue for WMD programmes. Cybercrime appeals to proliferators primarily because it provides a low-risk, high-reward method to bypass international sanctions and conduct PF. Along with exploiting foreign financial systems with a level of anonymity difficult to achieve through traditional sanctions evasion methods, cyber operations also allows proliferators to engage in industrial espionage and the theft of intellectual property from within the safety of their own borders.

In addition to this, the PF efforts of proliferators are only expanding as their accessibility to Artificial Intelligence (AI) tools also increases. These AI tools have transformed and continue to transform the PF landscape by lowering the barrier to entry for criminality and introducing a level of obfuscation that can overwhelm most monitoring and enforcement mechanisms.[38] While conventional methods of sanctions evasion remain common, AI tools are providing opportunities to amplify these PF strategies by increasing the realism, scale and speed of their outputs.



**Note: These examples were extracted from a PF document published by Saudi Arabia's Ministry of Foreign Affairs.[39]*

In addition to PF-linked cybercrime and AI-enhanced PF, proliferators have increasingly exploited overseas IT and digital labour arrangements, with the DPRK being specifically renowned for this type of PF. By deploying state-linked workers under false identities to secure remote roles abroad, foreign income is generated through legitimate employment that can directly contribute to the funding of WMD programmes. However, depending on the company, the ramification of hiring one of these workers can be far more detrimental. Firms that operate within sensitive sectors like defence, finance, energy and infrastructure can provide further opportunity for exploitation. While initial output by the employee may seem in line with their role, over time these agents can be strategically infiltrating systems, extracting confidential information and embedding code in order to compromise international security or initiate economic risk.

37. FATF - Cyber-Enabled Fraud: Digitalisation and Money Laundering, Terrorist Financing and Proliferation Financing Risks (2026).
38. https://www.rusi.org/explore-our-research/publications/commentary/beware-robots-ai-enabled-sanctions-evasion-here.
39. Saudi Arabia - Ministry of Foreign Affairs - Proliferation Financing Typologies and Red Flag Indicators (2026).

Typologies

The following typologies provide fictitious examples of potential Isle of Man exposure to PF. These examples are not exhaustive; however, associated red-flag indicators are included for each typology to illustrate how regulated entities may identify suspicious activity potentially linked to PF.

The typologies are not listed in order of likeliness or impact. All of the typologies outline a potential genuine risk to the Isle of Man. As the Isle of Man has had no criminal investigations linked to PF as of the publication of this report, the typologies below have been drawn from:

- Suspicious Activity Reports (SARs) received by the Isle of Man FIU.
- Open-source intelligence and adverse media.
- Adaptations of relevant international case studies, tailored to the Isle of Man's sectors.
- FATF and other FIU publications, highlighting emerging PF methodologies.
- Consultation with industry stakeholders, regulators and law enforcement.

Typology 1 — The Acquisition of Dual-Use Items by a Company

Grey Company, an Isle of Man-registered trading company, was incorporated through a local TCSP and maintained a bank account with an Isle of Man-regulated bank, Black Bank. Shortly after incorporation, Grey Company received several incoming wire transfers from corporate entities incorporated in jurisdictions neighbouring a country of proliferation concern. The payments were fragmented and originated from entities with no apparent commercial relationship to Grey Company.

Immediately after receipt, Grey Company placed a large order with Scarlet Company, a manufacturer of dual-use industrial equipment in Jurisdiction A and identified itself as the consignee.

Black Bank determined that the transaction volume and payment activity were inconsistent with Grey Company's stated business profile and limited operating history. This triggered Black Bank to suspect that Grey Company may have been used as a front company, facilitating a trade transaction involving dual-use goods on behalf of an unidentified end-user connected to a country of proliferation or diversion concern. Black Bank submitted a SAR to the FIU outlining the suspicions.

Red Flags

⇒ **Customer activity does not match business profile.**

⇒ **Fragmented funding by third parties not commercially linked to the transaction.**

