防制洗錢金融行動工作組織（FATF）報告

複雜的資武擴和規避制裁手法

2025 年 6 月

防制洗錢金融行動工作組織（FATF）係一獨立之政府間機構，專責制定並宣導政策，以保護全球金融體系免受洗錢、資恐及資助大規模毀滅性武器擴散之威脅。FATF 建議已被公認為全球防制洗錢（AML）及打擊資恐（CFT）的國際標準。

欲瞭解更多有關防制洗錢金融行動工作組織的資訊，請參閱 **www.fatf-gafi.org**
本文件和／或其中包含的任何地圖均不影響任何領土的地位或主權、國際邊界和邊界的劃定以及任何領土、城市或地區的名稱。

參考文獻：

FATF（2025），*複雜的資武擴和規避制裁手法*，FATF, 巴黎，https://www.fatf-gafi.org/content/fatf-gafi/en/publications/complex-proliferation-financing-sanctions- evasion-schemes.html

圖片來源封面照片：Sergey Nivens/Shutterstock.com

縮寫和首字母縮略詞

AML／CFT 防制洗錢／打擊資恐

AEC 匿名性增強的加密貨幣

AIS 自動辨識系統

APT38 進階持續性威脅 38

UBOI 最終實質受益權資訊

CBDC 中央銀行數位貨幣

CDD 客戶盡職調查

CPF 打擊資武擴

CVC 可兌換虛擬貨幣

DeFi 去中心化金融

DNFBP 指定之非金融事業或人員

DPRK 北韓

EDD 加強盡職調查

FIs 金融機構

FTB 外貿銀行

FTZs 自由貿易區

GECC 全球出口管制聯盟

IMO 國際海事組織

INR 建議註釋

IRGC 伊斯蘭革命衛隊

ML／TF 洗錢／資恐

MVTS 金錢或價值移轉服務

NRA 國家風險評估

OTC 場外交易

PF 資武擴

PoE 專家小組

P2P 點對點

PPPs 公私部門合作機制

RGB 偵查總局

SARs／STRs 可疑活動／交易報告

SRB 自律團體

TCSP 信託和公司服務業者

TFS 目標性金融制裁

UN 聯合國

UNSC 聯合國安全理事會

UNSCR 聯合國安全理事會決議

VASP 虛擬資產服務提供商

WMD 大規模毀滅性武器

1. 執行摘要

大規模毀滅性武器（WMD）之擴散及其資助活動，對全球安全及國際金融體系的穩定與完整性構成嚴重威脅。若公私部門未能強化技術遵循和執行效能，具高度複雜性的國家及非國家行為者將持續利用打擊資武擴（CPF）體系之監控弱點。由於 WMD 可能造成災難性影響，防止並打擊對這種非法活動的資助至為關鍵。

近年來，與資武擴（PF）及規避制裁相關的手法日益複雜，已成為全球金融體系的重要威脅之一。根據 FATF 之授權，本報告分析相關方法與趨勢，並且支援國家、區域及全球層級之威脅與風險評估。本研究詳述為規避與 PF 相關目標性金融制裁（TFS）人士所採用之技術（依據 FATF 建議第 7 項之要求），以及超出該建議範疇之外、涉及其他制裁制度（如國家或超國家制裁）之規避情形。

本研究旨在提供對於威脅與弱點之最新理解，揭示其間共同挑戰，並指出主要執法困難與良好實務，協助各國強化 PF 風險評估與風險抵減措施。本報告所採用的整合架構，並非為重新定義建議第 7 項之義務，亦非意圖導致或促進任何國家或超國家制裁制度之認可。[1]

FATF 評估認為，與 PF 和規避制裁相關之持續演變的**威脅與弱點**，對公私部門皆構成重大挑戰。當前風險環境特徵為：國家及非國家行為者透過使用採購網路來取得和／或採購兩用貨品、技術與專業知識。根據當前全球 PF 威脅，FATF 全球網路認為北韓為最主要參與者之一，並受聯合國制裁及 FATF 標準約束。

雖目前尚無普遍認可之估算數據可反映 PF 所涉及之資金總額，然近年來北韓已多次利用國際金融體系為其 WMD 計畫籌集資金。例如，2025 年 2 月，ByBit 遭駭客攻擊，損失金額達 15 億美元。此外，北韓亦透過 IT 工作者、其他行業及非法活動獲取收入，以支援其 WMD 計畫。

另有部分國家亦涉及與伊朗及俄羅斯聯邦相關之規避制裁手法，該等手法不受聯合國擴散相關制裁之約束，亦不在 FATF 的 PF 風險之定義範圍內。鑑於對風險的理解程度不同，威脅行為者得以利用各國及部門層面之弱點來規避與 PF 相關的制裁（詳見第 I 節）。

不法分子正採取更複雜之手段來規避制裁並規避出口管制。根據 FATF 全球網路提交之資訊，本報告關注於**四大主要態樣**：尋求中介機構以規避制裁；掩蓋實質受益權資訊（BOI）以進入金融體系；運用虛擬資產和其他技術；以及利用海事與航運部門（詳見第 II 節）。為因應此類複雜行為，本報告亦就偵查、調查與起訴、國內協調及國際合作之**挑戰與良好實務**提出建議（詳見第 III 節）。

[1] 更廣泛的規避制裁框架並不會產生與建議第 1 項或 FATF 標準任何其他部分相關的任何新義務。相反地，FATF 態樣報告的目標是要支援公私部門依照其獨特情境來評估及降低風險。

本研究有助於 FATF 全球網路深化對複雜 PF 與規避制裁手法之理解，並提供權責機關與私部門使用之相關**風險指標**（詳見附件 A）。惟研究同時揭示需進一步強化全球對 PF 與規避制裁風險之共識。未來數年內，威脅行為者將繼續利用 CPF 控制體系之漏洞，包括規避司法差異、以新興科技為手段及地緣政治變遷所帶來之機會。

為預防並防制複雜 PF 與規避制裁手法，FATF 全球網路應考慮下列行動（詳見建議乙節）：

1) **定期更新對威脅、弱點與態樣之認知，**因各國及部門間之風險理解程度不同；
2) **加強資訊共享，以提升公私部門發現 PF 或規避制裁行為之能力，**尤其考量現行多依賴可疑活動報告（SAR）或可疑交易報告（STR）啟動調查；
3) **將 WMD PF 的官方定義添納入** FATF 通用詞彙，並於五年內完成，以克服司法管轄權差異對國際合作之阻礙；
4) **進行橫向審查，於三年內完成 FATF 全球網路之 PF 風險評估回顧，**協助各國根據風險評估結果制定更完善之良好實務。

2. 背景

FATF 標準和 PF 工作概述

1. 2020 年 10 月，FATF 修訂了建議第 1 項與建議第 2 項（R.1 與 R.2）及其建議註釋（INR.1 與 INR.2），要求各國、金融機構、指定之非金融事業或人員（DNFBPs）以及虛擬資產服務提供商（VASPs），應識別、評估並認知其資武擴風險，即可能違反、不履行或規避建議第 7 項中所規定之目標性金融制裁（TFS）義務之風險，並採取與所識別風險相稱且有效之風險抵減措施。修訂後之建議亦要求各國加強與 PF 風險相關之國家層級合作、協調及資訊共享機制。

2. 為協助公私部門利害關係人有效履行修訂後建議所規訂之義務，FATF 於 2021 [2] 年發布《資武擴風險評估及抵減指引》，其提供以下方面的指導：

    1) 公私部門應如何進行風險評估，以識別、評估並認知 PF 風險；
    2) 如何依 FATF 要求採取措施，以抵減已辨識之 PF 風險；
    3) 監理機關或自律個體應如何監督和監控 FIs、 DNFBPs 以及 VASPs 以確保能適當評估並降低 PF 風險。

3. 2021 年之指引為 2018 年《打擊資武擴指引》之補充文件 [3]，後者主要協助公私部門利害關係人根據 UNSCRs 理解並落實第 7 項規定之義務，並防範規避制裁行為。在此之前，FATF 曾於 2013 年發布《打擊資武擴指引-執行聯合國安全理事會決議之金融規定以打擊大規模毀滅性武器擴散》[4]。

4. 在上述指引發布之前，FATF 已辨識針對現有 PF 風險與 CPF 措施，並於 2008 年《資武擴態樣報告》[5] 以分享調查結果，強化全球對相關發展之理解。其後於2010 年發布《打擊資武擴：政策制定與諮詢現況報告》[6]，在前一份報告基礎上，進一步列出根據 UNSCRs 實施 CPF 措施時應考量之政策選項，特別是關於 i）法律制度、ii）公私部門間之資訊共享和認知提升、iii）預防措施，以及 iv）調查和起訴。

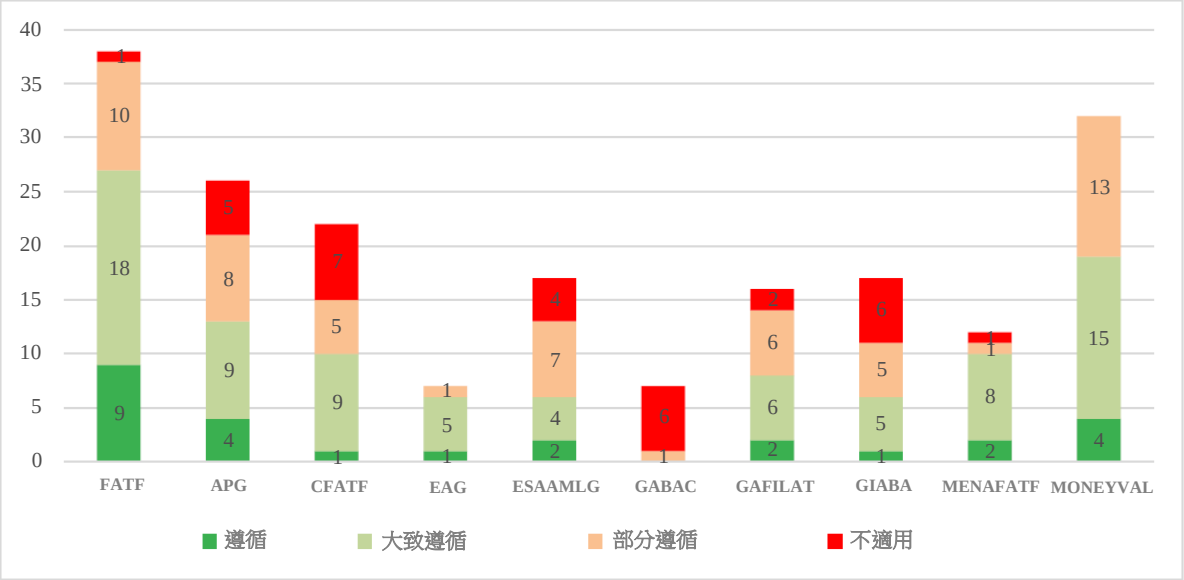
FATF 標準之現行實施狀況

5. 第 4 輪相互評鑑（ME）結果顯示，各國在遵守建議第 7 項（R.7）以及聯合國安全理事會決議（UNSCRs）有關擴散問題之決議實施與執行 TFS 方面，仍面臨挑戰。截至 2025 年 4 月 [7]，在 194 個 FATF 和 FSRB 成員國中，只有 13%（即26 國）評定為「遵循」於 R.7，而近半數（46%；共89 國）僅為「部分遵循」或「未遵循」。

---

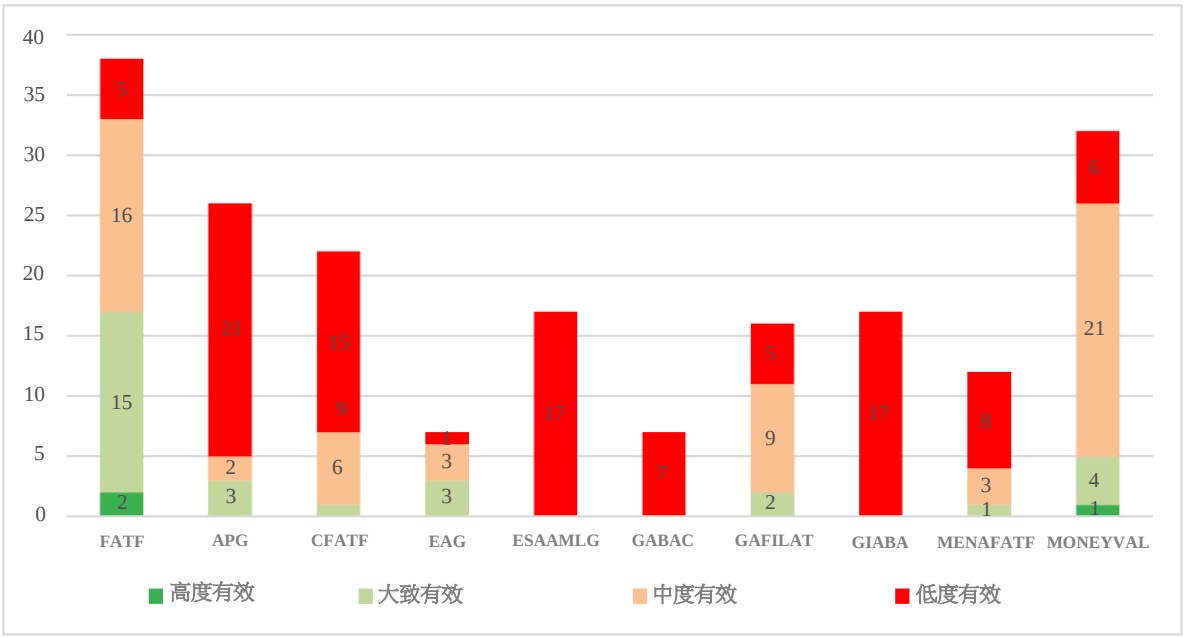
2 FATF（2021）《資武擴風險評估及抵減指引》
3 FATF（2018）《打擊資武擴指引》
4 FATF（2013）《打擊資武擴指引-執行聯合國安全理事會決議之金融規定以打擊大規模毀滅性武器擴散》
5 FATF（2008）《資武擴態樣報告》
6 FATF（2010）《打擊資武擴：政策制定與諮詢現況報告》
7 FATF（2024）綜合評估評級

圖 1. R.7 技術遵循評估結果（截至 2025 年 4 月）



6. 同樣地，整體之效能水準仍偏低，僅有 16% 之受評國家在 IO.11（即根據 UNSCRs 就擴散問題執行 TFS）中達到「高度有效」或「大致有效」評級。FATF 和 FSRB 成員國之間效能表現存在顯著差距：接受評鑑之 38 個 FATF 成員國中有 45% 獲得「高度／大致有效」評等，而接受評鑑之 156 個 FSRB 成員國中，僅有 10% 獲得相同評等。

圖 2. 直接成果 11：有效性評估結果（截至 2025 年 4 月）



前言

焦點概述

7. 本報告建構於以現有兩份主要指引之上，並予以更新：1）2018 年《打擊資武擴指引》– 有關實施 UNSCR 第 1718 號決議金融規範，以防止核武及其他大規模毀滅性武器（PFWMD）之擴散；2）2021 年《資武擴風險評估與風險抵減指引》。本報告旨在協助讀者全面瞭解與 PF 相關之複雜規避制裁手法態樣，並界定主要執法挑戰與良好實務，提供各國於進行 PF 風險評估及風險抵減措施時之參考。本報告運用下列關鍵術語：

方框 1. 關鍵術語定義

本報告採用 2021 年指引中所使用之廣義工作定義，該定義係以 2010 年狀況報告為基礎：

大規模毀滅性武器（WMD）擴散

指*製造、取得、擁有、開發、出口、轉運、經紀、運輸、轉移、儲存或使用核武、化學武器或生物武器及其運載工具與相關材料（包括用於非合法用途之兩用技術與兩用貨品）。*

資武擴（PF）

指籌集、轉移或提供全部或部分資金、其他資產或經濟資源，供個人或實體用於大規模毀滅性武器擴散，包括其運載工具與相關材料（含兩用技術與兩用貨品）之擴散。[8]

本報告重申，目前在國際機制與多邊論壇間，尚未對 WMD 擴散或 PF 形成統一標準定義；並於相關章節指出此一缺口之潛在影響及建立共同標準之必要性。

PF 風險

除非另有說明，根據修訂後之建議第 1 項及其註釋（R.1 和 INR.1），本報告嚴格且僅將 PF 風險定義為：嚴格且僅指可能違反、不履行或規避建議第 7 項中所述 TFS 義務之風險。

8. 本報告乃建構於各國及國際機構之廣泛研究與實務工作基礎上，旨在供 FATF 全球網路成員國使用，協助權責機關、金融機構（FIs）、指定之非金融事業或人員（DNFBPs）、虛擬資產服務提供商（VASPs）、非政府組織及其他相關實體，共同防制與 PF 相關之規避制裁行為。

[8] 這項 PF 工作定義是以 FATF 2010 年狀況報告中的定義為基礎，該定義對於本研究仍然具有相關性，特別是對於那些採取更廣泛方法來抵減與 PF 和規避制裁相關之風險的國家而言。2010 年的報告將 PF 定義為「提供資金或金融服務，全部或部分用於製造、獲取、擁有、開發、出口、轉運、經紀、運輸、轉移、儲存或使用核武器、化學武器或生物武器及其運載工具和相關材料（包括用於非合法目的之技術和兩用貨品兩者）的行為，違反國家法律或適用的國際義務。」

目標與架構

9. 本報告旨在提供與 PF 相關之規避制裁趨勢與方法的全球性觀點，目標在於協助各國抵減 PF 風險。本報告提供複雜的規避制裁手法、威脅與弱點之指標，並界定在偵查、調查及起訴與 PF 相關規避制裁案件方面之良好實務與主要挑戰。本報告之目標透過下列四項主要部分達成：

- **第一部分**：說明專案範疇之設定與實施計畫，並提供當前形勢之整體概述。此部分依據案例研究與文獻分析，識別出與規避制裁和 PF 相關的威脅和弱點。
- **第二部分**：提供與 PF 相關之複雜規避制裁手法之態樣概述。
- **第三部分**：說明在偵查、通報、調查及起訴 PF 相關規避制裁案件方面之挑戰與良好實務，並概述國內協調、合作及國際合作之各項機制。
- **結論和優先領域**：總結出整體的 PF 和規避制裁觀點，並且確定需要進一步開展工作的領域。
- **風險指標**：本附件旨在強化公私部門機構辨識與 PF 及規避制裁手法相關可疑交易及／或活動之能力。

方法論

10. 本報告之研究方法包括審查並細緻化現有關於 PF 及 PF 風險之可用資料，內容涵蓋：

- 透過文獻審查識別與 PF 相關的規避制裁之性質與範疇之演變趨勢，包括最近的 UNSCR 第 1718 號專家小組（POE）報告。此審查聚焦於威脅、弱點及新興趨勢與方法。
- 邀請 FATF 全球網路成員國提供與 PF 相關之規避制裁問題之意見。其中包括 a）策略性情報產品或案例研究，揭示與 PF 相關的規避制裁態樣及實例；b）風險評估與風險抵減措施中所辨識之威脅與弱點；c）偵查、調查及資訊共享機制；以及 d）良好實務與挑戰。
- 除 FATF 全球網路成員國所提交之風險指標外，另審查以下補充資料：i）他組織及機構所發布之 PF 風險評估指導，ii）PF 態樣研究，以及 iii）由各國發布之 TFS 指導。
- 鼓勵私部門、民間團體與學術界於公眾諮詢階段回覆若干問題，以協助本報告之內容完善，特別就國內協調與合作之挑戰與良好實務提供意見。

3. 第 1 節：規避與 PF 相關的制裁 – 現況、威脅與弱點

範疇

報告框架

11. 作為風險評估程序的一部分，各國會評估當相關威脅成功利用弱點而造成後果時所發生的洗錢（ML）、資恐（TF）以及資武擴（PF）風險。[9]根據 FATF 全球網路觀察，對國際金融體系最嚴重的 PF 威脅來自國家支援或附屬的行為者，包括但不限於與規避制裁及唯一受聯合國制裁之國家—北韓—相關聯的 PF 活動。

12. 在經修訂之 FATF 建議第 1 項的框架內，PF 風險嚴格且僅指可能違反、不履行或規避建議第 7 項所規定之 TFS 義務，其焦點僅集中於受聯合國制裁之國家（北韓）。基於此狹義定義的 PF 風險，各司法管轄區所識別之主要威脅行為者包括北韓，以及支援或與其合作規避聯合國制裁的國家行為者、個人與實體。

13. 正如 FATF 2021 年《國家洗錢風險評估指南》所述[10]，了解 WMD 擴散的更廣泛風險及其潛在資助，有助於理解與 FATF 之 PF-TFS 義務相關的風險，並支持以風險基礎方法的措施與 TFS 的落實。許多 FATF 成員國採用較 FATF 現行標準更廣的 PF 定義以降低更廣泛風險。因此，各司法管轄區提交的意見範圍反映出他們對目前全球 PF 威脅的理解，除了北韓（受聯合國制裁和 FATF 標準約束），亦包含其他國家行為者。許多國家將伊朗和俄羅斯聯邦視為當前 PF 威脅，縱使兩者未受到與擴散相關之聯合國制裁、亦未被 FATF 對 PF 風險之定義所涵蓋。

14. 本報告之範疇提供資武擴者所使用之複雜規避制裁手法的最新觀點，在相關情況下，亦更廣泛考量與 TF 和 PF 相關的規避制裁手法（無論制裁制度為何），以確保所提態樣具持續性與實用性，並回應共同挑戰。因此，本報告涵蓋所有司法管轄區最常提及之所有行為者，藉以協助 FATF 全球網路識別並抵減其 PF 風險。[11]

FATF 全球網路在 PF 風險評估方面的經驗

15. 評估相關弱點一項有效途徑，是執行 PF 風險評估。雖多數國家回覆已將 PF 風險納入或正納入其國家風險評估程序，惟跡象顯示對 PF 弱點之評估與／或理解仍處早期階段。例如，於本報告問卷之受訪國中，近半數未驗證是否存在 PF 弱點，另有六國認定不存在 PF 弱點。

---

9 FATF（2024）《國家洗錢風險評估指南》

10 FATF（2021）《資武器擴風險評估及抵減指引》

11 正如執行摘要和文件其他部分所述，本報告包含有關於用以逃避國家和超國家制裁制度之技術的資訊，藉以提供對威脅和弱點的最新瞭解，包括 FATF 標準建議第 7 項並未涵蓋的相關態樣之間的共同挑戰。更廣泛的規避制裁框架並非意圖重新定義建議第 7 項的要求。

16. 在若干情境下，各國呈現對 PF 和規避制裁之弱點程度較低，原因包括：與受制裁國家之地理距離；未與其維持外交或貿易關係；金融部門不發達且與全球金融市場整合有限；針對與 PF 相關的 TFS 有健全制度；管轄區內未發現 PF 案件。

17. 上述多屬可降低被濫用機率之正當因素。但需注意，近年全球環境因新技術（含新型支付系統）與地緣政治緊張而劇變；且前述因素未納入公私部門在 AML／CFT／CPF 控制面之更廣泛弱點，也未反映公私部門利用第三國各種中介機構規避制裁與出口管制之情形（見態樣 1）。由於 PF 威脅行為者熱衷於利用國際金融體系中之潛在盲點，因此可能需要更多支持及活動而識別和抵減 PF 弱點，並強化集體應對。

