

Countering Proliferation Financing: An Appraisal

Col. Vivek Chadha

Col. Vivek Chadha is a Senior Fellow at MP-IDSA, India

Summary

The Financial Action Task Force (FATF) is ideally placed to strengthen the United Nations Security Council Resolution 1540 (2004) against proliferation financing. This article provides a brief overview of this endeavour and highlights certain key initiatives of the FATF in strengthening the regime against proliferation financing.

Introduction

The proliferation of weapons of mass destruction (WMD) as a threat has remained at the forefront of international security concerns. In 2004, the United Nations Security Council adopted Resolution 1540. “The Security Council decided that all States shall refrain from providing any form of support to non-State actors that attempt to develop, acquire, manufacture, possess, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery, in particular for terrorist purposes.”¹ The Resolution focussed on several aspects of WMD proliferation, while finding a brief mention in the provisions of paragraphs 2 and 3(d). Given the complexity of the challenge, a body of experts was required to follow up with the mandate, capacity, and training to support this requirement of the United Nations.

FATF Initiatives

The role of the Financial Action Task Force (FATF) in countering money laundering and terrorist finance was seen as an ideal option to evaluate the threat emanating from proliferation finance. Accordingly, in 2007 the FATF began assessing the threat from proliferation finance and its potential linkages with terrorist financing.² This was undertaken through a typology report that “develops an understanding of the issues surrounding proliferation financing” with suggested measures to counter it. This implied three key aspects of the challenge at hand – identification of the threat; assessment of existing effectiveness of measures being undertaken by member countries; and finally, suggesting measures to combat it.³

The typology report in 2008 noted certain key weaknesses amongst member states. These included:

- Inadequate obligations amongst financial institutions to detect proliferation financing.
- Incomplete listing of controlled goods, including dual-use goods by jurisdictions.
- Legislations did not have provisions to criminalise proliferation financing activities.
- Even as certain jurisdictions had a framework in place, some did not have the resources to implement it, rendering themselves open to vulnerabilities and threats.

The methodology for evaluating the risks and putting in place measures to fight proliferation financing threats follows a pattern that emerges from existing case studies on the subject. The basis of any evaluation emerges from a comprehensive risk assessment of existing threats and vulnerabilities. This is followed by a seamless information and intelligence-sharing mechanism to allow agencies to take advanced measures to mitigate the threat. Past instances suggest that enforcement can only be undertaken when supported by legislative measures that allow actions like seeking verification of goods being transferred. The next step involves verification with the end-user to ensure utility as intended to offset the potential for misuse, including information regarding the change in end-user requirements.

Over time, case studies and typology reports suggested that vulnerability to proliferation financing existed beyond State institutions and formal financial institutions like banks. It was realised that the fight against potential

threats of proliferation financing also needed to focus on non-financial institutions and private entities that could be involved, especially in the case of dual-use technologies.

The FATF has since gradually enlarged the scope of accountability beyond traditional financial institutions. This now includes Designated Non-Financial Businesses and Professions (DNFBPs) and Virtual Asset Service Providers (VASPs). DNFBPs are institutions and professions that may not be typical financial institutions like banks, but nonetheless, are susceptible to exploitation and abuse. This includes professions like property dealing and gem and jewellery trade. Similarly, virtual assets, their holding, exchange and handling have grown rapidly. Despite this, its regulation and legal control remain inadequate. Seventy-five per cent of jurisdictions continue to remain non-compliant or only partially compliant with Recommendation 15 of the FATF, that deals with virtual assets as of April 2023.⁴ Incidentally, India was rated as Largely Complaint with Recommendation 15 during its 2024 Mutual Evaluation which was released to the public on 19 September 2024. However, international under-regulation of the sector can lead to the potential exploitation by terrorists and those involved in the financing of the proliferation of WMD.

The FATF Best Practices Paper identifies important domestic agencies involved in information sharing, to create the requisite synergies to fight against the financing of WMD proliferation. This includes the following:⁵

- Export control and customs/ border control agencies.
- Identifying, analysing, disseminating and sharing intelligence on proliferation activities.

- Reinforcing the role of Financial Intelligence Units to utilise suspicious transaction reports for identifying suspected individuals and organisations for their proliferation activities.
- Empowering law enforcement agencies to prosecute violators for export control violations through provisions in existing laws and regulations.
- Role of supervisors and authorities in identifying and reporting individual linkages with countries involved in proliferation activities.
- Raising awareness among trade promotion agencies regarding dealing with countries identified as a proliferation risk.
- Involving government departments with information exchange on proliferation risks to enable them to enforce existing guidance and UNSC regimes.
- Individuals and entities involved in enforcing international mandates against proliferation finance should receive all information to identify vulnerabilities and take action against concerned suspects.

Conclusion

FATF guidance suggests close linkages between corruption, money laundering and terrorist finance. The channels used by criminal gangs are equally susceptible to exploitation by terrorist organisations and groups involved in proliferation activities. This reinforces the importance of better awareness of proliferation financing threats through information-sharing mechanisms and empowering agencies to intervene to disrupt illicit financing channels.

Endnotes:

- ¹ “UN Security Council Resolution 1540 (2004)”, United Nations at <https://disarmament.unoda.org/wmd/sc1540/> (Accessed on 16 October 2024).
- ² “Financing of Proliferation”, Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism”, Council of Europe at <https://www.coe.int/en/web/moneyval/implementation/financing-proliferation> (Accessed on 16 October 2024).
- ³ “Proliferation Financing Report”, Financial Action Task Force, 18 June 2008, p. 1 at <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf> (Accessed on 16 Oct 2024).
- ⁴ “Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAS and VASPs”, FATF at <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html> (Accessed on 16 October 2024).
- ⁵ “Best Practices Paper – Sharing Among Domestic Competent Authorities Related to The Financing of Proliferation”, FATF, February 2012 at <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/BPP%20on%20Recommendation%202%20Sharing%20among%20domestic%20competent%20authorities%20re%20financing%20of%20proliferation.pdf.coredownload.inline.pdf> (Accessed on 18 October 2024).