⇒ **Funds received from countries of proliferation or diversion concern.**

⇒ **The immediate pass-through of funds to acquire dual-use items.**

Typology 2 — Professional Service Providers and Sanctions Evasion

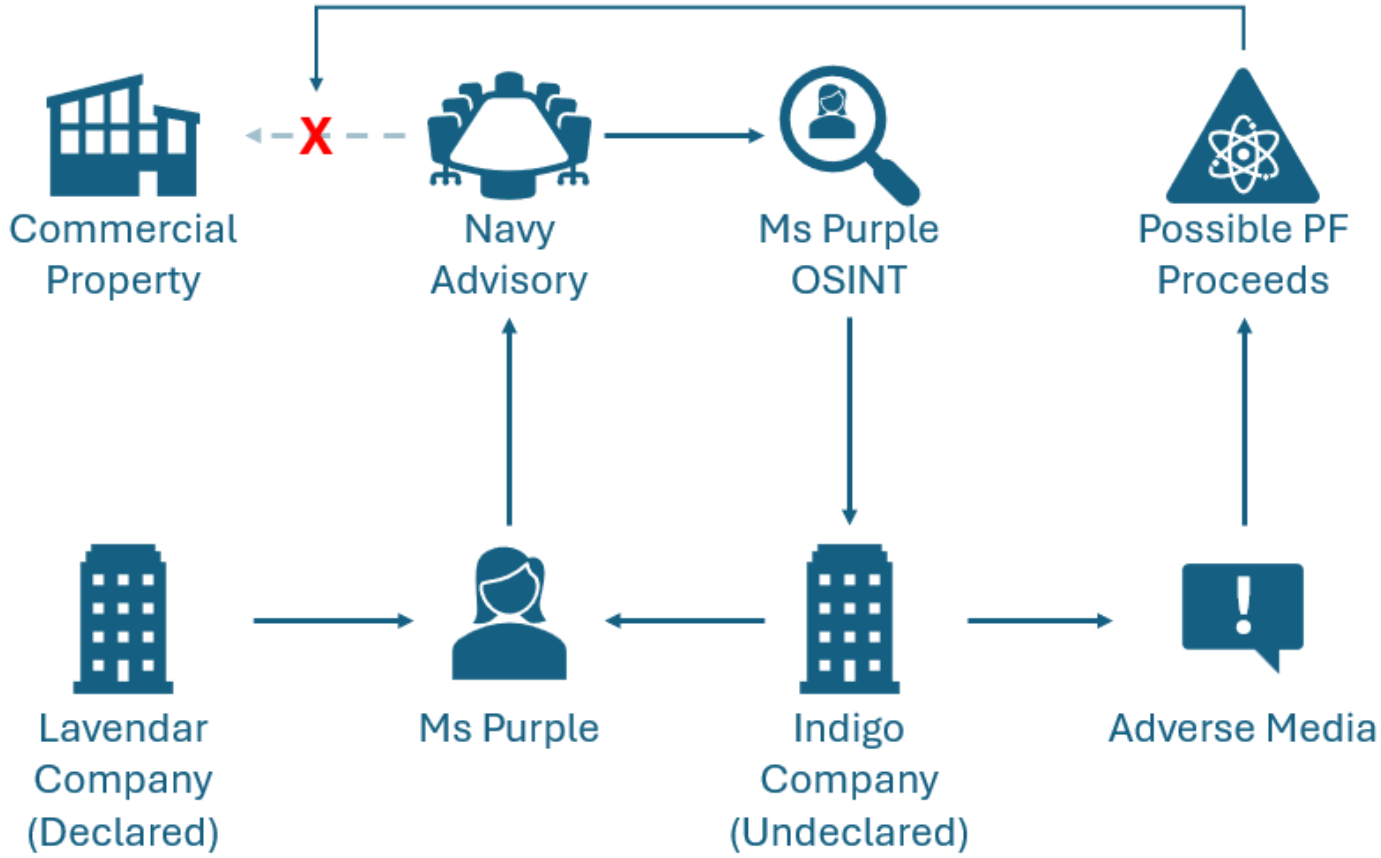
Navy Advisory, an Isle of Man-based professional services firm, was engaged to provide legal and transactional support to Ms Purple in the acquisition of a large commercial property on the Island.

During client onboarding, Ms Purple provided documentation declaring herself as the ultimate beneficial owner of Lavender Company, an overseas entity incorporated in a neighbouring jurisdiction, which was presented as the vehicle involved in the transaction.

Given the cross-border nature of the structure and the value of the proposed acquisition, Navy Advisory undertook risk-based onboarding and background checks on Ms Purple. These checks identified that she was also a director of Indigo Company, a manufacturing business, which had not been disclosed during onboarding.

Subsequent open-source and adverse media searches identified allegations that Indigo Company had acted as a supplier of dual-use goods to Jurisdiction F as part of a wider proliferation supply chain.

Although Ms Purple, Lavender Company and Indigo Company were not designated under any applicable sanction regimes, Navy Advisory refused the business. Navy Advisory submitted a SAR to the FIU stating that the undisclosed corporate association and adverse reporting raised concerns that the funds to be used in the transaction could represent value generated from, or associated with, proliferation-related activity.



Red Flags

⇒ **High-value real-estate acquisition supported by funds of unclear origin.**

⇒ **Failure to disclose corporate associations during onboarding.**

⇒ **Adverse media connecting a potential client to proliferation-related activity.**

Typology 3 – Nominee Directorship for Sanctions Evasion

Emerald TCSP, based in the Isle of Man, was approached to incorporate and provide registered office services to Green Company, which proposed to operate as a VASP. During onboarding, Green Company nominated Ms Silver as its sole director and ultimate beneficial owner. Ms Silver provided identity documentation and background information that appeared valid.

Open-source checks conducted by Emerald TCSP identified that Ms Silver had a limited digital footprint and professional history, inconsistent with the senior role described. Corporate records obtained from overseas registries showed that, prior to incorporation in the Isle of Man, Green Company formed part of an overseas group structure in which a Mr Pink was listed as the person with significant control.

Initial sanctions screening carried out by Emerald TCSP did not identify any adverse listings relating to Mr Pink. However, during a subsequent periodic review utilising enhanced screening tools and updated sanctions data, a variant spelling of Mr Pink's name was matched to an individual designated under a neighbouring jurisdiction's proliferation-related sanctions.

Upon discovery, Emerald TCSP submitted a SAR to the FIU stating they suspected that Ms Silver may have been acting as a nominee director, enabling Mr Pink to retain effective control over Green Company while circumventing sanctions restrictions.

Red Flags

- ⇒ **Individual appears to lack the experience expected for their role.**
- ⇒ **Name spelling variations or aliases across records that impede sanctions screening.**
- ⇒ **Controlling ownership traced to a sanctioned PF-linked individual.**

Typology 4 – Maritime Consultancy and High-Risk Vessel Operations

Beige Corporate Services, an Isle of Man-based corporate service provider, incorporated Crimson Company, which stated its business purpose as general maritime consultancy. Shortly after incorporation, Crimson Company entered into commercial management arrangements in respect of an ageing oil tanker and facilitated the application for the vessel's registration.

