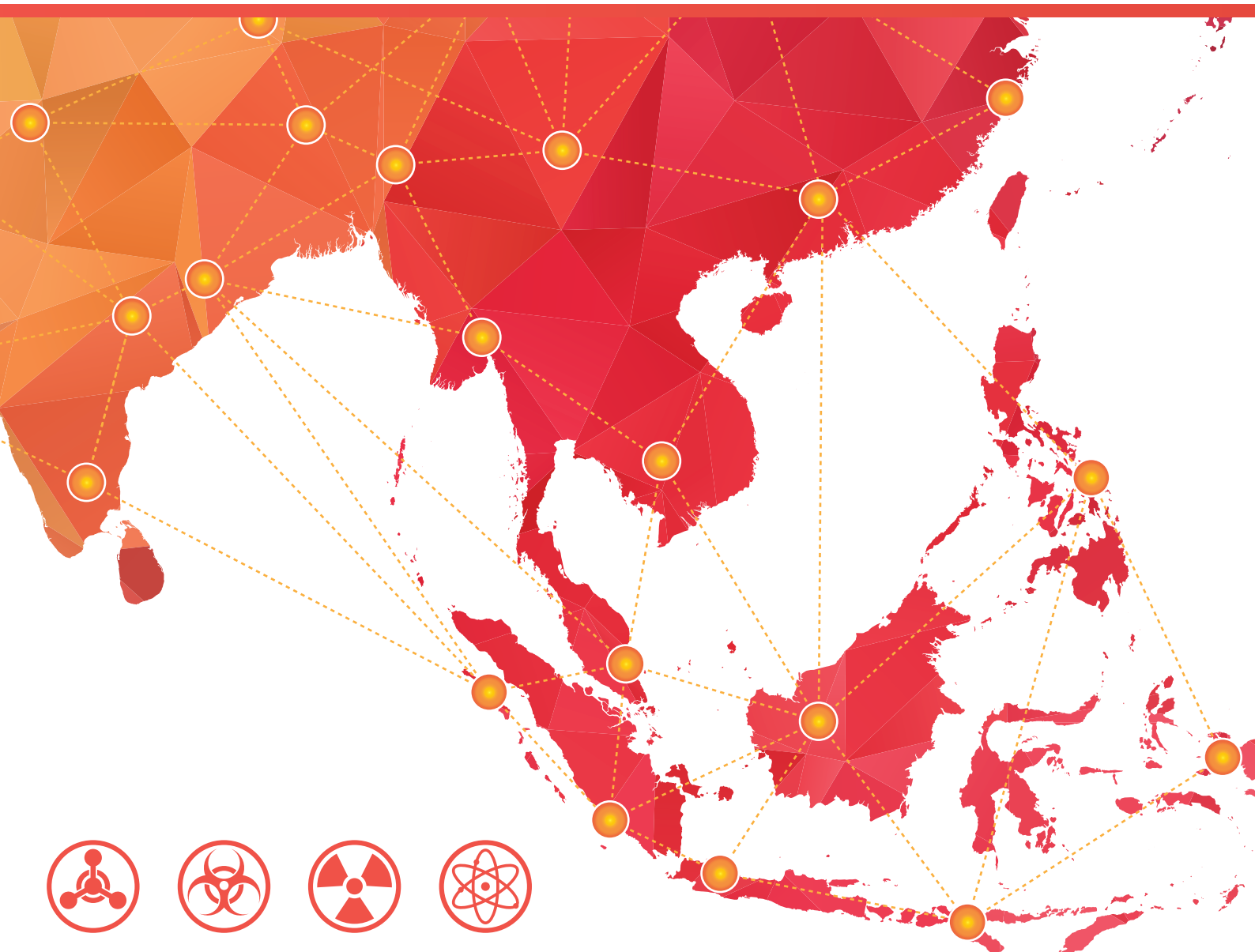


# **CBRN**

# **PROLIFERATION FINANCING:**

# **A PERSPECTIVE FROM**

# **SOUTHEAST ASIA**





**CBRN**

**PROLIFERATION FINANCING:**

**A PERSPECTIVE FROM**

**SOUTHEAST ASIA**

October 2023

# DISCLAIMER

The opinions, findings, conclusions, and recommendations expressed herein are those of the authors and do not necessarily reflect the views and positions of the United Nations and UNICRI, or any other national, regional or international entity involved. Contents of the publication may be quoted or reproduced, provided that the source of information is acknowledged. The designations employed and presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area of its authorities, or concerning the delimitation of its frontiers and boundaries.