現況

18. 儘管針對 WMD 計畫已建立完備之國際、超國家與國家制裁制度及出口管制，國家支援或附屬的行為者仍持續以複雜採購和創收手法支援 PF 行為者和／或活動。具體而言，主要威脅行為者正招募第三國的中介、掩蓋 BOI、運用新技術以及利用海事和航運部門來規避制裁、籌集資金和獲取兩用貨品（詳見第 2 節）。

19. FATF 對當前威脅與弱點之整體判斷如下：

現況－北韓

20. 自 2006 年進行其首次核試以來，北韓即受國際制裁。2006 年通過的 UNSCR 第 1718 號決議要求北韓停止核試驗，並對涉 WMD 計畫之個人與實體採取廣泛制裁與其他反制措施。

21. 儘管遭受近 20 年制裁，北韓仍持續透過洲際彈道飛彈試射提升其載具能力。例如，2024 年 10 月 31 日發射之「火星-19」ICBM，高度約 7,000 公里、射程約 1,000 公里，為其自 2021 年宣布五年軍事擴張計畫以來第 11 次 ICBM 發射。[12]

22. 與此同時，國際社會之應對並未跟上威脅演變。近十年UN 對北韓的制裁名單未新增任何國家。且UNSCR 第 1718 號決議委員會的專家小組（POE）於 2024 年解散。此舉對監督北韓違反相關制裁造成重大挑戰。[13] 許多國家長期依賴 POE 的兩年期報告作為 PF 國家風險評估依據。FATF 於 2024 年 6 月 全會亦指出，POE授權終止已削弱各國取得可靠資訊以支持評估北韓相關 PF 風險。[14]

23. 本研究期間，FATF 代表團提出兩項加劇推升北韓 WMD 籌資能力之因素：其金融互聯互通性強化，以及收入來源多樣化。

強化的金融互聯互通

24. 儘管 FATF 自 2011 年以來屢次重申，所有國家都必須根據 UNSCR 決議堅決實施 TFS，並採取應對措施以保護其金融體系免受來自北韓非法金融侵害，該司法管轄區近年與國際金融體系之連結性有所增強，即如 FATF 於 2024 年 6 月所述者，[15] 相關 PF 風險隨之上升。

---

12 北韓最新飛彈發射對區域穩定構成「嚴重威脅」| 聯合國新聞

13 安全理事會未能延長協助制裁委員會處理民主朝鮮民主主義人民共和國 | 會議報導和新聞稿

14 《呼籲高風險國家採取行動 - 2024 年 6 月》

15 《呼籲高風險國家採取行動 - 2024 年 6 月》

25. 在「朝俄全面戰略夥伴關係條約」[16]於 2024 年底生效，兩國承諾強化合作，包括：為海關資助和銀行業務的經濟合作創造良好條件；共同努力為北韓與俄羅斯聯邦建立直接關係創造良好條件；促進各地區經濟和投資潛力的相互了解。加強經濟聯繫，特別是與北韓金融機構或與 PF 有關的實體重新建立銀行聯繫，可能會為全球金融體系帶來新的弱點，多家北韓金融機構及其海外代表已依 UNSCR 1718 系列決議列入制裁名單。[17]

26. 自 2016 年以來，由於東道國實施制裁和北韓人員撤離，接待北韓銀行業者的國家數自14 國降至 4 國（2023 年底自印尼與利比亞再度撤離）。惟 2023 年到至少 2024 年中，北韓在鄰國和俄羅斯的銀行業者促成了價值數億美元交易支援其貿易和創收。截至 2024 年中，儘管 UNSCR 2321 要求東道國驅逐北韓銀行代表，仍有逾 50 名代表在境外營運。[18]此外，UNSCR 2270 要求關閉既有代表處且禁止於成員國開設或營運新的分支機構、子公司或代表處國家的領域。[19]另有代表團指出，2024 年 1 月曾有俄羅斯銀行業者促成了北韓建築工人赴俄賺取外匯之交易，使其得以繼續規避 UN 制裁。

收入來源多樣化以支援 WMD 計畫

27. 許多國家報告稱，與 PF 和規避制裁計畫最相關之犯罪活動包括偽造、欺詐、（網路）盜竊以及販賣武器、毒品、野生動物、走私和其他物品。與北韓相關之個人與實體透過非法活動及合法企業，於 AML／CFT／CPF 控制薄弱或者未受管制之國家或行業，例如新技術、海事和航運業（詳見態樣 3 和 4）。近年來，北韓除了專注於利用 IT 人員創造收入外，還以針對各種行業或非法活動獲取收入而聞名，其中包括：

- **假髮及假睫毛行業**：若干國監測北韓藉出口高獲利之假髮和假睫毛增加財政收入並抵減對其戰略武器計畫之制裁。2024 年上半年，該類產品佔北韓對鄰國出口總額的近 60%。為了生產這些產品，北韓從同一鄰國進口原料來製造半成品，然後北韓再將其送回企業進行最終加工並出口到第三國。負責生產之北韓貿易公司隸屬於 UNSCR 第 1718 號決議所列實體，顯示收益可能支援其戰略武器計畫。雖 UN 制裁不禁止公司購買北韓原產的假髮和假睫毛，但是參與生產和購買最終產品之公司，可能並不知其與受制裁實體存在關聯。
- **非法野生動物貿易**：主要來自撒哈拉以南非洲，該區與北韓具歷史淵源。此為其低風險、高報酬之資金來源。隨著近年來北韓在該區外交存在下降，

16 http://en.kremlin.ru/acts/news/75534

17 聯合國指明的相關實體包括端川商業銀行（KPe.003）、東地銀行（KPe.013）、岩蘆江發展銀行（KPe.009）。

18 UNSCR 第 2321 號決議要求東道國採取積極措施，例如驅逐北韓銀行代表，並禁止其境內或受其管轄的個人或實體為與北韓的貿易提供公私人金融支援。

19 正如 FATF 在 2024 年 6 月關於高風險司法管轄區的聲明中所述，「自 2011 年以來，FATF 不斷重申，各國需要根據聯合國安全理事會決議，有力地實施目標性金融制裁，並採取以下對策，保護其金融體系免受來自北韓的洗錢、資恐和資武擴威脅：終止與北韓銀行的代理關係；關閉北韓銀行在其國家的任何子公司或分行；限制與北韓人員的業務關係和金融交易。儘管有這些呼籲，北韓仍加強了與國際金融體系的連結性，正如 FATF 在 2024 年 2 月指出，這會升高資武擴（PF）風險。這需要我們提高警惕，重新實施和執行針對北韓的反制措施。根據 UNSCR 第 2270 號決議，北韓經常利用前台公司、空殼公司、合資企業以及複雜、不透明的所有權結構來違反制裁。因此，FATF 鼓勵其成員國和所有國家對北韓及其代表進行交易能力的加強盡職調查。」

透過外交人員之操作或許將更困難；另有評估指北韓公民化名第三方公民身分從事採購和運輸可能日益增加（例如，偽裝成來自已知野生動物販運過境國和目的地國的個人）。[20]

現況 – 伊朗

28. 因未遵守 UNSCR 第 1696 號決議（要求停止鈾濃縮），伊朗最初依聯合國安全理事會第 1737 號決議受到聯合國制裁，為多項決議中首個對涉及伊朗核計畫之個人和實體實施目標性金融制裁的決議。

29. UNSCR 經由第 2231 號決議聯合國安全理事會批准聯合全面行動計畫，伊朗同意限制其核計畫以交換制裁解除。根據 UNSCR 第 2231 號決議，對與伊朗核計畫有關的個人和實體實施的制裁將於 2023 年 10 月到期，且不再適用於 FATF 標準建議第 7 項。然而，鑑於相關威脅，一些國家仍以本國家制裁機制來對伊朗實施 TFS。

30. 伊朗依靠中東的軍事代理人以及伊朗境內外的一系列跨國犯罪組織（TCO）來抵減經濟制裁的影響。廣泛的海外商人協助伊朗走私石油，而銀行、黃金交易商和外匯公司可以成為洗錢和複雜的規避制裁之重要管道。正如各種案例研究所述，伊朗規避制裁和出口管制可以支援其飛彈、武器、軍用航空設備和 WMD 計畫的發展。

31. 伊朗代理人受益於進入犯罪市場，特別是外匯交易所，這些市場曾經作為 ISIS 和基地組織的資助管道。真主黨在這方面發揮了特別重要的作用，因為它擁有廣泛的走私活動、全球合法和非法商業網路，以及透過外匯公司在全球洗錢中佔據主導地位。真主黨涉嫌走私石油、武器和一系列受制裁的商品。[21]

32. 若干案例顯示，真主黨等代理利用遍布多洲的合法／非法商網與外匯公司主導洗錢，亦涉嫌走私石油、武器與受制裁商品，甚至違反對伊朗之制裁以取得武器裝備，強化其海外行動之犯罪市場連結。

現況 – 俄羅斯

33. 由於軍事入侵烏克蘭對俄羅斯經濟施加國際制裁壓力，俄羅斯聯邦不得不採取措施以維持其經濟和軍事地位。如本節前面所述，其中一項措施包括與北韓簽署全面戰略夥伴關係條約。[22] 該條約建立兩國之間的經濟和軍事聯繫，包括以下規定：加強戰略和手法合作；提供軍事援助；採取聯合措施加強國防能力（有關經濟協調的資訊，詳見第 26 段）。

34. 在 2025 年 4 月，北韓根據雙邊條約確認在俄烏衝突中部署北韓士兵，俄羅斯官員則證實北韓士兵在庫爾斯克地區活動。[23] [24] 在此之前，2024 年 3 月聯合國 1718 POE 報告引用了聯合國對烏克蘭境內存在北韓彈藥的調查努力。[25] 由於俄羅斯與北韓（聯合國二十年來制裁的主要 PF 威脅行為者）之間的經濟和軍事聯繫，多國將俄羅斯視為 PF 威脅。

---

20 聯合國正在調查北韓在非洲猖獗的野生動物販運活動 | 北韓新聞

21 正如執行摘要和文件其他部分所述，本報告包含有關於用以逃避國家和超國家制裁制度之技術的資訊，藉以提供對威脅和弱點的最新瞭解，包括 FATF 標準建議第 7 項並未涵蓋的相關態樣之間的共同挑戰。更廣泛的規避制裁框架並非意圖重新定義建議第 7 項的要求。

22 http://kcna.kp/en/article/q/6a4ae9a744af8ecdfa6678c5f1eda29c.kcmsf

23 http://www.rodong.rep.kp/en/index.php?MTJAMjAyNS0wNC0yOS0wMDFAMT-VAMUBAMEAxQA==

24 http://en.kremlin.ru/events/president/news/76805

25 https://docs.un.org/en/S/2024/215

其他威脅

35. 多國持續關切非國家行為者（如恐怖組織和犯罪組織）試圖取得和／或採購與 WMD 相關之物資，包括生物、化學和核子能力，相關的貨物、知識與技術。2022 年 11 月，UN 安全理事會延長 UNSCR 第 1540 號決議的授權，重點是防止 WMD、知識或前驅材料擴散至非國家行為者。[26] 該決議所涉義務與建議第 7 項及其註釋規定的義務是分開存在的。[27] 雖利用金融體系支援 PF 行為者個案不多，但許多國家認為，但其潛在影響重大，仍須持續監測；其態樣亦有助於理解與降低整體 PF 與規避制裁風險。

弱點

36. 如 FATF 2021 年 《資武擴風險評估及抵減指引》所述，弱點係威脅行為者可加以利用、從而支援或促進違反、不履行或規避 PF-TFS 的因素。現行 FATF 標準下，這適用於北韓及其協助規避聯合國制裁之相關行為者所構成的威脅。若採更廣視角，則延伸至一切運用公私部門弱點之 PF 行為者。

37. 各個國家應考量到國家（含結構性）及部門層面的弱點。前者包含對於 AML／CFT／CPF 在法律及監管框架之弱點。其他國家層級的弱點可能包括司法管轄範圍內的固有因素，例如經濟的規模和複雜性、經濟的非正規／現金化程度，或是法人與法律協議的多樣性。[28] 地理位置亦經常影響 PF 曝露，特別與北韓規避制裁手法存在潛在關聯。

38. 部門弱點係指某個部門之固有特徵易被利用以實施複雜的資武擴和規避制裁手法；例如產業配送管道之中介機構與代理商普遍存在，將妨礙對資金流動或資產流動向之追蹤。

國家層級的 PF 和規避制裁漏洞

39. FATF 全球網路辨識出一些最常見的國家層面的漏洞而有助於複雜的資武擴和規避制裁手法，其中包括：

經濟和貿易因素

40. 許多國家指出，PF 和規避制裁之威脅行為者將目標鎖定在作為國際金融中心的國家，因其對全球金融流動和運輸極為重要（詳見態樣 1）。PF 的弱點源自於由國際金融樞紐面向多樣且分散客戶群所提供之廣泛產品與服務。除此之外，這些成熟的金融體系和經濟體的開放性（包括經濟特區）及複雜程度使得跨境交易特別容易受到非法擴散網路的濫用。擁有配備航運和物流基礎設施之戰略性港口的國家也容易被濫用來規避與兩用貨品有關的制裁及出口管制。

---

26 安全理事會延長核子生化武器監測委員會任期 10 年，一致通過第 2663 號決議（2022）| 會議報導和新聞稿

27 《資武擴風險評估及抵減指引》

28 Money-Laundering-National-Risk-Assessment-Guidance-2024.pdf.coredownload.inline.pdf

41. 同時，許多國家亦指出，與受制裁國家維持經濟和貿易關係本身即存在弱點[29]，這升高了潛在的 PF 和規避制裁手法風險。地緣政治結盟、依賴關係或歷史聯繫，可能為 PF 威脅行為者創造可乘之機，在不知情的情況下鎖定該等國家，以規避制裁並獲取金融體系和資源。

42. 多數國家強調海關機構在預防和發現與 PF 相關的複雜規避制裁手法方面的重要性。海關機構在國內、地區和國際資訊收集及交換方面發揮關鍵作用（詳見第 3 節）。

監管因素

43. 儘管各國在實施 AML／CFT 規範方面已有進展， CPF 相關措施仍落後（詳見圖 1 和圖 2）。由於缺乏強有力的監管、立法和營運框架，部分國家無法實施必要的制裁義務和出口管制以阻止並反擴散網路。此外，複雜的 PF 和規避制裁手法運用各式各樣的混淆技術，在不受監管的行業或監管不足的行業，像是 VASPs，而這些技術甚至更難被偵知。進一步而言，在法律協議透明度及實質受益權上，法律較弱之國家其 PF 弱點更形加劇。取得實質受益權資訊之困難阻礙了當局尋求識別和追蹤 PF 路徑的跨境調查，尤當涉入多個法律框架不一致的國家時。

地理和人口因素

44. 若干國家報告了與受聯合國、國家和超國家制裁制度之國家地理位置相近所衍生之弱點，可能為非法網路跨境轉移資產和資源創造機會。具有戰略位置的國家擁有重要的航運通道和貿易路線，增加鄰近國家固有的弱點。例如，涉及到走私非法貨物的貿易規避制裁手法，更可能發生在受制裁管轄區附近的國家之間（詳見態樣 4）。案例研究表明，東亞國家可能面臨北韓協助的迂迴金融交易與運輸的風險；中東國家可能為伊朗的 WMD 計畫建立非法金融通道。同時，有國家報告與受 UN 制裁制度所涉之外交人員和其他相關行為者之存在相關之弱點。

其他國家層面的因素

45. 另一個弱點係全球金融體系中廣泛使用的大量外幣，例如美元。鑑於這些貨幣或以這些貨幣計價的帳戶容易被用於非法購買或規避制裁，各國應考慮到以這些外幣的跨境交易將受到影響。

46. 此外，擴散網路亦試圖利用工業和技術因素非法取得貨物。生產擴散敏感技術和產品之國家，先天較易受到 PF 與兩用貨品限制違反之影響。國防部門規模較大之國家，需要大量供應鏈提供材料、產品及服務。這就為 PF 網路提供利用複雜供應鏈的機會。

47. 最後，UNSCR 第 1718 號決議 POE 報告強調北韓依賴有組織或跨國犯罪網路，利用其運輸走廊及中間人以支援擴散活動。

---

[29] 在實務上，許多國家都尋求解決與逃避聯合國、國家和超國家制裁制度有關的弱點。然而，FATF 建議第 7 項僅適用於北韓，而該國是唯一受到聯合國制裁的國家。正如執行摘要和本文件內其他部分所述，本報告包含有關用於逃避國家和超國家制裁制度的技術的資訊，藉以提供對威脅和弱點的最新理解，包括並未被 FATF 標準建議第 7 項所涵蓋之相關態樣間的共同挑戰。更廣泛的規避制裁框架並非意圖重新定義建議第 7 項的要求。

產業層面的 PF 與規避制裁的弱點

48. 根據 FATF 全球網路提交的意見及公眾諮詢的結果，最容易受到複雜 PF 和規避制裁手法影響的行業包括：

銀行及其他金融部門

49. 許多國家認為銀行業和其他金融業，像是保險業，容易受到 PF 和規避制裁威脅行為者的攻擊。在國內和跨境進行金融交易後，支援 PF 行為者或活動的資金可能來自或透過合法或非法活動轉移。技術經常被用於模糊化這些交易的性質，包括利用多個帳戶和偽造文件，其中涉及貿易融資。

50. 通匯銀行很容易規避制裁，因為它們通常與委託銀行的客戶沒有預先存在的關係。[30] 一些私部門實體發現各種容易受到 PF 和規避制裁風險影響的複雜帳戶態樣和交易，這些風險尤其與牽涉到跟 PF 風險曝露較高和／或 CPF 控制無效之國家有關聯的通匯銀行業務相關。例如，透過開放帳戶交易（賒帳交易）進行的貿易很脆弱，因為缺乏有關運輸貨物的資訊。並且，電匯可供快速轉移資金，但它們通常包含有關交易目的或支援文件的有限資訊。

51. 若干國家並指出其他相關因素，包括具廣域分行網路之金融體系、快速便捷之銀行服務、未償還投資資產數量增加，以及個人持有的金融資產的豐富性。

虛擬資產和虛擬資產服務提供商

52. 許多國家對虛擬資產進行跨境支付和轉帳日增表示關切。由於建議第 15 項的實施落後（詳見態樣 3），PF 網路經常試圖利用各國針對 VASPs 的 AML／CFT／CPF 措施缺乏有效實施的狀況。在具有 AML／CFT／CPF 要求的國家，也存在 VASPs 未遵循義務之情形。各國尤關注以假名籌集和轉移資金相關的 PF 風險。許多不法分子試圖透過使用虛擬資產混合服務和匿名增強加密貨幣（AEC）提升交易匿名性，並處理大規模虛擬資產竊取所得（於洗錢過程中支援 WMD 擴散）。混幣和其他混淆技術可以使第三方難以追蹤或歸因交易。此外，各國亦注意到虛擬資產在北韓創收中所扮演的角色。

新型替代支付基礎設施

53. 一部分國家和非國家行為者正在探索新型支付管道和 SWIFT 支付系統之替代方案，以繞開與國家、超國家和／或國際制裁制度相連之金融接點。例如，在某些情況下，國家和非國家行為者，可能利用新興的數位支付系統，如點對點支付服務或數位匯款提供者。[31]

---

30 通匯銀行業務，尤其是向已知轉移／管道管轄區提供的通匯銀行業務，或 AML／CFT／CPF 控制無效的通匯銀行業務，可能會帶來更大的風險。然而，通匯銀行業務對資武擴的風險並非總是很高。代理關係的風險評估應根據案例方式進行，並且應始終將代理銀行所採用的內部控制和風險抵減措施納入考量。詳見 FATF 的《 *2021 PF 指引*》以進一步了解關於通匯銀行業務關係的資訊。

31 儘管對於 SWIFT 支付傳訊系統的替代方案存在潛在的風險管理疑慮，利用中央銀行數位貨幣（CBDC）來逃避制裁現今仍為理論性。另一方面，有些國家將 CBDC 視為讓權責機關更容易追蹤資金流向、降低非法資助風險的方式。

其他部門層面的弱點

54. 正如聯合國安全理事會第 1718 號決議 POE 報告和 FATF 2021 年《資武擴風險評估與抵減指引》，各國應注意其他更有可能違反、不執行或規避資助武擴-目標性金融制裁的行業，包括但不限於：信託和公司服務業者（TCSP）以及貴金屬和寶石經銷商。[32]

55. 此外，各國發現了其他幾個容易受到 PF 和規避制裁行為者利用的行業，包括航空、資訊科技（IT）、航海、核電和造船業。

[32] https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf

4. 第 2 節：規避與 PF 相關的制裁 – 態樣分析

目前趨勢和方法

56. 在本報告中，案例研究分為兩個不同類別：

a. **規避與北韓有關的 PF-TFS**，是涵蓋於 FATF 標準建議第 7 項

b. **規避其他制裁制度（像是國家和超國家制裁）**，不屬於 FATF 標準建議第 7 項的範疇

57. 本節根據 FATF 全球網路提交之資訊，提供複雜 PF 和規避制裁手法中使用之態樣之非詳盡列表。這些態樣形成指示 PF 行為之金融交易指標清單（詳見附件 A：風險指標）。

表 1。態樣概述

態樣	案例研究子主題	頁
1. 利用中介機構規避制裁	前台公司和空殼公司透過第三國銀行帳戶和資金轉移	21-29
2. 遮蔽 BOI 以進入金融體系	支援無執照金融協助者之第三方金融協助網路 北韓利用不同法人型態濫用信用卡和金融卡	29-37
3. 使用虛擬資產和其他技術	監管挑戰 利用虛擬資產轉移資金虛擬資產以及資金的產生 支援北韓 IT 工作者之外國實體和個人	38-46
4. 開發海事和航運業	變更船舶識別 ID 船對船轉運 停用 AIS 廣播 偽造文件	46-53

態樣 1：利用中間人來規避制裁

58. 多國報告稱，為掩蓋真正的最終用戶，運往涉擴散國家或受制裁國家的貨物採購網路正在運用牽涉到多個中介機構的複雜手法。此類策略使得偵測和調查 PF 和規避制裁案件變得十分困難。中介機構可能包含空殼公司和前台公司、金融協助者、銀行帳戶（包括通匯銀行業務關係），以及透過第三國的轉運。這些中介機構使用在遮掩資金來源、目的地和用途方面扮演著極為關鍵的角色。透過利用不同金融體系和監管框架的漏洞，中介機構能夠擴散網路來規避偵查和制裁（關於進一步資訊，詳見弱點乙節）。

使用前台公司和空殼公司

59. 許多國家報告顯示，PF 和規避制裁網路可以在第三國設立或與當地企業合作，作為中介機構和前台公司。此類實體可能是無實質營運之空殼公司，或進行表面合法之交易，以進入金融體系、促成支付和契約、以虛假藉口進出口貨物（例如將兩用貨品申報為僅供民用）。不法分子亦會透過更換公司名稱、所有權結構或註冊國別，以掩蓋與受制裁實體之關聯性。該等行為多見於涉及走私兩用貨品或物項之產業，如電子產品、化學品或工業設備，或是其他受制裁或出口管制規範之貨物。

方框 2. 案例研究：利用澳洲的公司結構規避制裁

2021 年 7 月 23 日，新南威爾斯州最高法院判處一名南韓出生的澳洲公民三年六個月監禁，罪名是違反澳洲對北韓制裁法。該人利用離岸銀行帳戶和一系列位於澳洲的前台公司與北韓進行各種商品的貿易，包括煤炭、石墨、銅礦石、黃金、原油（包括代表北韓購買伊朗汽油）、飛彈和飛彈相關技術。此案係澳洲首度就違反北韓相關制裁而起訴之案件。