Following registration, the vessel began exhibiting high-risk operational behaviour, including extended periods of AIS disablement, irregular voyage patterns and repeated activity near known ship-to-ship transfer zones associated with sanctions-evasion activity.

This behaviour was identified through post-registration monitoring by the Isle of Man ship registry and relevant intelligence alerts. As this was consistent with known maritime sanctions-evasion practices commonly employed by PF networks, the registry communicated their concerns to Beige Corporate Services and shared intelligence with the Isle of Man's FIU.

This initiated a re-review of Crimson Company's onboarding information and ownership declarations by Beige Corporate Services.

The re-review identified inconsistencies between the vessel's high-risk operational behaviour and the company's stated role as a maritime consultancy. Beige Corporate Services submitted a SAR to the FIU.

Red Flags

- ⇒ **A company is incorporated with a generic or non-specific maritime business purpose.**
- ⇒ **A vessel exhibiting high-risk operational behaviour.**
- ⇒ **Patterns of vessel activity consistent with known maritime sanctions-evasion practices.**
- ⇒ **Inconsistencies between a company's stated activities and the vessel's observed operations.**

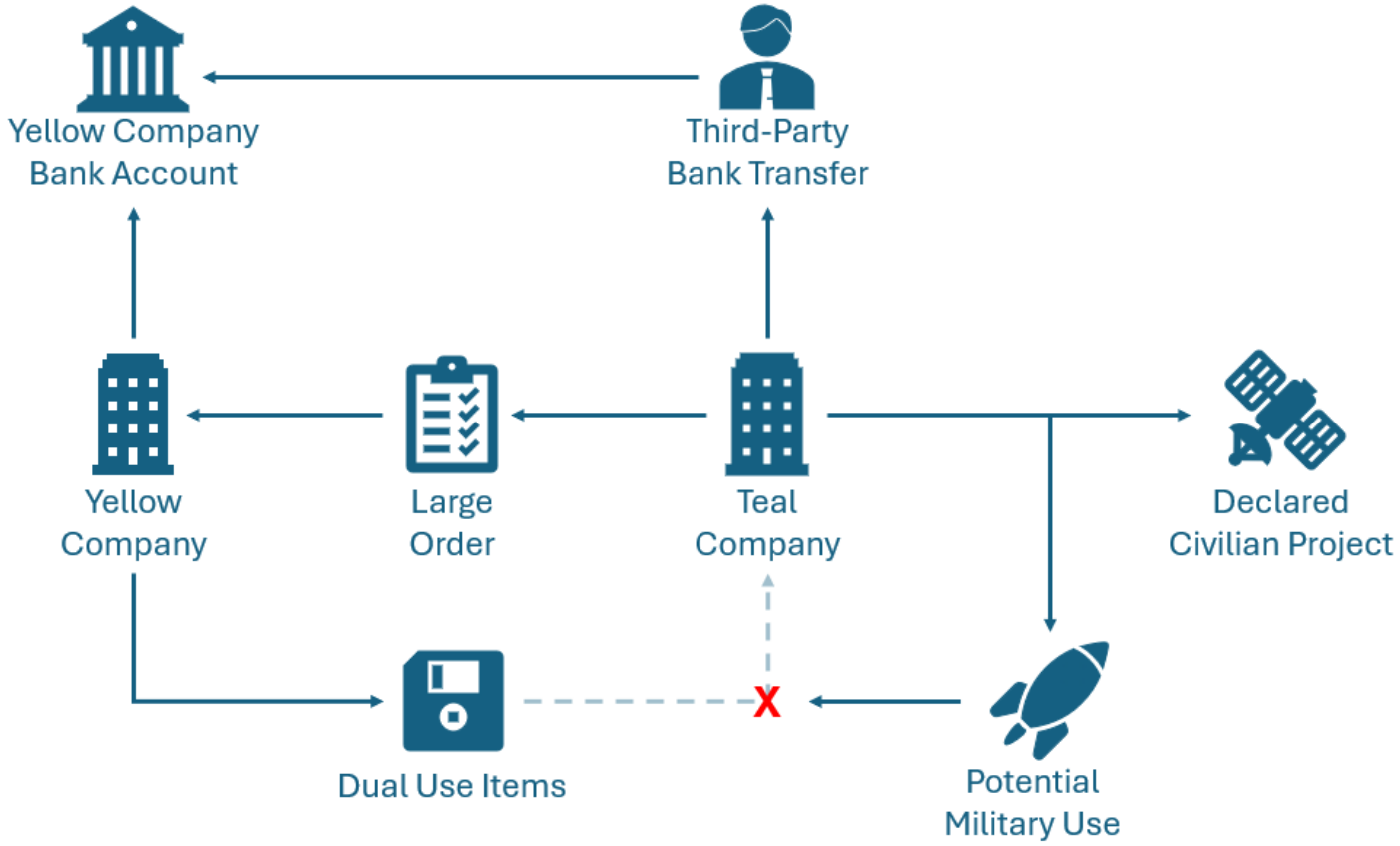
Typology 5 – An Isle of Man-Based Manufacturer of Dual-Use Items

Yellow Company, an Isle of Man-based manufacturer, produced specialised electronic components that were classified as dual-use goods due to their potential military and missile-guidance applications. Yellow Company exported its products globally and maintained accounts with an Isle of Man-regulated bank.