來源：澳洲

60. 中介機構亦可尋求律師和會計師之協助，以架構複雜結構以避免被偵知；或者尋求貨運代理和船運代理之支援，幫助建立複雜供應鏈，並如何利用制裁制度漏洞提供建議，使違禁貨物得以錯誤申報並以虛假藉口運送。

61. 前台公司是應用於軍事武器或國防部門之兩用貨品供應鏈的常見手段。不法行為者此類複雜手段，低釐清敏感商品可能涉及之規避制裁或出口管制之行為的調查效率。以下兩則案例研究說明匿藏此類兩用貨品最終目的地的複雜手法。

方框 3. 案例研究：向伊朗軍事實體走私原產於美國之電子元件的規避制裁手法

2024 年 1 月，四名中國公民在哥倫比亞特區被起訴，涉犯多年密謀從美國非法出口和走私美國原產的電子元件到伊朗等多項聯邦罪。被告涉嫌透過中國和香港非法出口和走私美國出口管制物品，為伊朗革命衛隊（IRGC）和國防與武裝部隊後勤部（MODAFL）附屬實體，該等實體負責監督伊朗飛彈、武器和包括無人機（UAV）在內的軍用航空設備的研發及生產。

早自 2007 年 5 起至 2020 年 7 月止，相關人士利用中國的前台公司取得美國原產之兩用貨品，包括可用於產製 UAV 、彈道飛彈系統和其他軍事最終用途的電子產品和零件，輸送給與 IRGC 以及 MODAFL 有聯繫的受制裁實體，例如 Shiraz Electronics Industries（SEI）、Rayan Roshd Afzar及其附屬公司。

期間，被告隱匿貨物運往伊朗及其實體的事實，並向美國公司就最終目的地和最終使用者做出重大虛假陳述，致使美國公司在虛假前提下對前台公司出口軍民兩用貨品，且將最終目的地偽稱為中國而非伊朗，違反美國的制裁及出口管制法規。相關指控是由司法部和商務部領導之多機構打擊小組協同偵辦。

來源：美國

方框 4. 案例研究：透過中間商向俄羅斯實體出口軍民兩用貨品

法國公司 A1 、 A2 作為中間商，購買外國電子元件後轉售給中東及北非（MENA）地區的另一個中間商實體（B 實體）。在中間商購買軍民兩用貨品後，又將電子元件供應給受美國制裁的俄羅斯母公司（C 實體）。這項擴散手法使得俄羅斯國防部門能夠獲得違禁物品，並增強其整體能力。

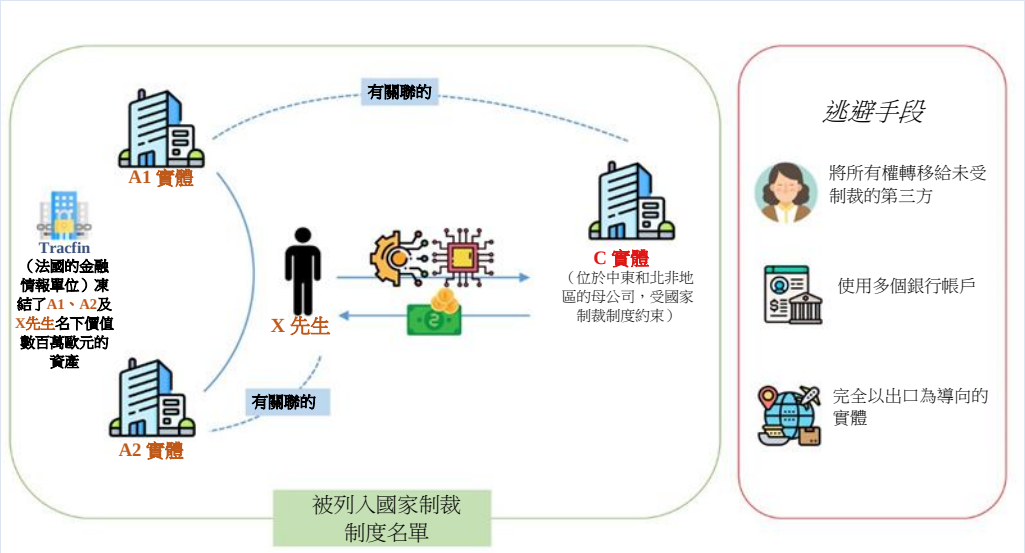
法國金融情報中心（FIU），TracFin，領導展開一項跨部會行動，凍結 A1、A2 和 X 先生（A1 和 A2 的最終實質受益人）擁有的 100 萬歐元資產以阻止該手法。同時美國財政部 OFAC 制裁 A1、A2 和 X 先生實施制裁；惟該個人和實體目前不受歐盟或法國限制措施的約束。隨後，TracFin 與法國銀行合作 [33]，根據控制標準限制其資金，原因是 C 實體已將其股份出售給外國投資人，惟其仍疑似對 A1 具有控制力； A2 由 X 先生全資擁有。

該複雜的規避制裁手法牽涉多項常見策略，包括將所有權轉讓給未受制裁的第三方（該人士的妻子）、利用多個銀行帳戶，以及運用完全以出口為導向之商業模式的實體，而儘管如此，惟該等實體實際上僅為過路性質。

最大的挑戰是制裁制度間之差異 [34]，易致資本外逃。協調一致之指定程序將有助於提高制裁效力，並確保跨國資產凍結具有法律依據。

33 在 EU 法律中，控制標準有助於確定資金或實體是否受到受制裁實體或個人的控制。例如，如果受制裁的個人或實體對資金或實體具有影響力或可以做出決策，這有助於決定是否存在控制權。

34 這種差異是偵查、調查和起訴與 PF 相關的規避制裁行為的關鍵因素其中之一，如第 3 節（詳見第 105-106 段）和結論（詳見第 146 段和優先領域）所述。



來源：法國

利用第三國過境來促成全球化供應鏈和國際貿易

62. 各國指出，擴散網路利用全球化供應鏈與國際貿易，掩飾貨品與技術之採購活動。他們可能會從多個供應商處採購零件以遮掩最終用途；經自由貿易區（FTZ）轉運（該等區域通常監管較鬆並允許重包裝與改標後再出口）；經多個港口或國家運輸，以隱匿真實的原產地或目的地，使用虛假文件、偽造的裝運單據、最終使用者證書或是提貨單來誤導貨物性質或最終收貨人。例如，被禁止運輸之飛彈元件可能會偽裝為工業機械並附篡改文件。下列兩則案例顯示更複雜之過境路線，偵知規避出口管制法規和制裁之行為。

方框 5. 案例研究：利用中間商規避出口管制規定

多起個案呈現反覆出現之態樣，由伊朗人管理或控制之第三國公司（有時位於其他歐盟管轄區）自法國供應商購得兩用產品後，再出口至伊朗。

某為伊朗彈道飛彈計畫供貨之伊朗公司企圖自法國供應商取得複合材料。該公司的伊朗籍負責人利用另一名伊朗人經營的第三國公司，將複合材料再轉出口至伊朗。

在 2020 年，一台工具機連續出口至歐洲 A、B、C 國，然後離開歐盟境內。此複雜貿易路徑和文件變更的目的是要掩蓋其後續運程，最終目的地為伊朗，期間並經中東某司法管轄區。

來源：法國

方框 6. 案例研究：透過國際合作偵得利用中介機構規避歐盟制裁之行為

2022 年，一家葡萄牙公司試圖透過阿拉伯聯和大公國的中間商向一家哈薩克公司出口應用於 UAV 的發動機，名義最終目的地為該公司。該貨物屬於歐盟對俄羅斯第 12 套限制措施的範圍，且跡象顯示最終目的地是俄羅斯聯邦。在調查期間，由於目的地受到質疑，該公司放棄了該批貨物的出口。

該公司試圖透過兩個不同的中介機構（UAE 之貨運代理與哈薩克零售商）來規避制裁，並隱藏最終使用者。該哈薩克公司與俄羅斯公司有著密切的商業聯繫，而且轉移的風險甚高，付款透過銀行轉帳進行。

其後，葡萄牙當局監控發現，該公司在 2023 年稍後又透過塞爾維亞和香港的中間商出口了其他安全和國防商品，目的地可能為俄羅斯。這兩家中間商都與俄羅斯聯邦有密切商業關係。

本案由安全情報局與海關合作偵辦，並藉由國際合作與海關調查推進。

此案例說明了採購網路調適於新情況和不同挑戰的能力。唯有各國進行有效合作、溝通順暢，方能抵減此等威脅。

來源：葡萄牙

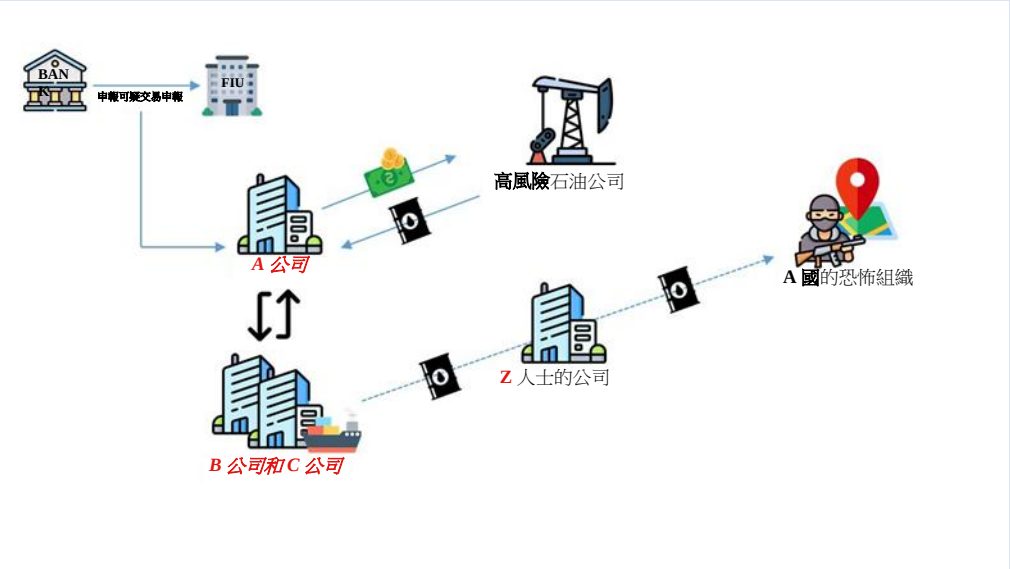
63. 除此之外，靠近受制裁國家或實體的區域運輸樞紐也成為規避制裁者轉移資金及商品的目標。尤其，PF 和制裁網路尋求掩蓋他們在國際金融樞紐的活動，他們希望大規模的商業、金融和貿易活動能幫助遮蔽他們的非法活動。

方框 7. 案例研究：利用航運公司為受制裁實體出售石油

2022 年 9 月，LEA 收到一份阿拉伯聯合大公國金融情報中心（UAEFIU）寄來有關於銀行所發出的 SAR／STR 的通知。該報告指出，A 公司向一家高風險石油公司進行的電匯被懷疑用於支援 WMD 擴散。LEA 和 UAEFIU 對 A 公司及其金融／商業活動進行了刑事和金融調查。

調查結果顯示，A 公司由外國人設立，與兩家阿拉伯聯合大公國貨運公司（B 公司和 C 公司）有關。進一步調查發現，B 公司與 C 公司屬於支援 A 國恐怖組織的個人所有。這兩家公司都利用 Z 先生的公司作為中介，簽妥貨運契約以將石油從高風險國家運往 B 公司和 C 公司，然後再運往恐怖組織。

調查亦發現，B 公司和 C 公司使用偽造文件向恐怖組織出售石油，以掩蓋石油的來源及產地。石油銷售所得被轉帳到 A 公司，該公司再將其傳送給高風險石油公司 – 這被懷疑是該受制裁實體用以支援擴散的幌子。調查發現，轉移的資金總額達 7,000 萬美元。LEA 逮捕了包括 Z 先生在內的所有嫌疑人，Z 先生承認參與協助伊朗規避 PF 制裁，並且暫停這些公司的業務活動。



來源：葡萄牙

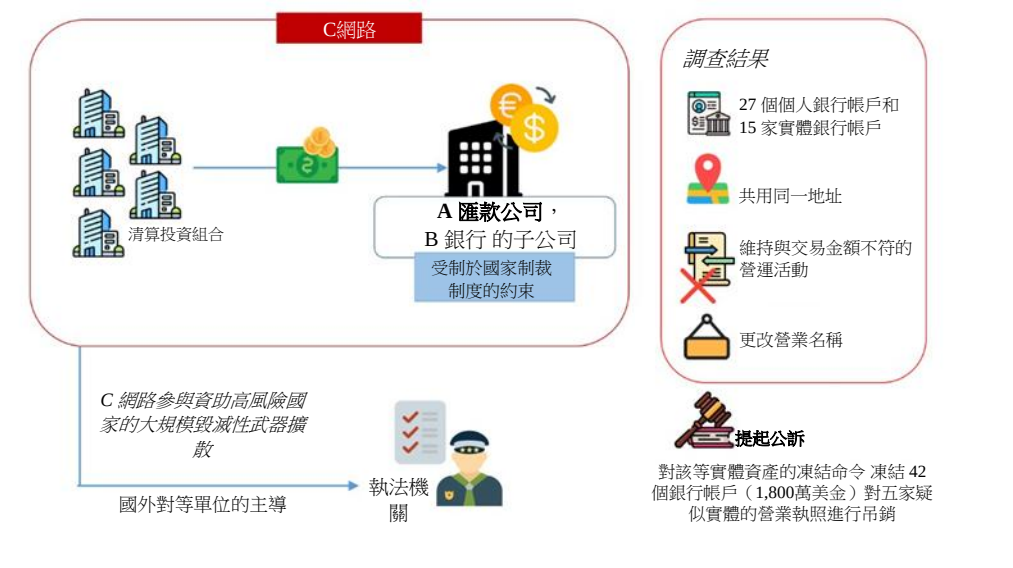
使用銀行帳戶和透過第三國資助

64. PF 和規避制裁行為者經常利用多層次金融交易來掩蓋資金的來源、目的地或用途，這是典型的洗錢手段。他們經常透過數個國家的多家金融機構來轉移付款以阻礙追蹤工作，並且在有監管漏洞的國家註冊前台公司或空殼公司。

方框 8. 案例研究：濫用金融體系和石油運輸來支援 PF

執法部門透過機密來源發現，五家阿拉伯聯合大公國公司與 B 銀行的子公司 A 高風險交易所進行了多筆高價值的進出交易。 A 交易所和 B 銀行均屬於「 C 網路」，並受到美國財政部 OFAC 的指定。五家涉嫌公司中的兩家透過清算投資組合獲取資金，並將資金轉移到 A 交易所， A 交易所又將資金轉移到 B 銀行以支援一個受制裁實體。LEA 已與相關利害關係人，阿拉伯聯合大公國金融情報中心（UAEFIU）、阿拉伯聯合大公國中央銀行（CBUAE）、地方登記處以及海關展開調查。

CBUAE 辨識出與該網路相關的 27 個個人銀行帳戶和 15 個實體銀行帳戶。地方登記處亦向 LEA 提供了現場檢查報告；這些報告顯示，涉嫌實體共用相同地址，在現場檢查之前傾向於更改其商標名稱，並且維持與交易價值不符的營運。同時，LEA 從國外對等單位獲得線索，證實 C 網路參與資助高風險國家擴散大規模毀滅性武器（WMD）。根據這些調查結果，檢察機關與 UAEFIU 及 CBUAE協調，對這些實體的資產發出了凍結令，凍結 42 個銀行帳戶，總餘額約為 1,800 萬美元（63,725,065 迪拉姆）。此外，地方登記處也暫停了五家涉嫌實體的貿易許可證。



來源：阿拉伯聯合大公國

65. PF 網路的目標是第三國的金融機構，他們試圖利用這些國家在實施國際和國家制裁制度方面的司法差異。不法分子利用銀行開設帳戶，並且透過通匯銀行業務關係間接進入國際金融市場，在不引起警告的情況下進行國際電匯。非法網路亦可運用不太可能發現可疑交易的非正式金融體系，並依賴對跨境交易報告要求或執法不太嚴格的國家。

方框 9. 案例研究：因構成伊朗革命衛隊（IRGC）用於創造收入的「影子銀行」網路而遭受制裁的實體和個人

在 2024 年 6 月，OFAC 制裁了將近 50 個實體和個人，他們構成了龐大的「影子銀行」網路的多個分支，國防部後勤支援部隊（MODAFL）和伊朗革命衛隊（IRGC）利用該網路獲取收入以從事多項活動，包含非法採購美國產電子元件以開發諸如 UAV 等先進武器，並且支援葉門的胡塞武裝和俄羅斯在烏克蘭的戰爭等活動。

為進入國際金融體系，MODAFL 利用伊朗的交易所，這些交易所管理香港、UAE 和其他地方的眾多前台公司，將包含石油銷售等外國商業活動產生的收益洗白成合法來源的外幣。相同的前台公司利用洗白的外匯在國際市場上購買武器零件。

來源：美國

方框 10. 案例研究：利用中介機構規避 TFS 並轉移不動產所獲得的收益

2015 年，一名駐法國的北韓外交官在巴黎購買一套公寓並出租，隨後於 2017 年被聯合國列入制裁名單。受到制裁後，他繼續收到該公寓租賃的收入。該個人發展出一項手法，涉及多個在第三國擁有銀行帳戶的中介機構，以隱藏其作為最終實質受益人的身分。在 2019 年，一家歐洲銀行發出警報後，這些收益被存入一個託管帳戶。

來源：法國

態樣 2：掩蓋 BOI 以規避制裁並進入金融體系

66. 複雜的 PF 和規避制裁通常牽涉到偽造 BOI、混淆最終使用者／最終用途和最終目的地，這對於公私部門兩者而言都很難發現。同時，許多混淆技術正在應用於數位領域，這可能會為偵查作業帶來額外的挑戰。由於 TFS 適用於經指定的個人和實體以及由這些指定人士所操控或擁有的資金，因此識別出實質受益人可有助於抵減與規避制裁相關的風險。

支援北韓進入金融體系的第三方協助者

67. 北韓經常運用欺騙手段，包括掩蓋 BOI，以規避聯合國和國家制裁制度並且進入正規的金融體系。北韓繼續利用設在外國的前台公司及空殼公司、秘密的海外代表和第三方協助者來掩蓋真正的發起人、受益人，和交易目的，讓北韓數十億美元的非法金融活動得以透過國際金融體系流動。支援北韓進入金融體系的複雜計畫之國家行為者，致使防止規避制裁變得難以進行。

方框 11. 案例研究：北韓和俄羅斯金融實體精心策劃複雜的規避制裁手法

2024 年 9 月，美國財政部海外資產管制辦公室（OFAC）指定了一個由五個實體和一名個人所組成的網路 – 以位於俄羅斯和俄羅斯佔領的格魯吉亞地區（Georgian region）的南奧塞迪雅（South Ossetia）為基礎 – 利用非法金融手法使北韓能夠進入國際金融體系，違反聯合國安全理事會第 1718 號決議規定的 TFS。[35] 同時，該等實體及個人也違反了聯合國安全理事會第 2270 號決議關於禁止與北韓銀行建立代理關係的規定。

這項行動針對的是北韓兩家國營機構，外貿銀行（FTB）和北韓光鮮銀行（KKBC），所精心策劃的複雜手法，這兩家機構都是聯合國安全理事會第 1718 號決議制裁名單上的指定實體。[36] FTB 是北韓的主要外匯銀行，對北韓資助其 WMD 和彈道飛彈計畫的非法金融網路非常重要。在俄羅斯聯邦的協助下，FTB 和 KKBC 繼續擴展北韓進入非法金融網路的管道。

在俄羅斯中央銀行精心策劃的一項手法中，位於格魯吉亞的南奧塞迪雅的 MRB 銀行（MRB）作為俄羅斯銀行 TSMR 銀行的中間人，與 FTB 建立秘密銀行關係。TSMR 銀行的一名高級官員協助 FTB 透過 TSMR 銀行向 MRB 存入現金。在 TSMR 銀行的高級官員組織在 MRB 開設對於 FTB 和 KKBC 的代理帳戶，並且與北韓代表協調以確保將數百萬美元和盧布的紙幣匯入 FTB 和 KKBC 在 MRB 的帳戶。北韓在 MRB 的帳戶至少有一部分被用來支付俄羅斯向北韓出口燃料的費用。

作為 2023 年底另一項手法的一部分，俄羅斯金融公司銀行股份公司（RFC）與 FTB 合作成立了一家總部位於莫斯科的公司 Stroytreyd LLC（Stroytreyd），以接收已倒閉的俄羅斯銀行所持有的受凍結的北韓資金。作為將凍結資產遣返北韓的努力的一部分，RFC 所擁有的 Timer Bank AO（Timer Bank）向 Stroytreyd 轉了價值數百萬美元的資金，而這些資金的最終收款者是 FTB。北韓政府官員與俄羅斯金融公司共同努力，增加北韓與俄羅斯之間的高層經濟交流，而且強化兩國之間的金融合作。FTB 也與 RFC 合作為其他北韓銀行開設帳戶，包括北韓的農業發展銀行。[37]

來源：美國

68. 即如許多國家指出，北韓也依賴包括外交人員在內的公民提供金融服務或轉移資產或資源，包括運送大量現金。這些手法難以察知，而且外交協議使得及時採取行動攔截或阻止此類活動變得更為困難。

35 https://home.treasury.gov/news/press-releases/jy2590

36 在 UNSCR 第 1718 號決議的名單上，FTB 被指定為 KPe.047，KKBC 被指定為 KPe.025

37 2025 年 1 月 10 日，日本標定 4 個個人和 5 個實體（MRB 銀行、俄羅斯金融合作公司、Stroytreyd LLC、TsMRBank 及 Timer Bank AO）以協助北韓-俄羅斯合作。

方框 12. 案例研究：北韓外交官配偶透過保險公司轉移資金

奈及利亞的保險公司涉嫌與受制裁國外交官的配偶合作，幫助北韓的國家保險公司，韓國國家保險公司（KNIC），追討債務、拓展業務、收款、資金轉移，並且擔任代理人或代表以規避聯合國制裁。KNIC 係於 2017 年依據 UNSCR 第 1718 號決議制裁制度所指定（KPe.048）。透過 KNIC 收到的資金被轉用於北韓的 WMD 計畫。

由一金融機構所提交的 SAR／STR 幫助奈及利亞當局偵知涉及不合理金額的金融活動。交易總價值估計超過 616,000 歐元。發現可疑活動後，金融機構凍結相關帳戶並且向奈及利亞當局回報。此外，奈及利亞正在考慮採取更多反制措施。

保險行業所針對的弱點則是保險公司透過第三方公司購買國際保險或者為國家基礎設施購買再保險的方式。此外，保險客戶和交易被用於規避制裁的手法，這表明需要加強對於相關實體的風險控制。

來源：奈及利亞

69. 許多國家都知道北韓利用外國人和由這些人註冊的前台公司來混淆 BOI，從而透過正規金融體系取得及轉移資金。例如，FTB 和 KKBC 藉由在中國境內銀行開戶的中國公民的名義建立前台公司網路，遮蔽與北韓的金融聯繫，透過國際金融體系轉移資金。

方框 13. 案例研究：北韓銀行和金融服務 – 外貿銀行

2020 年 5 月，美國當局對 30 多名個人提出刑事指控，他們涉嫌以各種身分為聯合國指定的 FTB 提供服務並進行禁制的美元交易。起訴書概述了最終代表北韓政府向美國公司支付的具體款項。FTB 前台公司與其他第三方公司之間的其他付款是透過美國通匯銀行清算。

起訴書中列出的個人在共謀期間導致通匯銀行透過 250 多家前台公司處理了至少 25 億美元的非法付款，這些付款途經美國。這些公司分別成立於奧地利、中國、科威特、利比亞、馬紹爾群島、俄羅斯和泰國。許多被起訴的個人常駐於這些國家，經營 FTB 的秘密「分支機構」，而多項重大活動集中在中國城市。

這些人與第三方金融協助者合作，創建前台公司，代表北韓支付購買大宗商品和其他貨品的費用，包括與精煉石油及煤炭貿易相關的付款。其他款項則支付予金屬、電子及電信公司。一旦交易對手認為舊公司可疑，被告就會創建新的前台公司。他們在 FTB 代理商之間的通訊會使用編碼的付款參考，以便 FTB 總部能夠指導購買並且準確評估自其前台公司到收款人的資金流動。最後，在運送實際貨物時，被告在契約及發票上標註虛假的最終目的地和最終使用者。

來源：美國

無執照金融協助者網路支援規避制裁

70. 除此之外，一些國家也發現伊朗運用複雜的規避制裁手法，包括混淆 BOI，為其 WMD 計畫採購兩用貨品。據觀察，伊朗經常使用在主要金融中心註冊的前台公司來轉移由伊朗政府掌控之貨幣交易所的資金。

方框 14. 案例研究：利用非法 TCSPs 進行兩用貨品交易

伊朗公民在荷蘭設立了多個曾經或現在活躍於科技領域的法人實體。這包括利用公認的參考公司[38]（RRC）以據稱能夠讓高技能移民更易於取得荷蘭居留許可。RRC 也是非法 TCSP 的一部分或與其直接相關，後者提供各種服務，例如公司註冊、開設銀行帳戶以及驗證至少一半的公司董事是否為荷蘭公民（以受惠於荷蘭稅收優惠和稅收協定）。

合法的 TCSP 受到荷蘭中央銀行的監管，然非法的 TCSP 則將其提供的服務劃分並設置於多個法人實體中。如此，這些服務就變得更廉價，而且這些信託服務也變得更難以辨認。因此，荷蘭央行很難對這些實體進行監管。在本案例中，據稱來自伊朗的資金透過知名金融中心流入，並被非法轉移到由非法 TCSP 所設立的荷蘭法人實體。然後，資金在這個結構內轉移，最終流向高技術移民。

本案例中，銀行對帳單顯示有多筆交易，對於伊朗的兩用貨品供應構成風險。這些貨物也適用於擴散目的。這些交易亦與伊朗高技術移民控制的科技公司有關。從而，可以總結出這些公司是作為前台公司之用。透過利用 TCSP（尤其是非法 TCSP）並建立公司網路，這些金融交易中的偵測變得極其困難。

來源：荷蘭

71. 無執照的 MSB 也被用來為代表國內和聯合國指定的恐怖組織行事的個人轉移資金。在以下案例中，阿拉伯聯合大公國當局發現一個利用前台公司作為哈瓦拉(hawaladar)的複雜手法[39]藉以轉移數百萬美元。雖然這是個人代表非國家行為者規避 TF-TFS 的一個例子，但它也可能與用於規避 PF 相關制裁的複雜手法種類有關。

38 一種公認的參考是從外國人的到來而受益的公司、學校或組織。

39 Hawaladar 是提供 Hawala 服務的匯款機構。

方框 15. 案例研究：無執照 MSB 被用來規避聯合國 1267 名單上恐怖組織的制裁

在 2022 年第一季，一家當地交易所向 UAEFIU 提報了一份 SAR／STR ，內容是關於 UAE 的一名外國居民接收到來自高風險管轄區的電匯。所有參與轉帳的各方都是 UAEFIU 取得的金融情報資訊的對象。

根據 UAEFIU 的調查及分析，主要嫌疑人共收到七筆電匯，總額達 350 萬美元，並且在 UAE 設立了一家前台公司以作為 hawaladar 來向高風險國家轉移資金，藉此支援伊斯蘭國（ISIL）和 Jabhat Al Nusra。這兩個團體都被列入 UAE 國家名單和聯合國綜合名單（UNSCR 第 1267／1989 號決議）。

UAEFIU 向國家安全局提供一份案件通報，詳細說明嫌疑人及其前台公司的資訊。國家安全局與 UAEFIU 和中央銀行合作調查嫌疑人的金融活動。據此，國家安全局發出命令以凍結嫌疑人合計 50 萬美元以及 4 公斤黃金的資金和其他資產。該前台公司的業務活動也被暫停。在整個調查過程中，嫌疑人承認向伊斯蘭國（ISIL）和 Jabhat Al Nusra 提供資金，用於購買包括槍枝彈藥在內的軍事裝備。

來源：阿拉伯聯合大公國

利用不同種類的法人規避制裁

72. 一些國家報告利用子公司和其他法人來遮掩實質受益人資訊。常見的手法包括運用複雜的手法來規避制裁，以及採取更直接的方法來針對沒有強力 AML／CFT／CPF 監控的行業作為目標。

方框 16. 案例研究：規避歐盟制裁的複雜手法

受到歐盟制裁的 A 個人與 B 個人協調訂定一項複雜的手法以協助規避制裁。首先，B 個人為一家有限責任公司（LLC）Blue 的所有者，成立了一家名為 Company Red 的子公司。接著，B 個人利用 Company Red 收購 A 個人在 LLC Green 中的股份。雖然 LLC Green 擁有一家歐洲公司的 2,850 萬股股份，不過由於 LLC Green 是被 A 個人控制，因此這些股份被凍結。從而，當 Company Red 收購 A 個人在 LLC Green 的股份時，它也收購了該歐洲公司被凍結的股份。作為出售 LLC Green 的交換，A 個人 獲得等值的經濟利益。

B 個人協助規避制裁，因為他和位於俄羅斯的公司（LLC Blue、Company Red 及 LLC Green）利用這個手法來出售由列名個人所掌控並持有歐盟公司之凍結股份的非歐盟公司，其唯一目的是解除歐盟對這些股份的凍結。

來源：歐盟委員會

方框 17. 案例研究：用以偽裝真正車輛所有者的複雜所有權結構

各式空殼公司被用來隱藏多輛價值數十萬歐元的豪華汽車的真正主人。該鍊條中的最後一家公司是一家在德國註冊的有限責任公司，擁有這些豪華汽車。雖然這家 LLC 的官方任務是管理這些車輛，但是中央制裁執行辦公室的廣泛調查證明，該公司的唯一職務是要隱藏這些車輛的真實所有權。

事實上，該公司並因此這些車輛是由一位被歐盟列入俄羅斯制裁制度名單的個人所掌控。調查發現名單上的個人與 LLC 之間存在聯繫後，這些車輛必須被凍結。進一步的調查能夠將更多資產關聯於該列名個人。

來源：德國

方框 18. 案例研究：利用子公司掩蓋與聯合國認定的北韓實體的聯結

BETA 公司從事建築和公共工程領域，包括向其他公司供應重型機械、固定起重機、移動起重機、挖土機、裝載機和卡車。BETA 的主要客戶是 GAMMA 公司以及幾家從事同一行業的中小型公司。BETA 的實質受益人 X 先生和經理 Y 先生兩人均為受聯合國制裁的北韓的公民。

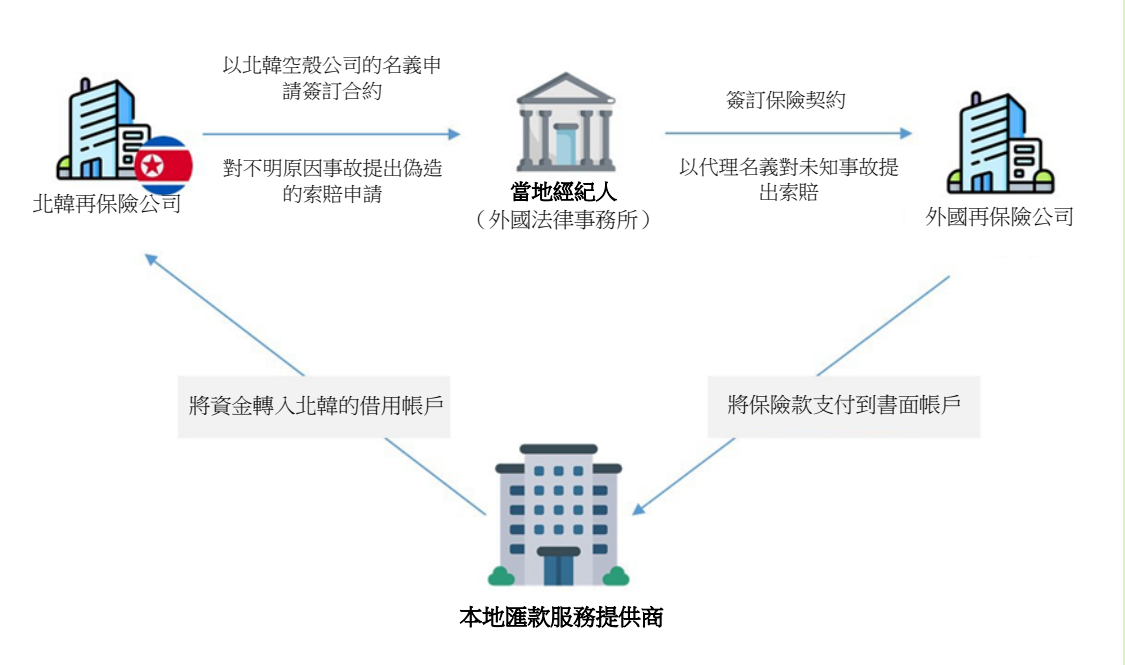
從事農業食品行業的 GAMMA 公司向 BETA 公司購買了農業食品機械。在 BETA 公司兌現了超過 30 萬歐元（2 億 CFA Francs）的異常支票後，塞內加爾的一家金融機構進行了客戶盡職調查，結果顯示 BETA 位於北韓平壤的母公司被列入聯合國 1718 制裁名單。

在驗證過與受制裁實體的鏈結之後，該金融機構向塞內加爾金融情報中心（CENTIF）提交了一份 STR，並且 BETA 公司的資產遭到凍結。STR 讓 CENTIF 能夠開展調查，但是調查並未顯示 GAMMA 有意參與規避制裁手法。

來源：塞內加爾

73. 北韓每年透過捏造事故、欺騙國際保險市場賺取數百萬美元。由於無法在北韓核實索賠，北韓再保險公司為所有國家基礎設施，像是橋樑及工廠，購買國際保險或再保險，然後偽造文件以領取保險金[40]。北韓動用空殼公司或借入帳戶以簽訂再保險契約並收取保險金。

方框 19. 說明性範例：北韓利用不透明的公司實體實施保險詐欺



北韓利用信用卡和金融卡

74. 許多國家意識到，與北韓有關的個人愈來愈多利用以中國公民名義非法取得的帳戶來混淆他們的財務狀況，並且利用虛擬資產進行支付和獲取當地貨幣，從而讓北韓能夠繼續規避聯合國制裁。

75. 北韓銀行人員疑似以詐欺手段管理眾多由主要的中國商業銀行所發行的非法銀聯金融卡，以數百名國內帳戶持有人的名義進行當地貨幣付款。有跡象表明，這是試圖藉由掩蓋交易和與北韓的聯繫來規避制裁，同時規避實施嚴格北韓制裁制度的國家，以獲取利潤並購買違禁物品。

76. 這些金融網路看似去中心化的性質也減少了任何個別中斷的衝擊，同時也使得政府當局更難以識別北韓的所有帳戶。有跡象表明，北韓正在利用非法獲得的銀聯金融卡來接收從被盜加密貨幣中提取的法定貨幣存款，以及協調一系列與 WMD 相關實體的交易。

40 為北韓提供保險或／和再保險違反了 UNSCR 第 2270 號決議第 33 條和第 36 條，這些條款禁止各國提供可能有助於北韓核計畫或彈道飛彈計畫的大量現金、黃金與保險服務。

態樣 3：使用虛擬資產和其他技術

77. 受制裁的行為者對數位經濟的運用呈現日益增長的趨勢。虛擬資產和其他新技術正被用來規避國際、超國家和國家制裁制度，並且資助 WMD 的行為者和活動。[41] 虛擬資產正被用於協助資金流動：

    a) 直接流向受制裁國家；以及

    b) 經由不實施制裁措施的第三方國家間接流入。因此，大多數國家將不法分子使用虛擬資產和其他的新技術視為主要的 PF *威脅*／弱點。

78. 更廣泛地說，各國也意識到其他新興科技，像是人工智慧，所帶來的規避制裁挑戰。不過，這個領域的證據和趨勢尚處於起步階段而難以得出結論，並且案例研究很少。

監管挑戰

79. 儘管努力應對與虛擬資產和其他技術相關的新興風險，但是許多國家的 VASPs 缺乏 AML／CFT 要求。截至 2024 年 4 月，四分之三的 FATF 全球網路國家被評估為未遵循或部分遵循有關虛擬資產和 VASPs 的國際標準。[42] 國際上法規及監督方面的缺陷使得該行業容易受到 PF 網路的濫用。只要不同司法管轄區在實施 FATF 虛擬資產標準和 VASPs 方面存在差距，PF 網路就能夠在框架薄弱或不存在的司法管轄區利用 VASPs 而不致被偵知或中斷。如下列案例所示，也有受 AML／CFT 框架約束的 VASPs 未能遵守適用要求的實例。

方框 20. 案例研究：幣安執法行動

2023 年 11 月，幣安控股有限公司（Binance，「幣安」）認罪並同意支付超過 40 億美元以解決美國訴訟。美國司法部對與多項制裁計畫有關的違規行為進行調查，包括未為匯款業務進行註冊以及違反國際緊急經濟權力法（IEEPA）。幣安的創辦人兼執行長承認未能維持有效的 AML，違反銀行保密法（BSA）。

部分由於幣安未能實施有效的 AML 計畫，不法分子以各種方式利用幣安交易所，包括進行混淆虛擬資產來源和所有權的交易；轉移勒索軟體變種的非法所得；以及轉移暗網市場交易、交易所駭客攻擊和各種網際網路相關詐騙的所得。

幣安使用者無須提交 SARs／STRs 就能夠與伊朗等受美國制裁國家的虛擬資產交易所進行交易。幣安使用者錢包與伊朗各式虛擬資產交易所進行大量直接交易，每筆交易價值超過 2,000 美元，而總額相當於超過 5 億美元。此一總額亦包含與受制裁實體和個人相關的虛擬資產錢包的多筆交易。

來源：美國

利用虛擬資產轉移資金

41 在 2025 年 3 月於印度舉行的私部門諮詢論壇上，與會者強調新興金融科技帶來的更大風險，尤其是包括北韓在內的國家行為者利用虛擬資產進行網路竊盜，其運用的方法是愈來愈複雜且縝密。

42 https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2024-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf

80. 虛擬資產被用來隱藏流向受制裁國家及其相關行為者的資金流動。當虛擬資產搭配一些技術手段時可以提供使用者更高程度的匿名性，並且能夠瞬時跨境轉移。除此之外，虛擬資產的國際性質可能帶來與驗核外國 VASPs 所在司法管轄區、國際合作所需的時間和資源，以及不同司法管轄區的監管框架和制裁制度間之差異相關的挑戰。特別是，各國提供的範例顯示出虛擬資產錢包和交易平台普遍運用於潛在的規避制裁。

方框 21. 案例研究：資金轉移到受國家制裁的 VASP

作為對使用新技術進行洗錢和規避制裁的更廣泛研究的一部分，烏克蘭的金融情報中心（FIU）發現加密貨幣交易所之間可疑的資金流動，包括國內制裁的 VASP。

FIU 發現，一家加密貨幣交易所（A 交易所）是由位於歐洲和其他國家（包括英屬維京群島、香港、英國和愛沙尼亞）註冊的公司所組成，並且自另外兩家高風險加密貨幣交易所（B 交易所 和 C 交易所 ）接收虛擬資產。儘管 A 交易所的所有者註冊為愛沙尼亞公民，但該案件引起了烏克蘭 FIU 的興趣，因為該所有者被認為是烏克蘭重要應為” 重要政治性職務人士和烏克蘭政客的兒子。

A 交易所從 B 和 C 交易所獲得大量資金。B 交易所被認定為俄羅斯所有的 VASP，並於 2023 年根據烏克蘭國內制裁制度而受到制裁。C 交易所被認定為高風險交易所，其所有者因涉嫌洗錢 7 億美元而遭到逮捕。烏克蘭 FIU 指出， B 和 C 交易所透過 Tron 區塊鏈將虛擬資產轉移到 A 加密貨幣交易，所以掩蓋資金的來源和流動。

FIU 的調查結果，目前被視為審前調查的一部分。

來源：烏克蘭

方框 22. 案例研究：利用各種手段將資金轉移至北韓

2024 年 12 月，南韓對一個實體和 15 名個人實施制裁，包括金哲民和金柳松，他們都是位於鄰國的 313 總局局長，因他們代表北韓籌集資金、發動網路攻擊以及竊取虛擬資產。[43] 藉由鄰國協助者的幫助，北韓利用虛擬錢包、銀行、電子金融平台以及其他的法定貨幣帳戶轉移資金。北韓將部分非法所得兌換成法定貨幣後，然後向平壤匯出一大筆錢，並且用兌換後的虛擬資產的法定貨幣所得購買制裁物資，為該政權的 WMD 計畫提供資金。

313 總局負責控制北韓武器及其他軍事裝備的研發和生產。同時，313 總局也參與向鄰國和世界各地部署北韓的 IT 勞動力。

來源：南韓

81. PF 和規避制裁相關行為者正在利用日益複雜的方法以透過虛擬資產洗錢非法所得並且混淆資金來源。像是北韓等國家正在透過匿名增強技術進行這類活動，例如混幣器、宣稱去中心化金融（DeFi）的安排、跨鏈橋以及缺乏 AML／CFT 控制措施的 VASPs 來從事此類活動。洗錢後，規避制裁的行為者通常會在集中於一些司法管轄區的場外交易（OTC）經紀商，將虛擬資產轉換為法定貨幣。[44] 在一些實例中，北韓指示場外交易經紀商將兌換後的資金匯入前台公司所持有的銀行帳戶，這些前台公司代表北韓購買商品。如上所述，在一些範例中，北韓利用非法取得的銀聯金融卡接收遭竊虛擬資產所衍生的法定貨幣存款。

方框 23. 案例研究：制裁指定用於洗錢的混幣器

在 2023 年 11 月，OFAC 指定了參與為北韓洗錢的混幣器，其中包括 Sinbad.io（辛巴達）。[45] Sinbad 是北韓資助的駭客組織 Lazarus Group 的主要洗錢工具。Sinbad 處理被 Lazarus Group 竊得的價值數百萬美元的虛擬資產，其中包括 Horizon Bridge、Axie Infinity 和 Atomic Wallet 等備受矚目的竊盜案。與 Blender.io 類似，Sinbad 在比特幣區塊鏈上運行，而且藉由混淆交易的來源、目的地和交易對手的方式無區別地促進非法交易。

來源：美國

43 https://www.mofa.go.kr/www/brd/m_4080/view.do?seq=375771

44 https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html

方框 24. 案例研究：北韓刑事起訴與相關執法行動

2023 年 4 月，美國司法部公布兩項起訴書，指控北韓 FTB 代表參與洗錢陰謀，目的在於利用虛擬資產為北韓創造收入。據稱，該名個人與兩名場外交易員合謀對被盜的虛擬資產進行洗錢，並且透過位於香港的前台公司用美元代表北韓政府購買商品。

同時，OFAC 亦指定了一名個人列為制裁對象，因其收取數千萬美元的虛擬資產，這些資產部分來自美國公司在不知情狀況下僱用的提供 IT 開發服務的北韓人。這些 IT 工作者獲得工作時，據悉他們是要求以虛擬資產支付工資，並且大部分工資是透過複雜的洗錢方式，將這些非法取得的資金匯回北韓。表面上向 IT 開發工作者收取金錢後，FTB 代表指示 OTC 虛擬資產交易商向前台公司付款，讓這些前台公司能夠代表北韓政權以法定貨幣支付菸草和通訊設備等商品。這項行動是 OFAC 與司法部及聯邦調查局持續合作的成果，並與 韓國密切協調，該國也因該名個人的非法行為，將其列為制裁對象。

來源：美國

虛擬資產和資金產生

82. 一些國家發現北韓透過竊取虛擬資產和網路攻擊等方式在全球籌集資金，用於其 WMD 與彈道飛彈計畫。在進行這類活動時，北韓及其相關行為者通常以區塊鏈技術和虛擬資產產業的組織為目標，包括 VASPs、DeFi 服務、區塊鏈橋開發者、虛擬資產交易公司以及投資虛擬資產的創投基金。

83. 在 2024 年，聯合國北韓問題專家小組的一份報告強調北韓政權在全球進行的網路活動，調查了 2017 年至 2023 年期間北韓共計對虛擬資產相關公司發動的 58 起疑似網路攻擊，價值約 30 億美元。[46] 根據 Chainalysis，2023 年與北韓有關的駭客從 DeFi 平台竊取約 4.288 億美元，同時也攻擊中心化服務（被盜 1.5 億美元）、交易所（3.309 億美元）以及錢包提供商（1.27 億美元）。[47] 許多國家也強調北韓透過欺詐手段部署 IT 服務人員來取得資金（在一些情況下是以虛擬資產形式收取報酬）並規避制裁。北韓行為者利用前文所描述的方法來洗白虛擬資產所產生的收益。

46 S/2024/215

47 Chainalysis 2024 加密犯罪報告（第 44-46 頁）案例研究北韓的原子錢包運用。

方框 25. 案例研究：網路竊盜和詐欺

2021 年 2 月，美國司法部指控三名北韓電腦程式設計師參與了一項廣泛的犯罪陰謀，實施了一系列破壞性的網路攻擊，從金融機構和公司竊取並勒索超過 13 億美元的資金和加密貨幣，建立並部署多個惡意加密貨幣應用程序，同時開發和欺詐性行銷一區塊鏈平台。

起訴書稱，三名被告是北韓軍事情報機構偵查總局（RGB）下屬單位的成員國，該機構參與了犯罪駭客攻擊[48]。這些北韓軍事駭客組織在網路安全社群有多個名稱，包括 Lazarus Group 和進階持續性威脅 38 (Advanced Persistent Threat 38)（APT38）。

起訴書指控該團夥在美國國內和國外為報復或獲取經濟利益之目的進行一系列的網路犯罪活動。被指控的手法包含建立並部署惡意的加密貨幣應用程式；瞄準加密貨幣公司和竊取加密貨幣；魚叉式網路釣魚活動；以及海洋鏈代幣和首次代幣發行。

根據起訴書中的指控，三名被告是 RGB 部隊的成員國，這些部隊有時由北韓政府派駐到其他國家，包括中國和俄羅斯。雖然這些被告是被網路安全研究人員稱為 Lazarus Group 和 APT 38 的 RGB 部隊的一部分，然而起訴書指控這些團體參與一項陰謀，目的是要造成破壞、竊取資料和金錢，並且以其他方式進一步促進北韓的戰略與經濟利益。