Yellow Company received an order from Teal Company, incorporated in Jurisdiction B, a country purported to be a PF-enabler, for a quantity of components significantly larger than Yellow Company had previously supplied to customers in that market. Teal Company stated that the goods were intended for civilian navigation projects and provided standard commercial documentation in support of the transaction.

The proposed deposit for the order was to be received into Yellow Company's Isle of Man domiciled bank account from a third-party entity, rather than directly from Teal Company. No clear commercial rationale was provided for the use of a third-party payer, which was inconsistent with Yellow Company's typical export arrangements and customer risk profile.

Although the proposed transaction pathway did not necessarily breach applicable trade restrictions, the combination of Jurisdiction B's reputation as a possible PF-enabler, the nature of the goods and the opaque payment arrangements meant that Yellow Company declined the business. While Yellow Company was not obligated to report this activity as a trade company, they subsequently submitted a SAR to the FIU that aided an ongoing investigation.



Red Flags

- ⇒ **Overseas purchaser incorporated in a jurisdiction associated with allegations of PF-enabling.**
- ⇒ **An inconsistent order quantity for the customer's declared use.**
- ⇒ **Payment proposed via intermediaries rather than directly from the purchasing entity.**

Typology 6 – Insurance Policy as a Value-Transfer Mechanism

Orange Insurance, an Isle of Man-regulated life insurer, received an application for a high-value capital-redemption bond from Mr and Mrs Burgundy. The policy was established as a single-premium investment product with a long-stated investment horizon. The source of funds was declared as private wealth accumulated overseas.

Within a relatively short period, the policyholders requested an assignment of the bond to a foreign legal arrangement established in Jurisdiction E, a jurisdiction associated with PF risk and limited beneficial-ownership transparency. The early assignment was inconsistent with the stated long-term wealth-preservation objective and lacked a clear commercial or estate-planning rationale.

A re-review of the premium payment highlighted that this investment had been funded via a third-party intermediary, rather than an account held by the policyholders. Based on this information and the unusual behaviour of the Burgundys, although the transactions were executed within the contractual terms of the policy, Orange Insurance submitted a SAR to the FIU. The SAR outlined their suspicion that the insurance product may have been used as a mechanism to hold, transfer or reposition value in a manner consistent with sanctions evasion or potential PF activity.

Red Flags

- ⇒ **The relinquishment of a long-term product after a short period without a credible rationale.**
- ⇒ **Assignment of policies to an entity established in jurisdictions of proliferation concern.**
- ⇒ **Funding of insurance premiums by third parties that are not clearly linked to the policyholder.**

Typology 7 – Ransomware Attack by a PF-linked Cyber Group

Mint Capital, an Isle of Man-based investment holding company, was targeted by a ransomware attack carried out by a cyber group assessed in open-source reporting as being linked to Jurisdiction H, a proliferating state. The attack was initiated through an AI-generated phishing email containing a malicious attachment, which enabled unauthorised access to Mint Capital's network.

Following a period of reconnaissance, the attackers deployed ransomware, encrypted critical systems and exfiltrated sensitive data. A ransom demand was issued requiring payment in a privacy-enhancing virtual asset, to restore operations and avoid further data compromise.

Blockchain forensics indicated that the wallet address created for the ransom payment was linked to cyber networks associated with the internationally sanctioned Jurisdiction H. This state was known to use ransomware activity to generate revenue in support of its strategic programmes, including WMD development.

Due to the links with a PF network, Mint Capital did not pay the ransom, as doing so would have resulted in their breaching of international sanctions. Mint Capital immediately informed the police and submitted a SAR to the FIU.