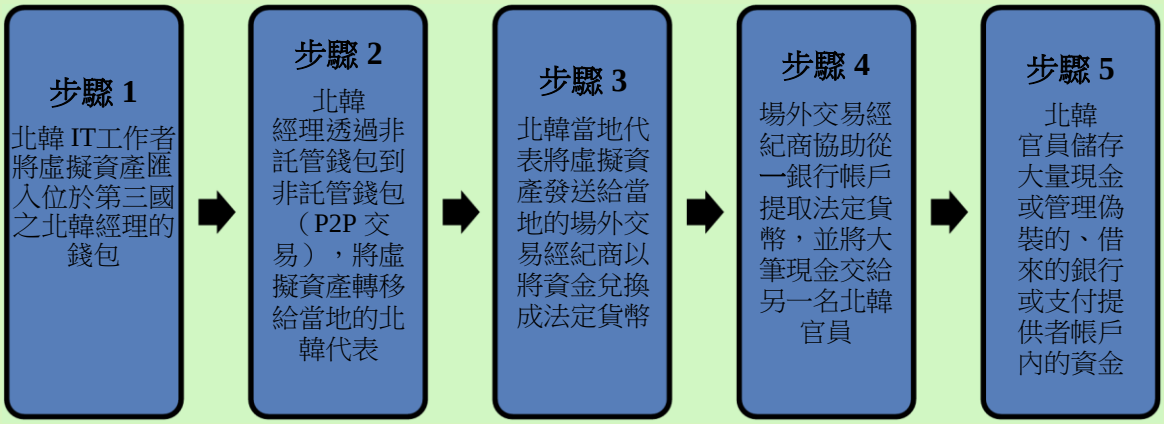
美國財政部和司法部也對兩名中國公民採取了行動，他們被指控透過加密貨幣交易所遭到駭客攻擊，洗錢超過 1 億美元的加密貨幣。根據訴狀，在 2018 年，北韓同謀入侵一家虛擬貨幣交易所，竊取價值近 2.5 億美元的虛擬貨幣。這些資金隨後透過數百筆自動加密貨幣交易進行清洗，目的是防止執法部門追蹤這些資金。訴狀進一步指控，2017 年 12 月至 2019 年 4 月期間，兩名被告對價值超過 1 億美元的虛擬貨幣進行洗錢，這些貨幣主要來自虛擬貨幣交易所駭客攻擊。OFAC 認定這兩名個人向 Lazarus Group 提供實質支援。

來源：美國

84. 此外，北韓向世界各地派遣數千名高技術 IT 工作者來創造收入，為其 WMD 和彈道飛彈計畫做出貢獻。這些 IT 工作者利用對特定 IT 技能，例如軟體和行動應用程式開發的現有需求，從亞洲、歐洲和北美等世界各地的客戶獲得自由工作雇用契約。在許多情況下，北韓 IT 工作者都以國際工作人員和／或非北韓遠端工作者的身分出現。利用協助人身分獲得專案的北韓 IT 工作者 可能會藉由分包專案以進一步掩蓋其身分和／或位置。這些資金透過各種方式被送回北韓以規避制裁，包括藉由運用中間人及掩蓋 BOI（詳見態樣 1 和 2）。虛擬資產也用於向北韓匯款。

[48] 在 UNSCR 第 1718 號決議名單上，RGB 被指定為 KPe.031。

方框 26. 案例研究：網路竊盜和詐欺



外國實體和個人實施欺詐以隱瞞與北韓 IT 工作者的豐厚交易

85. 並且，北韓 IT 工作者也吸收外國個人和公司，進一步掩蔽他們參與規避制裁手法以牟利的行為。在底下其中一案例例研究裡，日本公司成為與北韓相關的 IT 工作者籌集和轉移資金的目標。在另一個案例研究中，一名美國公民參與一項包括洗錢和身分盜竊在內的手法，以支援北韓 IT 工作者。

方框 27. 案例研究：用欺詐手段遮蔽與北韓 IT 工作者的豐厚商業關係

2024 年 3 月，一名擔任 IT 相關公司總裁的韓國公民與一名前員工因詐欺及其他罪名遭到逮捕。調查中發現，犯罪嫌疑人偽造記錄，要求據信位於中國的北韓 IT 人員透過線上平台開發由日本公司訂購的應用程式。這項活動被懷疑是為了支援一項規避制裁的手法，因為這些資金可能被用於北韓的 WMD 計畫而違反 UNSCR 第 1718 號決議。

2024 年 9 月，兩名日本人因與一名北韓 IT 員工合謀使用被禁止的「自動交易系統」進行外匯交易，並且在客戶資料庫中非法註冊和開立帳戶而被捕。這些嫌犯涉嫌將透過這些非法外匯交易獲得的資金匯往北韓。

來源：日本

方框 28. 美國司法部透過指控和逮捕 Nashville 協助者，挫敗北韓遠端 IT 工作者詐欺手法

2024 年 8 月，美國司法部公布一份起訴書，指控一名美國公民密謀洗錢貨幣工具並且觸犯其他多項罪行，目的在為北韓非法武器計畫（包括 WMD）籌措資金。根據法庭文件，該名被告參與一項協助海外 IT 工作者在美國公司獲得遠端 IT 工作的計畫，而這些企業誤認為他們僱用的是美國境內員工。實際上，這些 IT 工作者是北韓公民，他們利用被竊取的美國公民身分獲得這項遠端 IT 工作。

根據法庭文件，被告於 2022 年 7 月至 2023 年 8 月期間在其 Nashville 的住處經營一個「筆記型電腦農場」。受害公司將寄給「Andrew M.」的筆記型電腦運送到被告的住處。在收到筆記型電腦後，被告下載並安裝了未經授權的遠端桌面應用程式，並且存取受害公司的網路而導致電腦損壞。遠端桌面應用程式讓北韓 IT 工作者能夠在中國境內工作，同時讓受害公司看到「Andrew M.」正在被告位於 Nashville 的住處工作。

在 2022 年 7 月至 2023 年 8 月期間，與被告的筆記型電腦農場相關的海外 IT 工作者獲得超過 25 萬美元的報酬，其中大部分款項以遭盜用之美國公民的名義向美國主管機關虛假申報，包含向美國國稅局與社會安全局申報報稅紀錄。被告及其同謀的行為也導致受害公司在審計和修復其裝置、系統和網路方面耗費超過 50 萬美元的成本支出。被告與其他人士合謀洗錢，透過金融交易自受害公司收取付款，再將這些資金轉移到被告和美國境外的帳戶，試圖促進他們的非法活動並且掩蓋所轉帳資金為其所得。非美國帳戶包括與北韓和中國行為者有關的帳戶。

來源：美國

態樣 4：開發海事和航運業

86. 根據國際海事組織（IMO）的定義，*影子艦隊*或*黑暗艦隊*是指「[…] 為規避制裁而從事非法作業或從事其他非法活動的船舶 […]」。[49] 海運業已成為不法分子的主要目標，利用其複雜性、國際影響力、匿名性以及有限的 AML／CFT／CPF 控制。海運業涉及龐大的船舶、港口、物流和國際法規網路，不法分子可以利用這些網路規避制裁並且產生可貢獻於 PF 的收益。雖然 FATF 標準不涵蓋海運業，但是許多國家認為利用該行業作為其國家 PF 風險評估的關鍵弱點。為此目的，海事部門的各個層面及活動都有可能曝露於規避制裁和 PF 的風險，包括海上保險排設、海運公司、開放登記、商品貿易商和兩用貨品製造商。[50]

87. 不法分子可以採用一系列欺騙性的航運策略來掩蓋船隻、其來源或指名名單，遮掩其活動的真實性質並規避偵查。雖然技術上有重疊，不過手法可以區分為四種主要類別：船舶識別、船對船轉移、禁用或偽裝 AIS 廣播以及偽造文件。然而，重要的是注意到試圖實施 PF 和規避制裁手法的不法分子可以採取多種手法來達到他們的目標。

---

49 國際海事組織，「敦促成員國和所有相關利益相關者採取行動，防止『黑暗艦隊』或『影子艦隊』在海事領域從事非法活動」（2023 年 12 月 6 日）。A 1192 33

50 為協助成員國做好相互評估的準備並因應新出現的區域風險，APG 秘書處在聯合國毒品犯罪辦公室的支援下，發布一份船舶登記和 PF 風險狀況說明書：亞太防制洗錢組織

變更船舶識別

88. 如同在態樣 2 中所討論，不法分子可以掩蓋實質受益權資訊以迴避制裁制度並且進入正規金融體系。在海運領域，不法分子可以對商船進行物理改造使其偽裝成不同的載具，並且隱藏其身分以掩蓋其真實所有權和活動。例如，可以藉由漆塗船名、使用別名旗幟以及更改其唯一的 IMO 船舶識別號碼來篡改船舶的實體身分。透過對商船進行實體改造並掩蓋其身分，不法分子取得匿名性，並且可以遮蔽船舶非法活動的歷史。以下案例研究重點介紹一艘船隻改變其身分以規避 UNSCR 對於北韓的決議的範例。

方框 29. 案例研究：海運業透過非法煤炭產生收益

2022 年，在印尼海域巡邏的印尼當局扣留了 Petrel 8 號。在 2017 年，懸掛科摩羅國旗的散裝貨船 Petrel 8 號因向北韓非法運輸煤炭而被列入聯合國制裁名單。該案件牽涉到印尼當局與聯合國 1718 制裁委員會的協調。印尼外交部（MOFA）向印尼 FIU（PPATK）請求提供資訊，最終透過國際合作偵破該案。

調查顯示，印尼航運公司 PT Lintas Bahari Nusantara 從日本公司 UYO Co. Ltd 購得這艘船，價格約 50 萬日元，由 BCA 銀行提供融資。儘管初步調查並未發現與北韓有任何直接的財務聯繫，但是該船隻遭到扣留是因為它參與了對於北韓的持續規避制裁。他們以篡改船隻身分以及利用別名旗幟等方法來規避偵查。該船購買價約 610 億印尼盾（400 萬美元），用於向北韓運輸煤炭。收購 Petrel 8 需要將資金從一家印尼公司轉移到日本公司。

該案件凸顯出船舶所有權變更及非法貿易行為監控的弱點，同時強調需要加強國際合作以防止規避制裁。經過 2023 年與聯合國 1718 制裁委員會的討論，廢除 Petrel 8 的決定被認為是防止進一步規避制裁活動的最有效解決方案。

來源：印尼

船對船轉運

89. 船對船轉運的過程發生於貨物在公海的船隻之間搬移時。雖然船對船轉運是一種合法實務，但是這種實務被認為具有規避制裁的高風險，因為不法分子可能會採用這種方法來偽裝貨物的原產地或目的地。這使得政府當局更難追蹤受制裁的商品以及辨識違反國際制裁的行為。此外，缺乏透明度可能會造成海上保險公司在不知情的情況下，向參與非法船對船轉運活動的船隻提供航運保險。

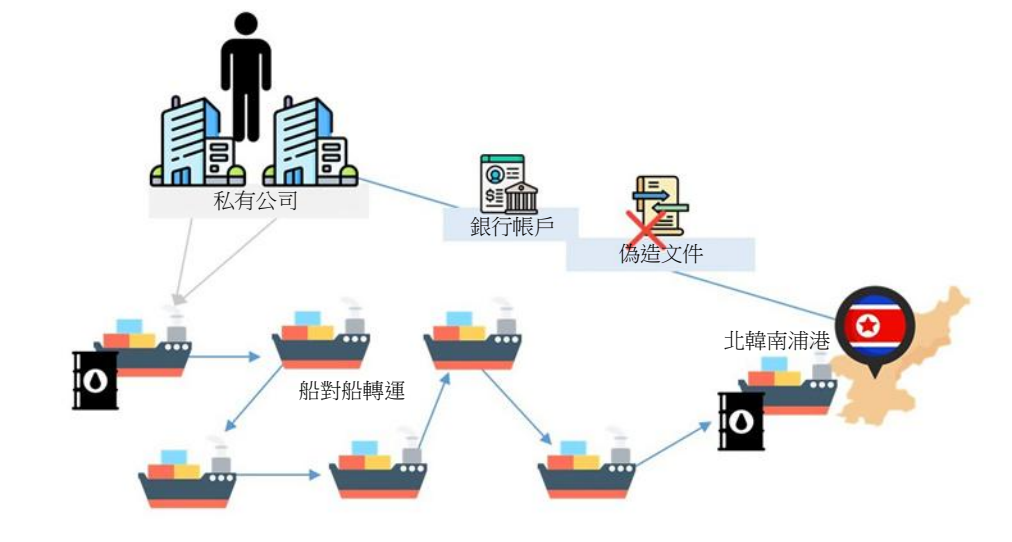
90. 根據一個司法管轄區報告，北韓擁有至少 28 艘能夠進行精煉石油產品船對船轉運的油輪，以及至少 33 艘能夠運輸煤炭的船隻。北韓進行的船對船轉運通常是未透過金融機構的現金交易，這凸顯了與財政援助和規避制裁風險相關的另一個弱點。下列案例研究，詳細說明不法分子如何運用船對船轉運來運輸違禁物品、規避制裁以及掩蓋真實的來源或目的地以規避偵查。

方框 30. 案例研究：利用海運業向北韓供應柴油

在 2019 年末，一名個人涉嫌與國外其他五人合謀七次利用船隻 MT Courageous 向北韓供應約 12,260 公噸柴油。前六次物資運輸皆經由船對船轉運進行，最後一次轉運是在北韓的南浦港進行。據稱，這些行動違反新加坡的聯合國北韓條例和 UNSCR 第 1718 號決議制裁制度。

為支付購買和供應柴油至北韓的費用，該名個人被指控四次利用他擔任董事的一家公司的銀行帳戶。該人亦據稱兩次偽造該公司的文件，並五次利用由其掌控之另一家公司的銀行帳戶收取向北韓禁止供應柴油的款項。除此之外，被告亦涉嫌向調查人員說謊、銷毀證據，也未告知警方另一艘船在 2019 年 2 月向北韓供應柴油。

從而，被告面臨多項指控，包括向北韓提供違禁物品、偽造帳目、透過犯罪行為獲取利益、妨礙司法公正，以及未揭露違禁交易。同時，被告擔任董事的第一家公司遭指控四項轉移金融資產的罪名，這些資產可能助長違反新加坡的聯合國北韓條例中的禁止活動，而第二家公司則面臨五項透過犯罪行為獲取利益的罪名。法庭訴訟正在進行。



來源：新加坡

方框 31. 案例研究：在公海上向北韓船隻轉移石油

從 2017 年 1 月至 2022 年 10 月，中華臺北檢察機關共調查了 11 件涉及北韓違反制裁的案件。[51] 牽涉到 PF 的最常見態樣是，由中華臺北石油公司控制的第三國管轄區的船隻在公海上向北韓船隻轉運石油，或者將石油轉交給第三國管轄區的船隻，然後再由第三國管轄區的船隻再轉售給北韓船隻。

[51] 其中五起案件遭到定罪，三起案件被判無罪，三起案件未起訴。

石油產品仍為中華臺北個人違反聯合國制裁規定交易最常見的商品。根據當地法律，在公海上進行石油貿易是合法的。航運公司的代表或實質受益人，包括外國公民、其他中介機構以及涉及複雜商業結構的人，以表面上合法的交易為中介，以掩蓋透過海上船對船隻轉運進行非法的石油轉運。他們也利用虛假出口資訊以及離岸公司和帳戶來阻礙資金追蹤。[52]

來源：中華臺北

停用及操縱自動識別系統廣播

91. 自動識別系統（AIS）是一種用於船舶的海岸追蹤系統，可提供識別和位置資訊，使當局能夠追蹤船舶移動。[53] 不法分子可操縱透過 AIS 廣播所傳送的資料，包括更改船隻名稱、IMO 編號或其他唯一識別資訊以幫助隱藏船隻的航行。並且，影子艦隊經常會禁用 AIS 廣播，實際上就是「變暗」並暫停對移動的追蹤。[54]

92. 根據各國報告，並反映在 UNSCR 第 2397 號決議（2017）中，懸掛北韓國旗、控制、租用或營運的船隻故意禁用或操縱 AIS 應答器以規避聯合國制裁，並且獲取收益，這些收益歷來是運用於該國的 WMD 和彈道導彈計畫[55]。下列的案例研究詳細描述兩起在民用船隻上偵知、扣押且沒收北韓原產煤炭的事件，這違反了聯合國安全理事會有關北韓的決議。

方框 32. 案例研究：偵查、扣押及沒收船上北韓原產煤炭

在兩起獨立事件中，柬埔寨發現北韓利用民用船隻協助出口煤炭，違反禁止此類活動的 UNSCR 第 2397 號決議和第 2375 號決議。在這兩起案件中，船隻和貨物均被沒收，並且涉案人員被判觸犯（1）非法進入柬埔寨和（2）意圖在柬埔寨海關區域內走私貨物的罪行。

根據聯合國義務，柬埔寨定期對從公海進入的財產和船隻進行調查與審檢，以發現其可能違反聯合國對北韓制裁的行為。有時，船舶會運用混淆技術來掩蓋其貨物的來源，像是關閉自動識別系統（AIS）來掩蓋船上的貨物、欺騙其位置或者進行船對船轉運。最近兩起船隻被扣押事件揭露了北韓船隻遮掩其非法貨物來源的手法。

在第一起案件中，一艘名為「HJL」的機動船（M／V）於 2024 年 2 月被柬埔寨當局扣押。該外國註冊船舶駛近北韓海域後，關閉了 AIS 廣播。次日，儘管該船仍在以虛假名稱航行，然其 AIS 廣播的位置顯示 HJL 號已拋錨。在 HJL 號進入柬埔寨領海後，柬埔寨當局於另一司法管轄區的協助下且提供關於可疑船隻的資訊將該船扣押。此次國際合作最終導致 HJL 號被扣押，該船載有 12,000 噸來自北韓的煤礦石。該船進入柬埔寨領海停泊，據稱是為與其買方會面。依照常規命令並考慮到船上物品，檢察辦公室凍結該船及其貨物以進一步調查和審判。

52 《資恐防制法》第 9 條第 1 項第 1 款的主觀要件要求犯罪嫌疑人「明知」與受制裁對象進行交易，然中間人的介入導致此要件的舉證困難。

53 國際海事組織，「船舶自動識別系統（AIS）船上操作使用指導修訂版」（2015 年 12 月 2 日）。A 1106 29

54 MO 規定，所有從事國際航行的 300 總噸以上的船舶以及所有客船，無論大小，均須使用 AIS。

55 UNSCR 2397

在 2024 年 5 月的第二起案件中，柬埔寨當局扣押了 M／V CNI 船隻，該船在北韓水域與一艘北韓船隻進行了船對船轉運，裝載了聯合國禁止的貨物，包括 4,800 噸煤礦石。而進一步調查發現該批貨物由第三國一家物流公司安排，該公司安排進口原產於北韓的煤礦石，不過透過偽造文件隱瞞其來源。

來源：柬埔寨

93. 上述兩個案例所顯示的漏洞，凸顯各國需要考慮增加監視頻率和巡邏力量，並且加強領海的追蹤系統，尤其是地理位置靠近國際水域的領海。

偽造文件

94. 掩蓋貨物來源或目的地的其他手法是在運輸源自或運往北韓的貨物時使用虛假文件，特別是對於兩用貨品的出口。在這種情況下，不法分子在貨物出發後更改運輸文件，藉此隱藏貨物的實際最終目的地。這種做法通常涉及在第三國設立空殼公司，而或多或少是由武擴實體直接控制。在海關當局和託運人看來，空殼公司是貨物的正式收貨人。然而，一旦貨物裝運，擔保人就會更改運輸文件，使得貨物重新定向到與 PF 相關的高風險司法管轄區。

95. 除了偽造涉及北韓的文件外，這也是規避其他地區制裁及出口管制的常見手法。以下案例研究重點，闡述不法分子如何在運輸過程早期操縱運輸文件，以掩蓋兩用貨品的出口。

方框 33. 案例研究：兩用貨品的偽造單據及不實申報

在 2021 年的許可證審核過程中，聯邦核子監管局（FANR）發現了一批含有兩用貨品的可疑貨運。X 公司位於 UAE 自由區，提交三份許可證以出口價值約 25,000 美元（95,040 迪拉姆）的逆變器。這些逆變器被列入 UAE 出口管制清單並且歸類為兩用貨品。由 X 公司所提交的文件包含一份提單和一份買賣單（BSP），其中關於賣方資訊和貨物原產國的資訊存在矛盾。文件指明這些貨物的目的地是高風險國家。

執法機構（LEA）的調查發現，X 公司提交了一份偽造的提單，該提貨單宣稱自己是託運人，而 BSP 則將賣方認定為位於 T 國的另一家公司。LEA 經過進一步調查後也認定，所謂的賣家主要從事堅果貿易，因此其業務與貿易交易不一致。進一步調查發現，這些物品其實是賣家自 H 國進口到 UAE。X 公司亦提供在 U 國擁有多個分公司的偽造文件，藉以誤導當局並規避對伊朗核計畫的制裁。

LEA 與 UAEFIU、CBUAE、EOCN、聯邦海關總署以及 FANR 合作進行刑事和財務調查。對 X 公司經營場所的實地檢查發現，該公司是作為位於高風險國家的逆變器買家的掩護公司。UAEFIU 及 CBUAE 查明並凍結與 X 公司有關的三個銀行帳戶，總餘額為 34,000 迪拉姆（9,500 美元）。此外，海關向 LEA 提供所有已查明且與試圖掩蓋實質受益權（BO）之分包進出口方有關的偽造文件。

FANR 準妥有關該批貨物的技術報告，並且向 LEA 提供確認，證實該物品是 UAE 出口管制清單中列出的兩用貨品。海關當局扣押這批貨物，LEA 下令凍結這批貨物（價值 95,040 迪拉姆 (約 26,000 美元)）。

來源：阿拉伯聯合大公國

方框 34. 案例研究：未依出口國規定的出口法律申報兩用貨品

2020 年，印度海關當局扣押了一艘懸掛亞洲國旗駛往巴基斯坦的船隻。在調查過程中，印度當局證實文件錯誤申報了這批貨物的兩用貨品。印度調查人員認定，這批待裝運的物品為「高壓滅菌器（Autoclaves）」，用於存放敏感的高能量材料以及導彈發動機的絕緣和化學塗層。這些敏感物品被列入在飛彈技術管制制度、印度和其他司法管轄區的兩用出口管制清單內。[56]

被扣押貨物的提貨單，證明了進口商與參與遠程彈道飛彈研發的國家發展綜合體之間的關聯。

來源：印度

[56] 未經相關部門正式核准而出口此類設備違反現行法律和契約。

5. 第 3 節。降低 PF 相關風險的挑戰和良好實務

透過 SARs／STRs 和制裁篩檢進行偵查

96. 為發現 PF 和規避制裁手法，各國嚴重依賴 SARs／STRs 義務和強力的制裁篩檢比對。為補充這些技術並且有效地識別與解決全球範圍內的非法活動，其他偵查方法包括共享跨境情報、機構間協調、國際合作以及包括開源情報和區塊鏈分析在內的監控工具。

97. 許多國家報告稱，它們仰賴強力的 SARs／STRs 義務來偵查 PF 和規避制裁手法，藉以識別和打擊複雜且不斷演變的手法。不同的國內法律框架和報告義務可能會要求報告實體提交 SARs／STRs，因為它更廣泛地牽涉到 PF和規避制裁。許多國家指出，報告實體的義務範圍可能包括進行徹底的客戶盡職調查、符合法律的規定、監控涉及高風險國家的交易，以及當發現可疑交易時履行所有的 SARs／STRs 義務。

透過 SARs／STRs 和制裁篩檢進行偵查 PF 及規避制裁的良好實務

98. 此外，一些國家要求報告實體將自動制裁篩檢系統整合在報告實體義務內，這包括與內部政策和程序相關的義務，藉此提高 SARs／STRs 的有效性。將國際和／或國家制裁名單整合在制裁篩檢系統內，報告實體能夠藉此發現與個人或實體比對的名單，同時利用與高風險交易和受制裁的個人、實體或活動相關的關鍵字。在一些國家裡，如果在篩檢過程中發現的正面比對結果，則報告實體將承擔進一步的義務，提交 SARs／STRs 並且向當局通報因制裁而被凍結的資產，或與受制裁實體有關的交易。以下兩個案例研究顯示如何運用 SARs／STRs 來啟動調查。

方框 35. 案例研究：負面新聞篩檢以及 SARs／STRs 偵知兩用貨品的非法購買

兩家法國公司作為中間人購買了美國原產的兩用電子元件，然後透過一系列實體將這些元件轉售給一家受到美國制裁的俄羅斯公司。

該案件是經由法國當局與私部門合作，在 TracFin 針對相關個人和實體（實體的 UBO）發出「警惕呼籲」後，利用監控與俄羅斯相關的負面新聞以及銀行發布的 SARs／STRs，所偵得。TracFin 的出版物亦指出，該個人的妻子在丈夫被指定為 OFAC SDN 前不到一個月被任命為其中一個實體的經理。

調查需要強力的跨部會合作以及與金融機構的成功夥伴關係，包括定期後續追蹤涉案銀行以避免任何資本外逃，同時確保在調查期間現有資金實際上無法使用。

來源：法國

99. 一些國家透過公私部門合作夥伴關係，投資於訓練、推廣、專業指導和監測機制，以增強遵循性並提高偵查能力。為此目的，發表諮詢、指導或者國家或國際確定的指標，能夠幫助報告實體偵知可疑的規避制裁和 PF 活動，並提交具體的 SARs／STRs 以履行其義務。有些國家也訂定國內法律框架，要求受監管實體根據這些建議或警報提交 SARs／STRs 以進一步增強偵查能力。

方框 36. 案例研究：發布詳細警報，使得金融機構（FIs）更易於提交 SARs／STRs

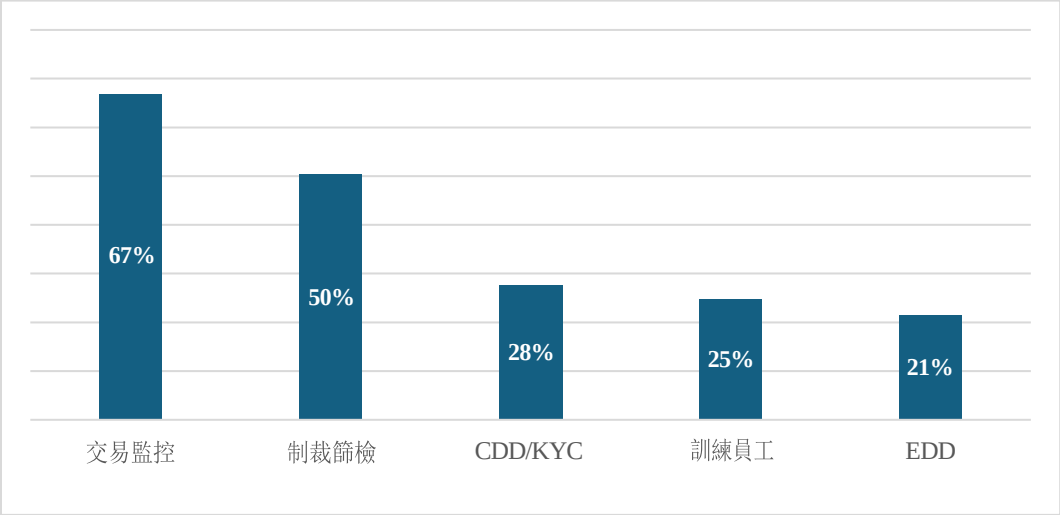
為方便金融機構提交與規避美國對俄羅斯和白俄羅斯出口管制有關的 SARs／STRs，BIS 和 FinCEN 發布了 2022 年聯合警報，向金融機構概述 BIS 目前的出口限制；一份可能規避出口管制的關注商品清單；以及選擇交易和行為紅旗警訊來協助金融機構識別與涉嫌可能與出口管制相關的可疑交易。該警報也要求金融機構在提交 SARs／STRs 時使用關鍵字「FIN-2022-RUSSIABIS」。

在該警報上擴展，BIS 及 FinCEN 於 2023 年 11 月發布一項聯合警報，強調與全球規避出口管制有關的紅旗警訊。該警報要求金融機構在提交 SARs／STRs 時使用關鍵字「FIN-2023-GLOBALEXPORT」。FIs 提交的 SARs／STRs 中包含與俄羅斯相關之關鍵字的數量多於包含全球出口關鍵字的數量，這主要是因為對俄羅斯和白俄羅斯實施的出口限制更為廣泛，FIs 更容易在他們接收到的資訊中識別出潛在的相關金融交易。

來源：美國

100. 根據大多數回應於 FATF 公開諮詢的私部門實體，降低與規避制裁和 PF 相關之風險的最佳方法是關聯於關鍵性的 AML／CFT 預防措施，像是客戶盡職調查、全面的風險評估、制裁篩檢工具、可能導致提交 SARs／STRs 的持續性監控、員工培訓、政策與程序、負面新聞篩檢，以及加強盡職調查（EDD）（私營部門最常引用的良好實務詳見圖 3）。並且，基於貿易的洗錢預防措施、即時警報和先進的技術解決方案也被認為很重要。然而，由於缺乏強有力的資訊共享機制，私部門可能難以透過標準風險管理程序，以偵知複雜的 PF 和規避制裁手法。

圖 3. 偵查規避制裁行為的良好實務



透過 SARs／STRs 和制裁篩檢以偵查 PF 和規避制裁的挑戰

101. 近三分之一的國家沒有報告使用 SARs／STRs 作為偵查 PF 的方法。由於相當多的國家沒有將 PF 定為犯罪，這也許可以解釋為什麼有些國家在一定程度上不依賴 SARs／STRs。不將 PF 視為刑事犯罪的國家或許不太可能要求報告實體在 SARs／STRs 中識別 PF。相反而言，報告實體可能會提交涉及 PF 行為者的 SARs／STRs，但是如果沒有對於這種非法活動的複雜偵查性質的進一步指導，那麼就可能會缺少將它們與 PF 行為者聯繫起來的重要資訊。

102. 同時，將制裁名單整合到國家 SARs／STRs 框架內並利用篩檢工具，可以在發現可疑的 PF 和規避制裁行為方面扮演核心角色。一些國家指出，制裁篩檢比對存在挑戰，因為他們體驗到基於通用關鍵字搜尋的個人／實體或無關資訊的錯誤正面比對。此外，由於需要比對多個識別符，包括出生日期、姓名、別名、多個版本的名稱、名稱的語音、拼寫差異及護照號碼，因此，比對演算法容易偵得錯誤的正面結果。然而，抵減措施可包含 EDD 、利用像是公司登記機構或實質受益權資訊（BOI）等開源情報，以及與其他的資料庫核實資訊。

103. 各國報告的另一項挑戰是經指定之非金融事業或人員（DNFBPs）對 PF 義務的理解與法令遵循程度較低。許多 DNFBPs 實體並未意識到他們在監測和報告 PF 相關活動方面的責任。[57] 在一些國家中，這可能使得當局難以發現金融機構以外部門的 PF 活動。不過，各行業的私部門實體報告稱，公共部門缺乏對相關 SARs／STRs 的回饋，這可能會使得因應這項挑戰變得更困難。

[57] 關於 FIs、DNFBPs 及 VASPs 的風險抵減措施的進一步資訊，詳見 2021 年《FATF PF 指導》中的第二節，PF 風險抵減。

其他的偵查方法

104. 為補充 SARs／STRs 和制裁篩檢比對，其他的偵查方法包括跨境情報、透過機構間協調和國際合作進行資訊共享，以及監測工具。值得注意的重點是，各國通常會整合多個偵查來源，以構成對非法資助和規避手法的全面瞭解。

105. 許多國家報告稱，海關當局以及跨境情報部門在偵查和調查與 PF 相關的活動，尤其是與高風險國家和貿易路線的鏈結方面，發揮關鍵性的作用。海關機構與地區和國際機構合作，並且能夠交換有關調查、海關申報、進出口資料和許可申請的資訊，藉此提高偵查能力並調查與武擴資助者規避制裁有關的潛在違規。這種交換可改善偵查能力而且有助於調查潛在的違規行為。尤其，這個領域的關鍵活動包括分析和監控對外貿易營運和貨物移動，包含流向高風險國家的資產、國防材料以及戰略和兩用貨品。情報共享，連同確保遵循的司法監管框架，凸顯海關當局在發現與 PF 和規避制裁相關的潛在違規行為方面扮演著關鍵角色。

透過其他偵查措施來偵查 PF 和規避制裁的良好實務

跨部會協調

106. 多數國家皆強調跨部會協調在偵辦 PF 及規避制裁上的重要性。具體而言，LEA 的調查和與其他權責機關的資訊交流，可以促使國內機構轉介案件、進行聯合調查並提高意識，如此有助於識別出指定個人和實體的資金及／或資產的流動情況。情報收集與調查工作的結合，是一種識別和偵知涉嫌 PF 與規避制裁案件的多元學科方法。

方框 37. 案例研究：受控兩用貨品出口的跨部會協調

在 2017 年，FINTRAC 收到加拿大執法部門自願提供的資訊，顯示一家加拿大電子公司疑似牽涉到受控兩用積體電路的運輸。

SARs／STRs 表明，該公司的交易活動與俄羅斯和東歐洗錢計畫的某些關鍵特徵一致。一份 SAR／STR 表示：

- 資金來自高層個人；
- 位於像是俄羅斯、亞塞拜然以及其他東歐國家的個人；
- 高層個人開設空殼公司以達洗錢目的；
- 註冊於避稅天堂國家的空殼公司；
- 透過避稅天堂國家的空殼公司匯出的資金。
- 該公司從可能的中間國家（包括一些歐洲國家）接收電子資金轉帳，以用於轉運兩用貨品或者其他的非法金融活動。在一些實例中，原產國與負責訂購電子資金轉帳之實體所明列的地址不符。此外，該公司也是地址列於俄羅斯的個人和實體所訂購之電子資金轉帳的受益人。

SAR／STR 指出，該公司的資金藉由向股東開出多張支票，並且透過向線上支付處理公司進行電子資金轉帳而耗盡。

當被問及 FINTRAC 揭露有關該公司之情報的影響時，加拿大執法部門表示，揭露的資訊引發新的調查，並且為他們提供額外的未知主題。他們特別指出，FINTRAC 的揭露與合作是他們了解所涉及的網路以及其案件整體執法成功的關鍵因素。他們補充說，FINTRAC 提供的資訊有助於在夥伴國家尋求正式起訴。

來源：加拿大

107. 除此之外，一些國家強調，發布指導產品，這可能包括趨勢、樣態及指標，對於發現可疑活動極為重要（詳見國內協調與協作乙節）。

國際合作

108. 鑑於 PF 和規避制裁的全球性，透過情報和資訊共享進行國際合作是偵查及預防的主要手段。有效的偵查措施需要國內當局與國際合作夥伴之間的協調。例如，金融情報中心（FIUs）可以透過 Egmont Group 進行資訊共享，該集團在促進 FIUs 之間的資訊共享、加強對與 PF 或制裁相關之可疑金融活動的偵查方面發揮關鍵作用。並且，國際合作可以協助各國系統性地分析與國際貿易活動相關的風險，有助於加強國家風險狀況。

監控工具

109. 監控工具在檢測 PF 和規避制裁方面也具有重要作用。這些工具利用各種資料來源，包括開源情報和複雜的區塊鏈分析技術。權責機關可以利用開源情報獲取廣泛的資訊，這可包括公司註冊、實質受益權資訊、衛星影像和地理空間資料，從而揭露不法分子的網路。

110. 一些國家也指出，區塊鏈分析工具有助於偵測規避制裁和 PF 活動。虛擬資產的使用可能會另增偵查的複雜性，但是在公共區塊鏈上運行的虛擬資產交易是可以追蹤的。區塊鏈分析使得權責機關能夠監控和追蹤資金流，辨識可疑活動，並且抵減虛擬資產的一些混淆行為。更多資訊詳見態樣 3（利用虛擬資產和其他技術）。

透過其他偵查措施來偵查 PF 和規避制裁的挑戰

111. 許多國家報告了在偵查方面遇到的多項挑戰，包括制裁計畫的管轄權差異以及相關制裁實體名單、國家法律要求和各種執法規定。另一個關鍵挑戰是北韓利用外交人員以協助提供金融服務或轉移受制裁的資產或資源，包括運送大量現金。北韓仰賴於運用外交豁免權以規避管制和調查措施。許多國家擔心實質受益權資訊的收集和／或可用性不一致，這進一步增加 PF 和規避制裁的偵查複雜度（更多資訊詳見樣態 2 和弱點乙節）。

調查和起訴

112. 自從 2010 年發布 FATF 的報告*《打擊 PF：2010 年政策制定和諮詢的狀況報告》*以來[58]，預防和打擊 PF 及規避制裁的法律框架可能已經顯著加強，然而在 2025 年，有效調查及起訴的案例仍然很少。如同 2010 年 FATF 報告所述，起訴 PF 案件的困難歸因於幾個挑戰，包括：PF 的非刑事化；PF 案件中的證據收集；PF 活動的國際性質；利用金融中介機構掩蓋非法活動；出口管制框架無效；缺乏對 WMD PF的普遍接受的定義；以及在該主題上的司法方法存在差異，包含國際合作。根據由 FATF 全球網路提交的報告，許多相同的核心挑戰似乎仍然是成功調查且起訴複雜 PF （以及規避制裁）案件的障礙。

58 《打擊資武擴》

調查技術與機制

PF 調查的良好實務

113. 許多國家報告稱，有效的 PF 和規避制裁調查是依據金融犯罪案件之標準程序的運用以及相關機構間合作夥伴的協力合作而定。SARs／STRs 是對於識別及瞭解金融活動中異常模式的關鍵輸入。利用 SARs／STRs 亦有助於揭發牽涉到規避制裁與非法活動的企業和個人之間的鏈結。

114. 一些國家報告稱，另一個重要的調查手段是追蹤虛擬資產，有時虛擬資產被用來躲避偵查。調查人員可以透過區塊鏈分析追蹤資金，即使金額很小，也能揭開財務模式以及與相關實體和個人的關聯。

115. 藉由發現財務資料中的模式及異常活動，進階分析在打擊 PF 方面發揮重要作用。這些工具可以幫助調查人員發現實體之間的鏈結，並識別涉及規避制裁的人員或企業網路。例如，高級分析支援鏈結分析，將帳戶、交易和各方連接起來以顯示非法網路如何運作。即時監控工具使得當局在偵得可疑活動時能夠迅速採取行動。結合來自於金融機構、海關記錄和情報報告等不同來源的資料也讓調查更為有效且完整。這些工具可以進一步辨識出非尋常的交易模式或者當使用隱私增強技術以隱匿資金來源時可予偵得。當資訊能夠在各機構之間共享時，這些工具在對抗 PF 方面會變得更加有效。

116. 一些國家報告了考慮採用與調查跨國犯罪嫌疑人和販毒者相同的手法的重要性，例如運用臥底探員和秘密消息來源。

方框 38. 案例研究：使用臥底探員和秘密消息來源打擊核子材料販運者

在 2024 年 2 月 21 日，美國司法部（DOJ）和美國緝毒局（DEA）宣布，發布一份替代起訴書，指控一名被告與同夥網路合謀將核子材料從緬甸販運到其他國家。在這次陰謀中，被告及其同夥向一名假扮成毒品和武器販子的 DEA 臥底探員（「UC-1」）在泰國展示了核子材料樣本。在泰國當局的協助下，該等核子樣本被查獲扣押並隨後移交給美國執法部門保管。美國核子法醫實驗室隨後對樣本進行分析，確認樣本中含有鈾和武器級鈽。

被告及其同案被告先前於 2022 年 4 月被指控犯有國際販毒和槍支罪，並且被勒令拘留。

根據替代起訴書中的指控，從 2020 年初開始，被告告知 UC-1 和 DEA 機密消息來源（「CS-1」），並稱能夠接觸到他想要出售的大量核子材料。同年稍晚，被告向 UC-1 傳送了一系列照片，照片中顯示岩石物質帶有蓋革計數器測量輻射，同時也傳送幾頁被告聲稱是實驗室分析結果的資料，表明所述物質裡含有釷和鈾。在被告的反覆詢問下，UC-1 同意作為 DEA 調查的一部分，幫助被告將其核子材料出售給 UC-1 的同事，該名同事假扮為伊朗將軍（「將軍」）以運用於核子武器計畫。被告隨後提出，向將軍提供比鈾「更好」且「更強」的「鈽」以達此目的。

在討論被告取得核子材料的問題時，被告也與 UC-1 討論了他希望購買軍用等級武器的意圖。為此，2021 年 5 月，被告向 UC-1 傳送了一份武器清單，其中包括地對空飛彈，他希望代表緬甸一個民族叛亂組織（「CC-1」）的領導人從 UC-1 購買這些武器。被告連同另外兩名同謀（「CC-2」和「CC-3」）向 UC-1 提議，讓 CC-1 透過被告向將軍出售鈾以資助 CC-1 的武器購買。

2025 年 1 月 8 日，被告承認密謀自緬甸向其他國家販運鈾和武器級鈽等核子材料，以及國際販運毒品和武器的指控。

來源：美國

117. 最後，許多國家強調透過定期會議進行跨部會合作的重要性，包括建立專門工作小組和專家工作小組。當金融機構、海關當局和執法機關共同合作時，他們可以加強調查，並且主動凍結與 PF 和規避制裁有關的資產及停止運輸。

方框 39. 司法管轄權範例：專門工作小組和工作小組打擊 PF 和規避制裁行為

- **法國**：由金融情報中心 TracFin 領導的專門工作小組對兩家向受制裁之俄羅斯實體供應電子元件的公司（實體 A1 和 A2）進行調查。這些公司作為中間商，購買零件並且透過第三國的另一家公司將其轉移給受制裁的集團。該工作小組包括 TracFin、金融機構和執法機構。他們分析銀行提交的 SARs／STRs，監控公司的資金流動，並且追蹤實質受益人的參與情況。他們的協調努力導致這些公司的資產遭到凍結並停止營運。

- **印尼**：工作小組對一艘散裝貨船，Petrel 8，號進行調查，該船涉嫌違反聯合國制裁向北韓運送煤炭。該工作小組是由外交部、海關當局和金融情報中心（PPATK）組成。他們結合金融情報和航運記錄以識別出該船歸屬於一家印尼公司，並且先前曾因類似活動受到制裁。該工作小組與聯合國制裁委員會協調，最終扣留該船並拆解。

來源：法國和印尼

進行 PF 調查的挑戰

118. 總體而言，PF 調查在許多方面與洗錢（ML）和資助恐怖主義（TF）調查有所區別。PF 專注於資助有助於支援 WMD 計畫的活動。它通常涉及強大的國家行為者或團體利用前台公司、貿易和複雜的所有權結構來規避制裁。不同於隱藏非法資金來源的 ML 和資助恐怖主義的 TF，PF 調查更依賴與潛在違反出口管制和制裁有關的情報。PF 的調查難度較大，因為人們對其風險的認識較低，而且它經常牽涉到合法商品（包括受管制商品）被用於非法目的。調查人員需要加強國內和國際合作，並且採用先進的分析工具來解決 PF 案件，這可能比 ML 或 TF 案例中通常需要的更加複雜。

119. 許多國家報告面臨類似的挑戰，包括利用空殼公司、多層化所有權架構，以及小額但頻繁交易等的 PF 手法、。這些手法使得相關各方，包括執法機構、監管機構、金融機構、金融情報中心以及檢察官，面臨困境，因為他們依靠正確的資料和強力的協作來追蹤參與複雜手法的實質受益人或組織（見態樣 2）。

120. 另一個挑戰是金融機構和其他受監管實體缺乏對 PF 風險、趨勢和方法的認識，包括缺乏足夠的 PF 風險培訓來強化 SARs／STRs 的品質。正如本報告前一節所述，許多國家並未將 PF 定為犯罪。這可部分解釋相關 SARs／STRs 的數量和品質方面的缺陷。

121. 更廣泛地說，政府當局和私部門實體之間的資源有限，也是許多國家面臨的挑戰。尤其，較小的國家可能沒有足夠的資金或專業知識來處置複雜的案件。這也可能是優先排序的挑戰，會對公私部門的資源分配造成影響。雖然一些國家可能已經建立包括 PF 在內的主要罪行，或者利用附帶罪行來起訴 PF 行為，但是缺乏對犯罪化採取一致態度的國家，可能會破壞調查並起訴 PF 相關案件的國際合作。

122. 最後，跨境案件需要與其他國家的合作，然而法律體系的差異，例如考慮可採納證據的不同規則、對金融犯罪的不同定義以及缺乏雙重犯罪，給開展跨境調查帶來挑戰。如果國家之間沒有達成資訊共享協議，調查資訊請求可能會嚴重延誤或被拒絕（詳見國際合作乙節）。

起訴和其他方法

PF 起訴的良好實務

123. 許多國家報告稱，起訴複雜的 PF 和規避制裁案件比調查這些案件更為複雜。成功起訴 PF 和規避制裁案件需要強力的法律框架，包括明確定義 PF 及其相關活動的法律，以及在法庭上收集與展示證據的能力。

124. 調查部門和檢察官之間的協調努力對於建立強力的案件也極為重要。熟諳先前案例，並且明瞭 PF 和規避制裁的犯罪者所運用的態樣知識與新方法，能夠提高成功調查且因而成功起訴的機會。同時，全球夥伴關係可以在 PF 起訴中發揮重要作用，彰顯出國際合作在解決這些複雜犯罪方面的價值。最後，嚴格的沒收和資產追回規定可能會導致更多的起訴，特別是針對流出國外的資金。

起訴 PF 案件的挑戰

125. 多數國家報告稱，起訴複雜的 PF 和規避制裁案件具有挑戰性。有些國家指出，很難提供證據證明受管制或禁止的貨物被送往受制裁的司法管轄區。而當無法克服這些證據挑戰時，有一些範例是檢察官依觸犯像是妨礙司法公正或偽造罪的其他罪行來掩藏其 PF 罪行以追捕犯罪者。其他國家提到外交豁免權可以限制對某些 PF 或規避制裁案件的追究。

126. 各國面臨的另一個挑戰是證明金融活動與 PF 或規避制裁直接相關，尤其是當證據分散在不同國家時。這會要求詳盡的文件和強力的國際合作，然而在如此複雜的情況下，要達成這些要求並非易事。

127. 國家之間共享資訊和情報有助於填補執法隔閡，而且各國能夠更有效地處理跨國案件，並防止 PF 網路利用全球金融體系的弱點。然而，許多國家缺乏這些機制。

128. 儘管許多金融機構、企業甚至檢察官都缺乏對 PF 的風險和複雜性的瞭解，但是培訓及提高意識對於成功起訴也非常重要。提供適當的訓練可以幫助他們認知可疑活動並且明瞭 PF 手法的運作方式。這尤其對於資源有限或缺乏處理 PF 案件專業知識的國家來說非常重要。