Red Flags

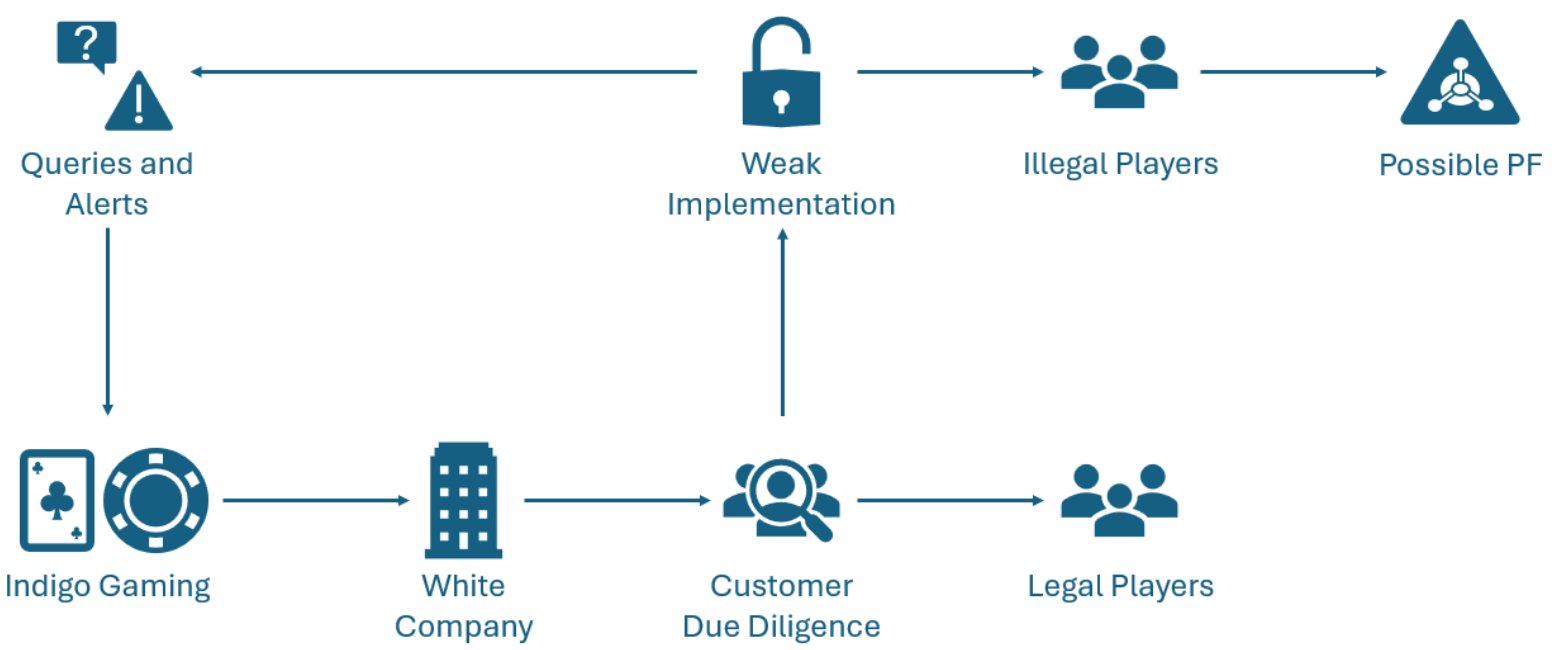
- ⇒ **Ransomware attacks claimed by cyber groups linked to a proliferating jurisdiction.**
- ⇒ **Ransom demands payable in privacy-enhancing virtual assets.**
- ⇒ **Wallet addresses provided for ransom payments associated with jurisdictions of proliferation concern.**

Typology 8 – e-Gaming Network Services Provider Customer Risk

Indigo Gaming , an Isle of Man-licensed network services provider, supplied its gaming platform and support services to White Company, an overseas gambling operator incorporated in Jurisdiction C. Under the commercial arrangement, White Company was responsible for conducting AML/CFT measures including customer due diligence and enforcing jurisdictional access restrictions.

Over time, Indigo Gaming received compliance queries and operational alerts indicating that White Company's platform was routinely accessed by individuals residing in Jurisdiction D, a country of proliferation concern, despite White Company's assurance that customers from that jurisdiction were restricted. Further review showed that White Company had limited geofencing controls and weak customer screening, allowing indirect access through VPNs and third-party payment methods.

Indigo Gaming suspected that White Company's platform could have been used to generate or process revenue derived from sanctioned or proliferation-linked jurisdictions, which, combined with weak customer screening, significantly increased the risk of serving actual designated persons. Indigo Gaming submitted a SAR on that basis following the termination of the business arrangement.



Red Flags

⇒ **The customer applies insufficient or ineffective customer due-diligence and sanctions-screening controls.**

⇒ **Limited visibility over how customers implement sanctions, jurisdictional restrictions, or PF-related controls.**

⇒ **Operator located in a jurisdiction with weak AML/CFT/CFP controls and a limited awareness PF risk.**

Typology 9 – Reinsurance Arrangements Enabling Maritime PF Risk

Cobalt Reinsurance, an Isle of Man-regulated captive reinsurer, provided excess-of-loss reinsurance coverage to a foreign maritime insurer through an international reinsurance programme. The cedant insurer underwrote a portfolio of commercial vessels operating globally, including oil tankers.

Before the reinsurance contract was agreed, information provided by the cedant insurer and the broker facilitating the reinsurance arrangement indicated that the underlying risks were low to moderate. No sanctions concerns were identified through standard screening; however, Cobalt Reinsurance did not have direct visibility over individual vessel operations.

During the reinsurance period, external maritime intelligence reporting indicated that certain vessels within the cedant's portfolio were operating along high-risk trade routes and calling at ports associated with sanctions-evasion activity and restricted trade. The cedant insurer did not proactively disclose these developments to Cobalt Reinsurance.

Following a review triggered by market intelligence, Cobalt Reinsurance assessed that its reinsurance coverage may have enabled the operation of vessels engaged in high-risk maritime activity, potentially exposing them to PF risk. Cobalt Reinsurance issued an immediate Notice of Cancellation to the cedant insurer and submitted a SAR to the FIU.

Red Flags

- ⇒ **Vessels operating on high-risk trade routes and ports.**
- ⇒ **Vessels engaging in behaviour that is inconsistent with the established risk profile.**
- ⇒ **Market reporting indicating an elevated sanctions-evasion risk.**
- ⇒ **Failure to disclose unexpected vessel behaviour by the cedant insurer.**

Typology 10 – Remote IT Workers for Fund Generation

Magenta Digital, an Isle of Man-based technology company, advertised a remote IT role through an online recruitment platform. Mr Gold applied using a professional online profile supported by identity documents that appeared valid. A virtual interview was conducted and despite minor delays in Mr Gold's responses, he was offered the position.

Shortly after onboarding, Mr Gold reported an urgent family matter and requested that company-issued equipment be sent to a new location, Jurisdiction G, that did not match the details provided during recruitment. Mr Gold continued to access corporate systems remotely and appeared to perform his role as expected.