阻止違反制裁的其他措施

129. 如本節所述，政府當局可能會考慮對違反 TFS 的行為提起刑事訴訟。此外，一些國家也考慮其他執法方案來糾正 TFS，包括與 PF 相關的違規行為。由於許多國家在起訴複雜的 PF 和規避制裁案件時似乎面臨著顯著的挑戰，因此在適當的情況下可能值得考慮採取其他措施。

方框 40. 司法管轄權範例：民事及刑事執法行動作為刑事訴訟的補充或替代

- **歐盟委員會**：歐盟 2024 年 4 月 24 日第 2024／1226 號指令引入了新規則，目的在於為所有成員國的自然人刑事處分以及法人的刑事或非刑事處分建立共同的基本標準，關閉現有的法律漏洞，並且首先增加違反歐盟制裁的威懾效果。[59]
- **英國**：違反財務制裁可能構成刑事犯罪，一經定罪，最高可判處七年徒刑。有民事和刑事兩者執法選項來補救違反金融制裁的行為。執法機構可能會考慮對違反金融制裁的行為進行起訴。2017 年法案建立的罰款制度為違反金融制裁法規的行為提供刑事起訴的替代方案。OFSI 是英國財政部負責實施這些罰款的部門。[60]
- **美國**：OFAC 的調查和執法權力完全屬於民事性質，與 DOJ、DHS 和商務部在此領域所行使的刑事制裁執法權力不同。在適當的情況下，執法行動顯現強力且有效的制裁法令遵循計畫的重要性，特別是對於參與複雜國際交易的公司而言，以確保採取措施防止牽涉到規避制裁手法。
- 在 2023 年 4 月，菸草和香菸製造商 British American Tobacco（BAT）同意支付 508,612,492 美元，以解決其因明顯違反 OFAC 對北韓和 WMD 擴散者的制裁而可能承擔的民事責任。在出口菸草及相關產品並收取這些出口貨款的過程中，BAT 促使美國金融機構處理包含受制裁之北韓銀行凍結財產權益的電匯，同時出口金融服務且協助向北韓出口菸草。[61]
- 在 2022 年 4 月，OFAC 與總部位於澳洲的國際貨運代理和物流公司 Toll Holdings Limited（「Toll」）達成和解協議，因為該公司明顯違反多項制裁計畫，包括處理涉及北韓、伊朗和敘利亞的交易。一個關鍵的漏洞是 Toll 的法令遵循職能缺乏足夠的風險管理與盡職調查。[62]

來源：歐盟委員會、英國和美國

國內協調與合作

跨部會機制

59 新規則的目標是要確保所有成員國皆能對這類違法行為進行刑事調查和起訴。這些包括與違反和規避歐盟制裁有關的一系列刑事犯罪，例如像是：未能凍結資產；違反旅行禁令和武器禁運；提供禁止或限制的經濟和金融服務；將應予凍結的資金轉移給第三方，或者提供虛假資訊以隱瞞應予凍結的資金。其中也包含加強凍結及沒收歐盟制裁所得、工具和資產的規定。除此之外，新規則旨在加強成員國權責機關之間，以及成員國與其他相關歐盟單位、機關、辦事處和機構之間的合作與溝通。

60 金融制裁執行和罰款指導 - 英國政府

61 根據法庭文件，英美菸草新加坡行銷公司（BATMS）對哥倫比亞特區提交的刑事資訊表示承認犯行，該資訊指控 BAT 及 BATMS 合謀實施銀行詐欺和合謀違反 IEEPA。BAT 就同一指控達成延期起訴協議。

62 Toll 透過美國金融機構促成近 3,000 筆與海運、空運及鐵路運輸相關的付款，而透過美國金融機構，使得受美國制裁或者位於受聯合國或美國制裁之國家的個人或實體受益。在超過一半的相關期間內，Toll 的法令遵循職能未能考慮與其營運複雜性相稱的政策和控制，其中包括分布在其各個業務部門的近 600 個發票、數據、支付和其他系統應用程式。執法行動顯示，在一家銀行對 Toll 遵照美國制裁的法令遵循情況表示擔憂之後，Toll 於 2016 年 6 月採取措施，停止與受美國制裁國家的所有業務，以降低其風險曝出。然而，Toll 並未實施必要的法令遵循政策和程序來防止涉及受制裁個人或實體的付款，也沒有測試貨物是否涉及位於聯合國或美國制裁管轄範圍內的人員。

130. 有效的跨部會機制有助於抵減與複雜的 PF 和規避制裁手法相關的風險。為了建立有效的跨部會框架，多國報告稱需要相關政府部門之間持續進行合作與協調。對許多國家而言，相關參與者包括 AML／CFT／CPF 官員、執法機構、監理機關、司法機關、進出口管制和許可當局、海關、邊境管制以及情報機構。多國報告稱，許多權責機關之間的密切合作與協調促進相關資訊的及時交流。透過這項跨部會程序，政府當局能夠給予最大協助啟動並展開對 TFS 制度和其他相關 PF 活動的潛在違規行為的調查。

跨部會合作的良好實務

131. 根據 FATF 全球網路提交的報告，各國採用跨部會機制以根據下列三種重疊類別其中之一來解決 PF 和規避制裁問題：1）對 TFS 的一般協調，包括 PF-TFS；2）專門關注 PF-TFS 和出口管制法規；或 3）專門關注 PF-TFS 和出口管制法規，以及更廣泛的協調，藉以啟動複雜的 PF 和規避制裁調查、起訴與其他措施。

132. 根據 FATF 建議第 7 項，FATF 全球網路有義務毫不遲延地實施 TFS 以遵守所有與 PF 相關的聯合國安全理事會決議。[63] 大多數國家都已建立實施 PF-TFS 的法律框架，其中通常包括運用現有的 TFS 跨部會機制。這種跨部會機制讓各國能夠履行其基於規則的最低要求，以解決建議第 7 項中提到的潛在違反、不實施或規避 TFS 的行為。

方框 41. FSRB 秘書處範例：GAFILAT 為成員國進行 TFS 凍結模擬演練

GAFILAT 正在進行模擬演練，讓成員國測試其依據 FATF 標準實施 TFS 的跨部會程序。根據 GAFILAT 訂定的方法和手冊，成員國回應於目的是要測試 TFS 能力和控制機制（包括公私部門的機制）的場景。

透過演練，GAFILAT 尋求為成員國提供實用工具以識別潛在的弱點並加強其 TFS 系統。演練結束後，GAFILAT 提供一份非公開報告，為該國提供回饋及指導。自 2024 年起，GAFILAT 為三個成員國進行過三次牽涉到 TF-TFS 程序的模擬演練。展望未來，GAFILAT 計畫展開更多模擬演練，包括針對其他成員國的 PF-TFS 程序的會議。

來源：GAFILAT

133. 在兩用貨品方面，出口管制當局負責監管大多數商業物品的出口，這些物品通常被稱為「兩用」貨品，即既有商業用途又有軍事用途或擴散用途的物品。[64] 許多國家超越了 UNSCR 第 1718 號決議規定的 TFS 要求，優先實施出口管制法規，作為打擊 PF 和規避制裁之更廣泛的風險管理工具。

---

63 這要求各國毫不遲延地凍結任何由聯合國安全理事會根據聯合國憲章第七章指定或授權的個人或實體，或代表其行事、按其指示行事、或由其擁有或控制的個人和實體的資金或其他資產，並且確保不直接或間接地向其提供任何資金或其他資產，或為其利益提供任何資金或其他資產。而前提是，代表指定個人和實體行事或受其控制或者由其擁有或控制者未被國家／超國家制裁制度所指定。

64 在涉及國家安全、外交政策、供應短缺、核不擴散、飛彈技術、化學和生物武器、區域穩定、犯罪控制或恐怖主義問題的特定情況下，需要取得雙重用途出口許可證。許可證要求是依照貨品的技術特徵、目的地、最終用途、最終使用者以及最終使用者的其他活動而定。即使無需許可證，出口前也可能會有其他的要求。以下兩個範例說明對與 PF 和規避制裁相關的出口管制法規的特別焦點。

方框 42. 司法管轄權範例：納入出口管制的跨部會機制法規

- **印度：**建立對於 PF 業務及政策協調的多個機制，包括對 SCOMET（特殊化學品、生物體、材料、設備和技術）核發許可的部際工作小組（IMWG），該小組負責討論兩用貨品出口許可申請及相關事宜。同時，根據印度 2005 年 WMD 法案成立的多機構協調機制是由印度金融情報中心（FIU-India）擔任主席，也包含監管機構、執法機構和其他相關組織的參與。[65]
- **新加坡：**出口管制部際委員會（IMC-EC）負責監督新加坡的出口管制框架，包括與 WMD 和 PF 有關的政策及營運問題。IMC-EC 是由外交部擔任主席並且由相關政策和執法機構組成。IMC-EC 也負責監督新加坡執行 UNSCR 相關決議的情況，同時當新加坡收到與 WMD 和 PF 有關的資訊／情報時協調跨部會後續行動。

來源：印度及新加坡

134. 即如本報告前文所述，明瞭這種 WMD 擴散的更廣泛風險及其潛在資助，可能對瞭解違反、不實施或規避 PF-TFS（即 FATF 標準中所涵蓋之 PF 風險的狹義定義）的風險有積極的貢獻，並且有助於實施基於風險的措施和 TFS。在此情境下，下列範例說明更寬廣的協調範疇，以啟動複雜的 PF 和規避制裁調查、起訴與其他措施。

方框 43. 司法管轄權範例：因應更廣泛的 PF 風險的跨部會機制

- **日本：**在由國家警察廳和財政部共同主持的 AML、CFT 及 CPF 政策跨部會委員會之下，財政部與金融廳進行「聯合檢查」，亦即他們聯合進行財政部的外匯檢查和金融廳的 AML 檢查，目的是要共享個別監管機構檢查官員的知識和檢查資訊，同時有用且有效率地確保金融機構遵守相關的法律及法規。此外，當日本海上自衛隊（JMSDF）艦艇或其他資產發現涉嫌非法海上活動時，包括 UNSCR 決議禁止的船對船轉運在內，防衛省會將資訊提供給相關省廳。
- **馬來西亞：**有兩個主要的跨部會小組補充馬來西亞 CPF 制度的多機構合作與協調：由投資、貿易和工業部戰略貿易控制員（STC）擔任主席的戰略貿易行動委員會（STAC)；以及由馬來西亞國家銀行擔任主席的國家反洗錢協調委員會（NCC）。STAC 主要負責 2010 年戰略貿易法（STA 2010）的實施，該法案規範戰略物項及技術的出口、過境、轉運和經紀，其中主要由與 PF 相關的執法機構和技術機構參與項目。NCC 由相關 AML／CFT／CPF 部門和機構代表，負責訂定、實行及監督打擊 ML／TF／PF 的國家策略。

來源：印度及新加坡

65 根據 WMD 法案的相關規定，印度設立各種諮詢委員會以處理有關 WMD 及其運載系統、核子及核子相關物品、化學武器及相關物品、生物等定期地召開武器和相關物項，以及兩用貨品出口管制，會議。該等會議包含印度政府相關組織的參與，藉以審議有關 WMD 法案和印度政府其他關於 WMD、其運載系統和相關兩用貨品和技術之相關規定的政策與相關事項。

- **美國：**出口執法部門（隸屬於美國商務部工業和安全局，BIS）可存取金融犯罪執法局（FinCEN）的銀行保密法（BSA）數據，與出口業界合作並進行調查以支援刑事及行政處罰。同時，根據 2018 年出口管制改革法案（ECRA）的授權，BIS 透過出口管理條例（EAR）監管並執行對兩用貨品、某些彈藥和商業物品的出口管制。BIS 與出口業界合作防止違法行為，並且進行調查以收集支援刑事和行政處罰的證據。BIS 亦與 FinCEN 和 OFAC 以及美國執法機構密切合作，監控透過 PF 進行的非法採購、規避制裁和規避出口管制手法的行為。

來源：日本、馬來西亞和美國

跨部會協調的挑戰

135. 各國報告對於成功的國內協調所遭遇的各種障礙，然而許多挑戰都與普遍缺乏對解決 PF 風險的理解和／或認同有關，特別是相較於 ML 和 TF。由於 PF 和規避制裁網路通常得到國家行為者的支持，因此需要與情報界進行定期溝通，獲取可操作的資訊對於揭露複雜的公司結構和解決規避制裁手法極為重要。

136. 然而，一些國家報告了情報共享的障礙，包括當牽涉到限制資訊存取的外國合作夥伴時。這項挑戰使得適時分享資訊與選項以採取立即行動來因應 PF 行為者或活動變得複雜。在一個司法管轄區內，缺乏瞭解 PF 的影響優先順序，這使得確保相關部門關注該主題、分享相關資訊和及時回應政府間提交的問題變得窒礙難行。[66]

137. 一些國家報告稱，缺乏相關資源、知識、經驗和技術來適當因應與 PF 和規避制裁手法相關的風險。雖然過往十年來，FATF 全球網路中的許多國家均投入資源，更新法律框架，以根據 FATF 標準解決 PF 問題，不過這並沒有顯著促進 PF 相關措施的有效實施。截至 2025 年 4 月，在第 4 輪相互評估過程裡接受評估的 194 個國家中，雖然超過一半（54%；105 個國家）遵循 R.7（13%；26 個國家）或大致遵循 R.7（41%；79 個國家），但是這 105 個國家中只有 24%（105 個中的 25 個）在 IO.11 上獲得高度或相當有效的評級。總體而言，17% 的受評估國家（194 個中的 32 個）在 IO.11 上得到高度或相當有效的評級（詳見圖 1 和圖 2）。

138. 然而，在建議第 1 項的情境下，建議第 7 項中提到的識別、評估和瞭解 PF-TFS 風險的義務正在宣導全球評估 PF 風險的努力，這可能會在未來數年增強有效性。超過一半的國家報告稱，他們在過去五年內完成 PF 風險評估或 NRA 中的 PF 章節，而近四分之一的國家正在進行其首次的 PF 風險評估，預期將在 2025 年底完成該程序。

公私部門之間的資訊共享

139. 公私部門合作機制（PPPs）可以成為加強利害關係人之間合作的寶貴平台。這些夥伴關係目的在於讓政府與私部門共享有用資訊（例如態樣、規避指標、良好實務、挑戰）。當公共部門共享可操作資訊時，私部門能夠更便於分析自己的客戶和交易

66 對於該專案，一些國家報告稱遇到了其自身的跨部會間障礙，對相關資訊和案例研究的共享造成限制。鑑於 PF 和規避制裁計謀的複雜性，一些國家報告稱無法解密情報以及／或者與 FATF 全球網路的其他成員國共享其他敏感資訊。

記錄，以利識別目前及歷史潛在的非法活動，包含潛在的規避制裁。慢慢地這種類型的交流增強公共部門識別及抵減風險的能力，並且針對私部門實體發布目標化指導，同時保留其維護客戶隱私的責任。

140. 為支援資訊共享，許多國家報告稱，它們正在訂定及監控 PF 和規避制裁手法的風險指標和紅旗警訊，而焦點是著重於交易與貿易模式（詳見附件 A：與資武擴有關）。一般來說，各國透過定期的宣傳和提高意識活動以與公私部門兩者共享風險指標清單。然而，近一半的國家沒有報告制定或維持這類的風險指標和紅旗警訊。這可能表明這些國家缺乏對 PF 風險指標和其他金融犯罪的區分，或者缺少對複雜 PF 和規避制裁的優先考量。由於大多數國家依靠 SARs／STRs 來偵查 PF 和規避制裁活動，因此公共部門和私部門之間可能存在資訊隔閡，故而損害預防措施的有效實施。

公共部門的良好實務

141. 大約三分之一的國家報告稱，他們的重點關注於透過實施其 TFS 法律框架以拓展私部門，包括接收 SARs／STRs 及毫不遲延實行 TFS。然而，同樣多的國家報告稱，透過各種 PPPs 模式，公私部門的協作更為穩健，而其主要重點通常並非 PF，即使是有工作小組或其他機制可供討論 PF 及規避制裁相關問題亦然。有些國家除了財政部、FIUs 和監管機構的參與外，也報告執法和情報主導的私部門外展活動。

方框 44. 司法管轄權範例：公共部門對 PF 和規避制裁向私部門外展

- **法國：**已建立「提高意識」機制，透過中央銀行下屬的銀行和保險監理機關以及財政部向私部門提供資訊與交流。除金融機構外，公私交流主要針對那些被認為風險曝露最高之行業的專業人士，包括 DNFBPs 和人道主義非營利組織（非營利組織，NPOs）。 FIU 不定期與法國金融實體（銀行和信貸機構）組織特定的會議，其中一些會議是針對於資武擴問題。這些報告實體對於該機構而言最為關鍵，因為它們佔 2023 年收到的 SARs／STRs 的 52.6%。這些會議有雙重目的：(i) 提高意識；(ii) 解決銀行在打擊 PF 框架內可能面臨的痛點及問題。TRACFIN 與一些法國主要銀行舉辦了一系列會議，以更加明瞭關於 PF 的法令遵循情況，並且就他們在發現 PF 案件和實行 CPF 機制方面遭遇到的挑戰獲得回饋。
- **美國：**美國商務部的 BIS 監管並執行出口管理條例（EAR），並與 FinCEN 和美國政府其他部門協調，定期為金融機構發布指導及建議。這些出版物包含紅旗警訊紅旗警訊和風險指標，以協助金融機構辨識出可能與規避美國出口管制有關的交易。最近的出版物重點關注全球規避制裁和出口管制、伊朗無人機（UAV）相關活動以及烏克蘭-俄羅斯衝突所引生的相關 PF 威脅。[67, 68, 69]

來源：法國和美國

67 FinCEN 與 BIS 聯合通知，FIN-2023-NTC2，2023 年 11 月 6 日

68 Microsoft Word - 伊朗 UAV 產業諮詢 - 最終發布日期為 6 月 9 日 10AM（003）

69 FinCEN 和 Bis 聯合警報 OCC-OGC-FO

挑戰公共部門

142. 鑑於 PF 和規避制裁的本質，以及國家行為者和情報收集的頻繁參與，通常會牽涉到難以公開分享的敏感資訊。許多國家都建立了 PPPs，不過其主要目標一般是改進 SARs／STRs 的有效運用，而專門針對 PF 或規避制裁問題的合作夥伴關係的範例則不多。大約四分之一的國家報告稱，他們收到 SARs／STRs 以此作為他們就 PF 和規避制裁相關問題向私部門進行外展的程度。然而，新加坡和英國利用 PPPs 來克服一些公共-私人以及私人-私人之間關於 PF 和／或規避制裁方面的資訊共享挑戰。

方框 45. 司法管轄權範例：克服 PF 和／或規避制裁的資訊共享障礙

- **新加坡**：2024 年 4 月 1 日，新加坡金融管理局連同新加坡六家主要商業銀行推出了數位平台 COSMIC，即「洗錢／資恐資訊和案例的協作共享」。如果達到規定的門檻，COSMIC 允許 FIs 彼此安全地共享展現出多個「紅旗警訊」的客戶訊息，這些警訊可能表明潛在的金融犯罪問題。這使得 FIs 更容易偵知並從而阻止犯罪活動。COSMIC 目前聚焦於商業銀行的三大金融犯罪風險：法人濫用、濫用貿易融資進行非法目的，以及資武擴風險。COSMIC 目標是要幫助 FIs 識別不法分子並立即採取行動中斷非法活動和網路，同時也支援金融系統的執法和監督。
- **英國**：執法機構（LEAs）經常運用聯合洗錢情報特別工作組（JMLIT）與私部門共享情報，而私部門則將情報分享給 LEAs。這使得私部門能夠瞭解戰略樣態和手法威脅。金融制裁實施辦公室（OFSI）最近成立了 JMLIT 規避制裁小組，由英國 FI 聯合擔任主席。

來源：新加坡和英國

私部門的良好實務

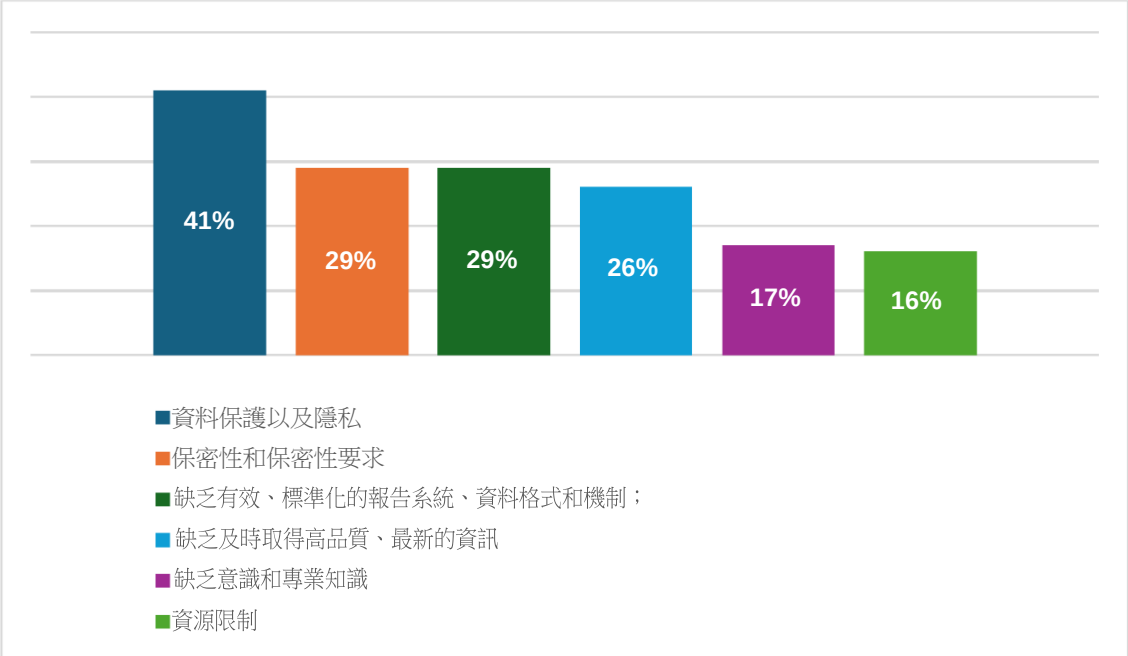
143. 許多私部門實體報告稱，PPPs 是促進在規避制裁和 PF 問題上公共-私人和私人-私人之間資訊共享的有用工具。然而，值得注意的是，私部門在資訊共享方面提供的挑戰範例遠遠多於良好實務（詳見後文對於私營部門的挑戰）。此外，也對於公共部門改進和擴大現有的 PPP 倡議提出一些建言。例如，私部門實體要求更流線化的程序以與 FIUs 和執法機構共享資訊；採取一致的方式以與公共部門及時共享情報；並且制定更清晰的法律框架及／或指導方針，以鼓勵在更多國家進行公私資訊共享。此外，一些私部門實體表示，由於缺乏跨部會共享，資訊共享的有效性遭受損害。儘管如此，一些私部門實體認為，FATF 可以在推進討論及分析跨行業 PF 和規避制裁風險方面扮演重要作用。

對於私部門的挑戰

144. 金融機構、DNFBPs 和 VASPs 是預防及打擊複雜的 PF 與規避制裁手法的重要參與者。然而，私部門實體對 PF 的瞭解通常不如對 ML 或 TF 的程度。因此，目前大多數 PPPs 範例主要是著重於公共部門提高對 PF 的認知並提供有關提交 SARs／STRs 的資訊，這可能無法為私部門提供機會學習如何採取具體步驟來識別及偵查複雜的 PF 和規避制裁手法。為偵知並報告這些複雜的手法，私部門可能需要更多關於評估相關活動的指導，像是貿易交易和多方之間大量資訊的交換。相關文件可能以各種形式和媒體儲存，這使得很難將數據與國際和國家制裁名單進行交叉引用。

145. 許多私部門實體報告了多項其他的資訊共享挑戰，包括資料隱私條款實施不均衡、其他監管限制和司法管轄權差異、保密性和信任問題、情報傳播延遲、資料格式不一致以及資源限制（詳見圖 4）。尤其，私部門強調了平衡資料隱私和預防措施義務的困難。此外，一些非銀行金融機構 和 DNFBPs 報告需要行業指導，因為目前的外展工作主要是注重大型銀行的活動。

圖 4. 對於資訊共享的最大挑戰



國際合作

146. 為促進執法的一致性並減少不法分子以預防控制較弱的國家或實體為目標的機會，公私部門可受惠於對 PF 和規避制裁的法律框架採取一致的作為。由 FATF 所訂定的標準，像是實施 TFS，已獲各國採用，其中亦包括將 PF 明定為犯罪並在一些情況下加強出口管制，從而為打擊 PF 創造出一個共享框架。例如，各國採取類似措施來對抗金融機構濫用行為，可減少在國際金融體系中存在較弱環節的可能性。宣導標準化出口管制以及最終使用者驗證有助於防止敏感技術被轉用於禁止用途，同時阻止潛在的資武擴問題。

147. 國際合作對於解決像是虛擬資產之新金融科技相關的新興威脅也極為重要。在此情境下，如前文所述，FATF 虛擬資產聯絡小組一直在深入討論有效實施針對虛擬資產的 AML／CFT／CPF 措施的挑戰和良好實務，尤其是與日俱增的北韓偷竊及濫用虛擬資產的風險。

國際合作的良好實務

148. 一些國家報告稱，有效的國際合作仰賴於政府、金融機構及私部門參與者之間的情報交流。分享關於可疑交易、受制裁實體和高風險活動的資訊有助於辨識及阻斷 PF 網路及規避制裁者。例如，跨國共享 SARs／STRs 有助於揭露與武擴相關的複雜交易鏈。大多數國家的 FIUs 報告稱，它們與其他 FIUs 簽署條約和諒解備忘錄（MOUs）以供交換情報，包括與 PF 活動相關的情報。例如，艾格蒙聯盟金融情報機構（Egmont Group of FIUs）促成 160 餘國之間的安全通訊與協力合作，允許即時共享可操作的資訊。

方框 46. 案例研究：關於受管制兩用貨品出口的國際合作

FINTRAC 收到一件來自 FIU 的自發性傳播，其中詳細說明其管轄範圍內的金融機構所提交的 SARs／STRs，報告 90 筆可疑電匯，總額約為 250 萬美元。該自發性傳播包括牽涉到因俄羅斯國防部門非法採購兩用貨品之故，而遭受另一司法管轄區的國家制裁制度之實體的電匯。SARs／STRs 確定了數個潛在的洗錢指標，並且識別出多筆從 FIU 管轄範圍內的列名實體發至加拿大內的實體，以及非法採購活動高風險國家內的實體。

FINTRAC 評估了該自發性傳播，並且製作一份揭露文件，詳細說明藉由 SARs／STRs 及電子資金轉帳報告向 FINTRAC 提報的金融活動。揭露內容包括一家加拿大實體與相關個人／企業之間的金融交易，這些個人／企業先前因涉嫌向俄羅斯最終使用者非法出口兩用／軍用貨品而遭到調查。此外，SARs／STRs 描述了與俄羅斯和東歐洗錢手法中已知的洗錢態樣一致的交易，以及在加拿大制裁之後對俄羅斯實體的持續交易。

該揭露文件提供涉嫌非法採購網路的概要說明。該揭露文件已發送給多個聯邦揭露文件接收機構以及其他的 FIUs。

來源：加拿大

149. 跨國執法合作讓各國能夠因應 PF 和規避制裁的複雜性與跨國性本質。多國工作小組增強政府當局調查及摧毀網路的資源和專業知識。例如，協調行動可揭露涉及多個國家的前台公司、中間人和複雜路線，這些被武擴網路用以購買及資助 WMD 計畫。

方框 47. 案例研究：西班牙國家警察與歐盟同行合作打擊 PF

西班牙最近遇到數起需要與其他歐盟國家進行國際合作的案件。在每個案例中，中介公司都隱藏材料的目的地。所涉及的實體是公司網路，其中一些公司在不同國家設有子公司，以及其經理。行動中也有「協助者」或中間人。在不同案件中偵查到的主要風險指標是異常的銷售量，以及在進行財務分析後發現的轉移來源與不同的金額。

在一個案例中，國家警察局正在調查透過使用前台公司和中間商將價值約 500 萬歐元的國防物資，特別是軍用飛機零件轉移到俄羅斯。該調查揭露來自前台公司銷售業務的相關付款及款項清洗行為。在歐盟國家框架內，國際合作使得對經由複雜的公路和空中路線且途經不同國家的貨物進行調查成為可能。

在另一起案件中，國家警察局正在調查價值超過 80 萬歐元的化學物質被轉移到俄羅斯的案件，這種行為是歐盟制裁所禁止的。其中一些物質是爆炸物和化學武器的先質。這些化學物質在出口前被儲存在西班牙港口的自由區。在西班牙，國家警察和海關進行了聯合調查。由於運輸是透過公路進行，因此需要與其他國家的機構合作來調查物資跨越歐洲邊境的路線。

來源：西班牙

方框 48. 案例研究：美國和南韓對資助北韓 WMD 的行為者實施制裁 [70]

2024 年 3 月，OFAC 與南韓（ROK）協調，指定位於俄羅斯、中國和阿拉伯聯合大公國的六名個人和兩家實體，這些實體為北韓創造收益並促進金融交易。透過這些行為者產生的資金最終被用於支援北韓的 WMD 計畫，違反聯合國安全理事會第 1718 號決議規定的 TFS 規定。南韓聯合指名這六個相同的個人和實體，因為他們牽涉到透過海外北韓 IT 工作者進行非法資助和創造收入。

這項行動的目標是受指定北韓銀行的代理人並連同在國外僱用北韓 IT 工作者的公司。北韓銀行代表、IT 工作者以及僱用他們的公司創造收益，而且獲得對北韓政府極為重要的外匯。這些行為者主要透過位於俄羅斯和中國的網路進行運作，策劃手法，設立前台公司或空殼公司，並且管理秘密銀行帳戶以轉移和掩蓋非法資金、規避制裁，並且資助北韓的非法 WMD 和彈道飛彈計畫。

來源：美國

150. 一些國家和國際組織，即如聯合國毒品犯罪辦公室（UNODC）和世界銀行，提供培訓、技術協助以及資金挹注來加強資源有限國家的機構和執法能力。這些計畫的重點是改善監管框架、加強監測系統以及提高公私部門對 PF 風險的意識。提供實行有效出口管制和最終使用者查驗方面的專業知識，並且協助各國採用先進的監測系統來偵查及報告與武擴相關的金融活動，對於打擊資武擴而言非常重要。

[70] 美國財政部，「財政部制裁資助北韓大規模毀滅性武器計畫的行為者」（2024 年 3 月 27 日），財政部制裁資助北韓大規模毀滅性武器計畫的行為者 | 美國財政部

方框 49. 管轄權範例：歐洲計畫 EU P2P（合作夥伴對合作夥伴）

EU P2P（合作夥伴對合作夥伴）出口管制計畫是針對加強全球兩用貨品和武器貿易的出口管制。由歐盟委員會和歐洲對外行動署管理，並由法國專家組織協調，該計畫的目標是透過加強國家和區域能力，促進並增強在雙重用途出口管制、武器貿易條約實施以及武器出口管制領域的國際合作，同時兼顧安全與經濟考量的平衡。該計畫包括對 PF 風險意識的提升活動以及為起草國家武擴資助風險提供技術協助。

來源：法國

對於國際合作的挑戰

151. 正如本報告其他部分所討論者，法律框架與制裁計畫的司法管轄差異對有效的國際合作打擊複雜的 PF 和規避制裁手法成為主要挑戰（包括對 PF 定罪的不同方式，這些將在偵查、調查和起訴章節內加以討論）。 PF 網路與該等協助規避制裁的網路跨境運作，利用監管差異、槓桿運用不同的金融體系和國際貿易，對全球安全造成威脅。從而，應對這些風險需要強力的國際合作，加強政府當局預防、偵知及阻斷非法活動的能力。同時，由於許多國家缺乏用以有效地監測和打擊 PF 及規避制裁行為的基礎設施或專業知識，因此需要各國和國際組織之間的合作。

6. 結論及優先領域

152. 雖然許多國家近年來完成了 PF 風險評估，或者將於 2025 年底前完成首次評估，但是 FATF 全球網路在識別和抵減與複雜的 PF 和規避制裁手法相關的威脅和漏洞方面仍處於不同階段。不幸的是，未來數年打擊並防堵 PF 和規避制裁的共同努力可能會變得日益困難。資源豐沛的國家和非國家行為者將繼續鑽研執法、預防措施及法律框架中的漏洞，並且運用新技術與地緣政治格局的持續變化。

153. 保護國際金融體系以避免遭受這種不斷演變的 PF 風險的最佳方式就是加強世界各地訂定 CPF 控制的現有和新興聯繫。過去十年來，各國在更新其 CPF 法律框架和實施 PF-TFS 方面取得顯著進展，不過在有效實行 CPF 制度方面可能需要集體的向前邁進。在對 FATF 建議第 1 項進行修訂的背景下，FATF 全球網路已經制定朝向此一目標邁進的藍圖。如同在 2021 PF 指導中所述，各國必須識別、評估、瞭解和抵減其 PF 風險。此外，私部門實體需要實施程序以識別、評估、監控、管理及抵減 PF 風險，但是它們可以在其現有的 TFS 及／或法令遵循計畫框架內執行。[71] [72] 各國亦應考慮是否需要採取額外措施來解決 PF 風險，包含透過偵查和報告工具、國內協調與協力合作、調查和起訴以及國際合作。[73]

154. 這項研究表明，PF 和規避制裁行為者經常依靠中間人來掩蓋其非法活動，並且隱瞞運往武擴國家或受制裁國家的兩用貨品及其他物品的真正最終使用者。人們採用複雜的手法來遮掩那些規避制裁的個人、公司和國家的身分，故而難以偵知非法活動。為宣導 FATF 全球網路在預防和打擊複雜的 PF 及規避制裁手法方面邁出共同的一步，有一些優先關注領域應考量。

---

71 資助武擴風險評估與抵減指導

72 在 PF 風險方面，金融機構和 DNFBPs 藉由偵查且防止不實施、潛在違反或者逃避目標性金融制裁以尋求加強並補充全面實施建議第 7 項的嚴格要求。在決定抵減某一部門 PF 風險的措施時，各國應考慮與該相關部門有關聯的 PF 風險。透過採取風險基礎的措施，權責機關、金融機構以及 DNFBPs 應能確保這些措施與已識別的風險相稱，同時使他們能夠決定如何依最有效的方式配置其自身擁有的資源。

73 根據建議第 2 項及註釋，各國應建立跨部會框架以更有效地抵減 PF 風險。

關於 CPF之進一步 FATF 工作的建議

a) **對 PF 進行定期更新**：考慮定期更新本報告的現況、趨勢與方法部分。在可預見的未來，PF 和規避制裁風險仍將是 FATF 全球網路需要應對的重大挑戰。然而，我們對這個問題的集體瞭解所依據的威脅、弱點和態樣必定會不斷發展與重塑。鑑於評估 PF 風險的性質，各個國家及私部門必須維持明瞭現況。沒有聯合國安全理事會第 1718 號決議 POE 報告，FATF 應協助主要利害關係人監控風險狀況。

b) **促進公私部門合作**：考慮運用本報告及公眾諮詢的見解，建構對私部門的外展而作為 FATF 活動的一部分，然後利用他們的回饋制定後續指導報告，該報告更著重於能夠與 FIs、DNFBPs 和 VASPs 合作採取的行動以加強 CPF 預防措施。例如，可以為 2026 年私部門諮詢論壇組織一次相關會議或一系列會議。由於 FATF 全球網路報告稱高度依賴於 SARs／STRs 來啟動 PF 和制裁調查，因此可以透過更協調的宣傳及指導來加強相關部門之間的公私資訊共享。

c) **WMD PF 定義**：五年內，考慮在 FATF 通用詞彙表中增加 WMD PF 的官方定義，將 FATF 全球網路 PF 風險評估的橫向審查結果納入考量。如本報告所述，不同司法管轄區在處理 PF 和規避制裁方面的差異可能會破壞或複雜化有關該主題的偵查、調查與國際合作。統一且普遍接受的定義將能抵減預防及打擊 PF 和規避制裁的挫折。

d) **PF NRA 的橫向審查**：三年內，考慮對 FATF 全球網路的 PF 風險評估進行橫向審查。如本報告所述，各國正處於識別、評估、理解和抵減 PF 風險的不同階段，並且利用一系列的新技術來進行。此外，對於與 PF 和規避制裁相關之弱點的理解似乎參差不齊。有鑑於公私部門兩者都面臨著根據 FATF 標準以更佳瞭解 PF 風險的重要任務，因此在 FATF 全球網路有更多時間來評估 PF 風險之後，橫向審查可能有助於確定良好實務。

附件 A：風險指標

1. 以下所提供的指標為非詳盡清單，係根據本項專案期間 FATF 所收到的資訊所整理而成。這些指標係經設計以強化公私部門實體辨識出與相關 PF 和規避制裁手法有關聯之可疑交易及／或活動的能力。雖然所確定的幾項指標似乎與 PF 或規避制裁並無直接或排他性的聯繫，並且可能表明存在其他形式的非法活動，不過當嘗試識別 PF 和規避制裁手法時，它們可能仍然有所關聯。

如何使用這些指標

2. 指標能夠增加出現異常或可疑活動的可能性。與一客戶或交易相關之單一指標的存在，本身可能不足以保證 PF 交易或規避制裁的懷疑，也不一定能清楚表明此類活動，但是能夠促使在適當情況下進行進一步的監控與檢查。同樣，一些指標的出現也應進行更密切檢查。一個或多個指標是否意指存在可疑交易或活動亦依據一機構或市場參與者提供的業務、產品或服務，以及如何與其客戶互動而定。

3. 下列指標與公私部門兩者均相關。對於後者而言，這些指標與金融機構相關，包括銀行和貨幣價值移轉服務、指定之非金融事業或和人員、虛擬資產服務提供商，以及在軍民兩用貨品或者其他相關領域經營或與其接觸的中小型企業和大型企業集團。在私部門，這些指標係為由法令遵循、交易監控、調查分析、客戶審查和關係管理以及其他致力於防範 PF、規避制裁與前置犯罪的人員使用。

4. 一些風險指標需要對通常保存在外部來源的各種資料元素（例如金融交易、海關資料）進行交叉比較。由於對於外部數據的依賴性，私部門可能無法觀察到底下確定的所有指標。對於某些風險指標，私部門將需要來自權責機關的額外情境資訊，即如透過與執法部門或 FIUs 的接觸。在使用這些指標時，私部門實體亦應考量到客戶背景資料的整體性，包括在盡職調查程序中從客戶處獲得的資訊、交易中涉及的貿易融資方法（如適用），以及其他相關的情境風險因素。

5. 下表列出劃分為三大類的風險指標：1）客戶資訊／行為；2）交易；以及 3）貿易活動。客戶資訊／行為指標可用於當進行 CDD 時，而交易指標可用於監控交易，包括出口交易。貿易活動可提供進一步的情境資訊以納入到更廣泛的風險管理程序。雖然每個類別中的一些風險指標之間會有重疊，但是 FATF 全球網路尋求優先提供盡可能多的資訊來支援公私部門。

1. 客戶資訊／行為

1. 使用公司工具（例如空殼公司）來掩蓋所有權、資金來源或所涉及的國家／實體，特別是受制裁的國家。
2. 透過交易分層來模糊最終使用者，採購代理透過多層次公司、經紀人和中介機構來安排貨運、通訊及財務。
3. 當客戶使用複雜的結構來隱藏進出口貨物的連結時，例如運用分層的信用狀、前台公司、中介機構和經紀人。
4. 變更標準業務文件以隱藏最終客戶。
5. 各方的詳細資料與 WMD 制裁或貿易管制所明列的各方類似（例如姓名、地址或電話號碼）
6. 這些帳戶是由所有權結構不透明的公司、空殼公司或一日公司擁有，或是由這些公司進行交易。
7. 客戶牽涉到供應、銷售或運交受限制或高風險商品和／或技術。
8. 客戶先前曾與現受制裁的個人或實體進行過交易或維持關係。
9. 各方實體上位於轉移擔憂的國家（容允透過其領土提供武擴敏感貨品或其資助的國家）
10. 客戶或客戶的交易對手與國內制裁制度所指定的實體和個人進行交易，或者含有與國內制裁制度指定之實體和個人列出的識別碼相關的交易，像是電子郵件地址、實際地址、電話號碼、護照號碼或可兌換虛擬貨幣（CVC）地址。
11. 隸屬於處置兩用貨品或受出口管制產品之大學及研究機構的客戶。
12. 交易涉及所謂的民用最終使用者，但是基礎研究表明該地址為軍事設施或與受關注國家的軍事設施位於同一地點。
13. 客戶購買新船而無明顯的經濟或商業目的。
14. 商業模式完全以出口為導向，充當過境實體。
15. 公司的營運包括航運、進出口、紡織、服裝、漁業和／海鮮業。
16. 客戶堅持對交易保密或是對與制裁和 PF 相關之監管法令遵循，顯現出不夠的關注。
17. 交易涉及其商業登記表明從事「特殊目的」項目的實體。
18. 客戶要求借用同事的個人資訊以確保契約。
19. 客戶交易的貨物與其正常業務無關，可能涉及兩用設備或技術（例如化學反應器、工具機、飛彈系統零件）。
20. 客戶的聯絡資訊，像是電話號碼，與目的地國家不符。
21. 客戶拒絕向銀行、託運人或第三方提供詳細資訊，包括有關於最終使用者、預期最終用途或公司所有權的細節。
22. 儘管處置大量交易，然而作為非法活動的前台公司在網路上缺少線上存在性。
23. 進行電子郵件或網址的網路欺騙，使非法查詢看似來自於合法企業，通常會運用已知的業務關係。
24. IP 位址與客戶報告的位置不符。
25. 公司名稱過於通用、非描述性，或是容易與其他知名公司實體的名稱混淆。此外，公司名稱可能經常以不同的方式拼寫錯誤。

2. 交易

1. 交易涉及從相同最終使用者的外國銀行帳戶，向多個類似的供應商進行小額付款。
2. 交易涉及最後一刻的付款路線變更，該路線先前由一關注國家排定，而現在路線是經由不同的國家或公司。
3. 透過金融體系進行受禁制交易，導致金融機構違反國內制裁制度處理付款。
4. 資金可能會在公司之間循環流動，一家公司停止付款，而另一家公司開始向同一受益人付款。
5. 客戶利用金融服務及／或進行與實際貨品交易有實體距離的交易。
6. 在金融交易文件中，省略對受制裁方或國家的提及。
7. 交易要途經以制裁執行力弱或從事非法貿易手法而聞名的國家或金融中心。
8. 使用複雜或不尋常的支付途徑，包括多家金融機構的連鎖，尤其是透過缺乏 PF 控制或制裁的國家。
9. 使用開放帳戶／開放信用額度而併同於已知轉運國進行付款的交易。
10. 信用狀項下的購買委託給開證銀行，而非實際的最終使用者。
11. 在核可開立帳戶之前，客戶要求先開立與兩用貨品或出口管制產品有關的信用狀。
12. 他們的存款帳戶中的未償還存款金額急劇增加，隨後出現現金提款，表明存在這類交易的可能性。
13. 客戶將與近期現金存款價值相近的資金匯往海外。
14. 客戶使用個人帳戶支付產品費用。
15. 使用多個銀行帳戶。
16. 缺乏明確的貿易交易理由或支付大額款項的理由，特別是假如這不符合客戶的正常業務活動。
17. 貨物的數量和價值與付款的數量不符。
18. 客戶要求以虛擬資產付款，以規避 KYC／AML 措施。
19. 透過虛擬資產服務提供者進行轉帳，尤其是如果涉及監管較低的國家或是沒有進行適當盡職調查而使用去中心化交易所。
20. 使用非官方或替代管道，例如哈瓦拉（hawala），可用於規避制裁限制。
21. 為虛擬資產創建新地址，以創造其不參與受制裁加密貨幣交易所的「外觀」。
22. **交易**涉及支付予在 2022 年 2 月 24 日之後成立，且位於非全球出口管制聯盟（GECC）國家的公司，該款項用於支付國防或兩用貨品。

3. 貿易活動

1. 在貨物抵達貨運站後變更其運送指示代理處時，在出口商不知情的情況下更改貨物的裝運說明。
2. 最後一刻運輸指示的變更與客戶歷史或商業實務相矛盾。
3. 裝運前或裝運期間最終收貨人或地點的貨運文件變更。
4. 客戶要求出貨至其身分文件上未列出的地址。
5. 產品的品質與輸出之目的地國家的技術水準不符。
6. 該（等）交易涉及的貨物運輸不符合正常的地理貿易模式，亦即涉及的國家通常不出口或進口或是通常不消費有關類型的貨物。
7. 牽涉到可用於軍事或核子計畫的設備或材料（例如高強度合金、離心機）的貿易交易。
8. 將貨運代理或包機業者列為最終使用者。
9. 產品以迂迴方式運輸，包含使用小型或過時的船隻。
10. 物品先以小量、密集的裝運方式運到中心位置，然後併裝。
11. 交易涉及在高風險轉運區域內經營的貨運代理公司。
12. 透過轉運點安排購買，通常用於將限制物品轉運至禁運目的地。
13. 與對於產品及目的地非典型運輸路線相關的交易。
14. 當貨運代理／報關公司在貿易文件中被列為產品的最終目的地。
15. 當貨物目的地／裝運國家與發送／接收款項的國家不同而無任何合理理由時。
16. 偽造像是提單、發票等航運文件，以隱瞞航運路線、啟運港口、收貨人或航運代理。
17. 替換受制裁或出口管制的商品名稱，以及使用虛假契約以隱藏最終使用者。
18. 像是商業發票的輔助文件並未列出實際的最終使用者。
19. 在文件中對貨物進行錯誤分類以規避偵查，例如對限制物品使用非敏感描述。
20. 商業、運輸和財務文件中的資訊存在差異。例如，發票和貨運資訊（貨物類型、重量、價值、目的地）之間的差異。
21. 北韓出口商透過貼上標有第三國的原產國標籤來掩蓋北韓生產的商品的原產地。
22. 第三國供應商將製造或分包工作轉移至北韓工廠而未通知客戶或其他相關方。

23. 懸掛北韓國旗的商船經過實體改造以掩蓋其身分並冒充為不同船隻。
24. 奢侈品經常被運往第三國的中央倉庫。
25. 涉及限制性奢侈品的交易迅速轉向新的購買者。
26. 建築材料的採購和交付。
27. 與所述商業目的無關的重大金融活動，例如與紡織品、漁業或煤炭出口無關的付款。
28. 製造或貿易公司的客戶在對於工業產品交易或是其他的貿易交易中使用現金。
29. 貨物申報價格相較於運輸成本是否偏低。
30. 船舶的登記旗幟經常更換。
31. 涉及 FTZ，可用以混淆敏感物品的來源和流動。