Over time, Magenta Digital identified unusual technical activity associated with Mr Gold's account, including excessive login times, access patterns inconsistent with use by a single individual and activity occurring outside of expected working hours. Magenta Digital subsequently became aware of news reports describing how certain proliferating states use remote employment and false identities to generate foreign income in support of sanctioned programmes.

A subsequent internal review assessed Mr Gold's employment and resulted in the termination of their contract. Magenta Digital submitted an SAR to the FIU stating their suspicions of Mr Gold as a remote IT worker with links to a PF State.

Red Flags

- ⇒ **Requests by newly onboarded remote employees to change their declared location.**
- ⇒ **Unusual system-access behaviour inconsistent with a single employee account.**
- ⇒ ***BEWARE OF:* Subtle video anomalies in a virtual interview consistent with AI-based face swapping.**

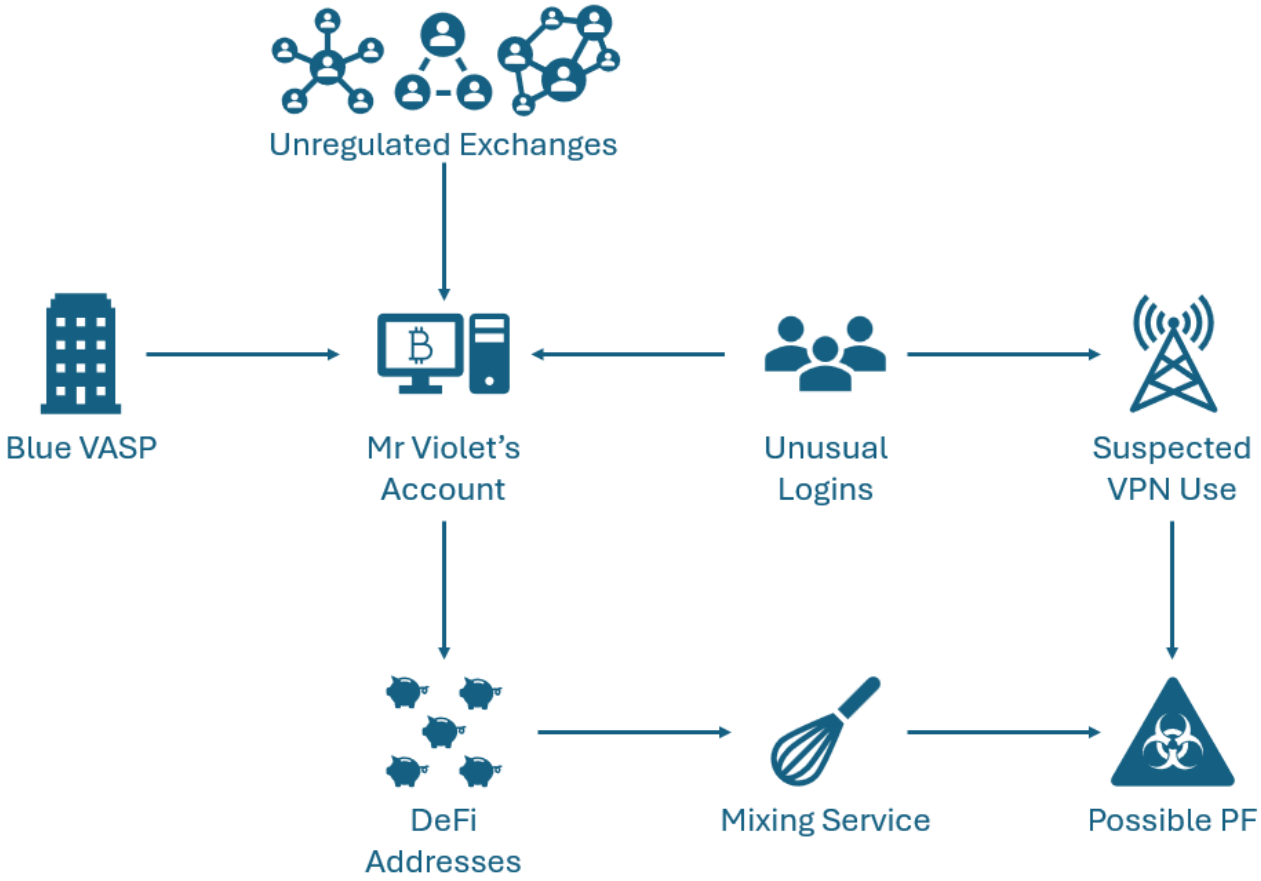
Typology 11 – Virtual Asset Services and Transactions

Mr Violet opened an account with Blue VASP, a VASP registered in the Isle of Man. This was stated to be a personal account. Customer due diligence was provided and appeared valid at onboarding.

Shortly after activation, the account received a large volume of stablecoins from several unregulated exchanges known to deal in privacy-enhancing coins, such as Monero. Once received, the stablecoins were converted to Bitcoin and quickly transferred from Mr Violet's account to a number of decentralised finance (DeFi) addresses. The Bitcoin was subsequently passed through a mixing service, further obscuring the origin of the funds.

An internal investigation, conducted by Blue VASP, identified that the account was accessed across multiple devices via a number of Isle of Man IP addresses in close succession, suggesting use by more than one individual. The investigation also revealed an anomalous transaction that was traced to an IP address located in a sanctioned proliferating state. Blue VASP assessed that this was unlikely to be incidental and instead indicated the use of a Virtual Private Network (VPN) to disguise the true geographic location of the other transactions.

This geographic indicator, combined with the suspicious speed, complexity and opacity of the transactions, resulted in Blue VASP enacting an immediate account freeze. Blue VASP submitted a SAR which outlined that Mr Violet's account was likely used as a drop account that could have been used to facilitate sanctions evasion and proliferation-financing activity.



Red Flags

- ⇒ **Account access from multiple devices suggesting shared or proxy control.**
- ⇒ **Receipt of funds from unregulated exchanges associated with privacy-enhancing coins.**
- ⇒ **Transactions inconsistent with the customer's expected activity.**
- ⇒ **Use of a mixer to obscure transaction trails.**
- ⇒ **IP address anomalies suggesting VPN use and geographic links to a high-risk neighbouring jurisdiction.**

Conclusion

The typologies presented demonstrate the diversity of potential PF methodologies relevant to the Isle of Man. While the jurisdiction's regulatory framework is robust, PF risks persist due to the complexity of international financial transactions, the adaptability of proliferators to exploit legitimate sectors and the continuous development of obfuscation tools and techniques.

The FIU encourages all regulated entities to maintain awareness of PF indicators and sector-specific vulnerabilities, to undertake robust customer due diligence and enhanced due diligence where required and promptly report suspicious activity to the FIU.

Continued vigilance, intelligence sharing and industry collaboration remain essential to protecting the Isle of Man's financial system from abuse.

Contacting the FIU

If you have queries in relation to this typology report, or wish to discuss matters arising from its content, you may contact the FIU for guidance. The FIU can be contacted by telephone on +44 (0)1624 686000 or by email at fiu@gov.im. General information, guidance and access to the online reporting system (THEMIS) are available via the FIU website at www.fiu.im.

To note: When submitting a SAR that relates to PF, it is necessary for the submitter to categorise the suspected criminality as 'Proliferation Financing' regardless of the legislation that it is submitted under.

Suspected breaches, or attempted breaches, of Isle of Man, United Kingdom or United Nations financial sanctions (including dealings with designated persons or frozen assets) must be reported to the FIU as soon as practicable. Where relevant, disclosures should include designation details, unique identifier references, and information concerning ownership and control. Updated guidance on sanctions reporting can be accessed via the FIU's website or the following link: https://www.fiu.im/sanctions/.

Information relating to other sanctions regimes, such as OFAC designations, or intelligence of relevance to the FIU where no suspicion has yet been formed, may be disclosed under Section 24 of the Financial Intelligence Unit Act 2016. Section 24 disclosures may be made by any person for the purpose of assisting the FIU in exercising its statutory functions, noting that suspicious activity from the regulated sector must still be reported under POCA and/or ATCA as appropriate.

Suspicious activity relating to money laundering or suspected criminal property must be reported under the Proceeds of Crime Act 2008 (POCA), using the appropriate reporting option within THEMIS. Where the same matter has been reported to another jurisdiction, this should be clearly stated within the disclosure narrative.

Where a person or business knows, suspects, or has reasonable grounds to suspect that a terrorist financing offence is being committed, or that funds are linked to terrorism, they must make a disclosure under the Anti-Terrorism and Crime Act 2003 (ATCA). In urgent or live situations, reporters are encouraged to telephone the FIU without delay in advance of, or in parallel with, submitting a disclosure via THEMIS.

The FIU encourages early engagement where uncertainty exists regarding reporting obligations and reminds all sectors that timely, accurate, and high-quality disclosures are essential to protecting the integrity of the Isle of Man's financial system.

Glossary

AI	Artificial Intelligence
AML	Anti-Money Laundering
ATCA	Anti-Terrorism and Crime Act
CPF	Counter-Proliferation Financing
CTBT	Comprehensive Nuclear-Test-Ban Treaty
CTF	Counter-Terrorist Financing
DeFi	Decentralised Finance
DPRK	Democratic People's Republic of Korea
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
HMRC	His Majesty's Revenue and Customs
IFC	International Financial Centre
IRGC	Islamic Revolutionary Guards Corp
ML	Money Laundering
NATO	North Atlantic Treaty Organization
NRA	National Risk Assessment
PF	Proliferation Financing
PF-TFS	Proliferation Financing Targeted Financial Sanctions
POCA	Proceeds of Crime Act
SAR	Suspicious Activity Report
TCSPs	Trust and Corporate Service Providers
TF	Terrorist Financing
UK	United Kingdom
UN	United Nations
UNSCRs	United Nations Security Council Resolutions
VASPs	Virtual Asset Service Providers
VPN	Virtual Private Network
WMD	Weapons of Mass Destruction

Definitions

Malign Actor

A malign actor is an individual, group, or state entity that deliberately engages in harmful, deceptive, or coercive actions designed to undermine laws, destabilise societies, or attack institutions.

Advanced Malware

A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system.[40] Advanced malware strains are engineered with advanced capabilities.

Backdoors

A backdoor attack is a way to access a computer system or encrypted data that bypasses the system's customary security mechanisms.[41] A custom backdoor has been developed or modified specifically for a particular operation, victim, or threat actor.

Ransomware

Malware that encrypts data and demands payment for decryption.[42]

Social Engineering

Tactics that exploit human behaviour to gain unauthorised access to sensitive information.[42]

Spear-Phishing

Sending emails to targeted individuals that could contain an attachment with malicious software, or a link that downloads malicious software.[43]

Zero Day Vulnerabilities

The use of malicious code that takes advantage of software vulnerabilities (or bugs) that are not yet known to vendors or anti-malware companies.[43]

40. https://www.eac.gov/sites/default/files/document_library/files/Glossary_Cybersecurity_Terms%28v.2.0%29.pdf.
41. https://www.techtarget.com/searchsecurity/definition/back-door.
42. https://www.sans.org/security-resources/glossary-of-terms/cyber-attack.
43. https://www.ncsc.gov.uk/sites/default/files/documents/common_cyber_attacks_ncsc.pdf.

Resources and Links

Reference Number	Resource
1	https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf.coredownload.inline.pdf
2	https://www.gov.uk/government/publications/uk-strategic-export-control-lists-the-consolidated-list-of-strategic-military-and-dual-use-items-that-require-export-authorisation
3	https://www.cnas.org/publications/reports/the-financing-of-nuclear-and-other-weapons-of-mass-destruction-proliferation
4 & 12	https://static.rusi.org/guide-to-conducting-proliferation-risk-assessment-2024.pdf
5 & 8	https://assets.publishing.service.gov.uk/media/65a01397e96df50014f844fe/Risk_assessment_of_proliferation_financing__1_.pdf
6	https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Complex-PF-Sanctions-Evasions-Schemes.pdf.coredownload.inline.pdf.
7	https://static.rusi.org/20190513_guide_to_conducting_a_national_proliferation_financing_risk_assessment_web.pdf.
9	https://www.nato.int/en/what-we-do/deterrence-and-defence/weapons-of-mass-destruction
10	https://main.un.org/securitycouncil/en/content/resolutions-0
11 & 13	https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Complex-PF-Sanctions-Evasions-Schemes.pdf.coredownload.inline.pdf
14	https://www.belfercenter.org/publication/north-koreas-oct-9-nuclear-test-successful-or-failed.
15 & 21	https://home.treasury.gov/system/files/136/2024-National-Proliferation-Financing-Risk-Assessment.pdf
16	https://ipdefenseforum.com/2025/05/north-koreas-shadow-economy-fueled-by-illicit-activities/#:~:text=North%20Korea's%20cyber%20capabilities%20have,stolen%20funds%20through%20complex%20networks
17	https://www.cyfirma.com/research/dprk-sanctions-violations-in-cyber-operations-post-un-panel-demise/
18	https://www.eia.gov/international/analysis/special-topics/World_Oil_Transit_Chokepoints
19	https://www.eia.gov/todayinenergy/detail.php?id=65584
20	https://www.ft.com/content/02aefac4-ea62-48db-9326-c0da373b11b8?syn-25a6b1a6=1
22	https://www.csis.org/analysis/russias-latest-nuclear-saber-rattling-nuclear-testing
23	https://press.un.org/en/2023/sgsm22022.doc.htm
24	https://cepa.org/article/russias-year-of-truth-the-missing-military-hardware/

Resources and Links

Reference Number	Resource
25	https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/09/pub25-094-tracking-the-components-of-missiles-and-uavs-used-by-russia-in-ukraine.pdf
26	https://platform.opennuclear.org/thoughtroom/external-contributions/russia-the-iran-nuclear-programme-and-the-degradation-of-non-proliferation-norms-and-tools
27	https://finance.ec.europa.eu/document/download/ae2e63e2-4c4d-4f77-9757-c408ddbcede1_en?filename=240924-preventing-russian-export-control-sanctions-evasion%20.pdf.
28	https://www.csis.org/analysis/parading-chinas-nuclear-arsenal-out-shadows.
29	https://www.researchgate.net/publication/345436280_Sino-Iranian_Oil_Investment_Current_Status_Analysis_and_Countermeasure_Research.
30	https://www.csis.org/analysis/parading-chinas-nuclear-arsenal-out-shadows
31	https://www.bruegel.org/analysis/what-war-iran-means-china
32	https://www.kcl.ac.uk/news/north-koreas-proliferation-illicit-procurement-apparatus-within-china
33	https://undocs.org/S/2021/211
34	https://c4ads.org/blogposts/against-the-grain
35	https://publications.parliament.uk/pa/cm201919/cmselect/cmfaff/109/109.pdf
36	ISIL: https://news.un.org/en/story/2023/06/1137492 Aum Shinrikyo: https://www.cwccoalition.org/events/anniversaries/tokyosubwaysarinattack30th/ Al-Qaeda: https://ctc.westpoint.edu/reevaluating-al-qaidas-weapons-of-mass-destruction-capabilities/
37	https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Cyber-Enabled-Fraud%E2%80%93Digitalisation-and-ML-TF-PF-Risks.pdf.coredownload.inline.pdf
38	https://www.rusi.org/explore-our-research/publications/commentary/beware-robots-ai-enabled-sanctions-evasion-here
39	https://mc.gov.sa/en/guides/pages/default.aspx
40	https://www.eac.gov/sites/default/files/document_library/files/Glossary_Cybersecurity_Terms%28v.2.0%29.pdf.
41	https://www.techtarget.com/searchsecurity/definition/back-door.
42	https://www.sans.org/security-resources/glossary-of-terms/cyber-attack.
43	https://www.ncsc.gov.uk/sites/default/files/documents/common_cyber_attacks_ncsc.pdf.