This publication was produced with the financial support of the Foreign Commonwealth and Development Office (FCDO) of the United Kingdom of Great Britain and Northern Ireland. Its contents do not necessarily reflect the views of the FCDO.

# ACKNOWLEDGEMENTS

This report was prepared by Giuseppe Di Luccia, Consultant at UNICRI and Research Associate at King's College London, under the guidance of Carlotta Zenere, Francesco Marelli and Francesco Miorin from the CBRN Team at UNICRI. Special appreciation to Katy Carroll and UNICRI's Public Information Unit for their support in the editing and graphic design, respectively.

UNICRI would like to express its gratitude to the experts from the national authorities, and international organizations that provided their insights in the data collection process, and their feedback during the review phase.

© United Nations Interregional Crime and Justice Research Institute (UNICRI)  
Viale Maestri del Lavoro, 10  
10127 Torino, Italy  
+39 011 6537 111  
[www.unicri.org](http://www.unicri.org)





# LIST OF ACRONYMS

**AML** – Anti-Money Laundering

**AMLC** – Anti-Money Laundering Council

**AMLIO** – Anti-Money Laundering Intelligence Office

**APG** – Asia Pacific Group on Money Laundering

**CBRN** – Chemical, Biological, Radiological and Nuclear

**CFT** – Combating Financing of Terrorism

**CPF** – Counter-Proliferation Financing

**DNFBP** – Designated Non-Financial Businesses and Professions

**DPRK** – Democratic People’s Republic of Korea

**FATF** – Financial Action Task Force

**FCDO** – Foreign Commonwealth and Development Office

**IAEA** – International Atomic Energy Agency

**ITDB** – Incident and Trafficking Database

**JCPOA** – Joint Comprehensive Plan of Action

**KOMID** – Korea Mining Development Trading Corporation

**ML/TF** – Money Laundering and Terrorism Financing

**OPCW** – Organisation for the Prohibition of Chemical Weapons

**PDR** – People’s Democratic Republic

**PF** – Proliferation Financing

**PF-NRA** – Proliferation Financing National Risk Assessment

**RUSI** – Royal United Services Institute

**STMO** – Strategic Trade Management Office

**TFS** – Targeted Financial Sanctions

**UAV** – Unmanned Aerial Vehicles

**UNICRI** – United Nations Interregional Crime and Justice Research Institute

**UNSC** – United Nations Security Council

**WMD** – Weapon of Mass Destruction



# FOREWORD



As we navigate the interconnected and increasingly intricate landscape of the 21st century, the complexities posed by vulnerabilities in global financial systems have become more glaring. This applies particularly to security and non-proliferation of weapons of mass destruction.

This report by the United Nations Interregional Crime and Justice Research Institute (UNICRI) is the culmination of rigorous research, extensive interviews, and data analysis by a dedicated team of experts. It aligns with UNICRI's mandate as the UN research and training institute for criminal justice and crime prevention.

Proliferation financing is a critical yet often overlooked aspect of the wider proliferation process. This report gives the issue much needed prominence in the global security discourse. The report analyses the challenges and threats of proliferation financing in the vibrant and diverse Southeast Asia region. Its dual objectives are to enhance the understanding of Southeast Asia's proliferation financing landscape, detailing its risks, challenges, and associated trends; and to spark dialogue among policymakers, financial institutions, regulatory bodies, and other stakeholders on strategies to counter this emerging area of concern. Both are necessary to strengthen regional and global frameworks to prevent the misuse of financial systems for proliferation activities.

Southeast Asia, with its extensive maritime borders, rapid economic growth, expanding financial markets, and intricate network of cross-border transactions, presents opportunities to improve law enforcement, as well as vulnerabilities to exploit by malicious actors. From a security perspective, the presence of terrorists and related entities with the capacity to carry out attacks is a major concern. The region's vulnerability is magnified as several countries already serve as preferred routes for diverse forms of illicit trafficking.

The risks of proliferation financing are multidimensional, encompassing economic and security concerns alongside social and political dimensions. These are global threats with implications that extend beyond national borders. The challenge for security actors is to understand these issues better and to build appropriate, robust, coordinated responses to mitigate them effectively.

I hope this report will contribute to a broader, shared understanding of the risks and challenges posed by proliferation financing and inspire stakeholders to join forces in combating this grave threat to our collective security. The task is arduous, but with knowledge sharing and international cooperation, I am confident we can make meaningful progress in the fight against proliferation financing. I invite you to engage with our report and join UNICRI's quest to build a safer world for all.

**Antonia Marie De Meo**  
Director, UNICRI

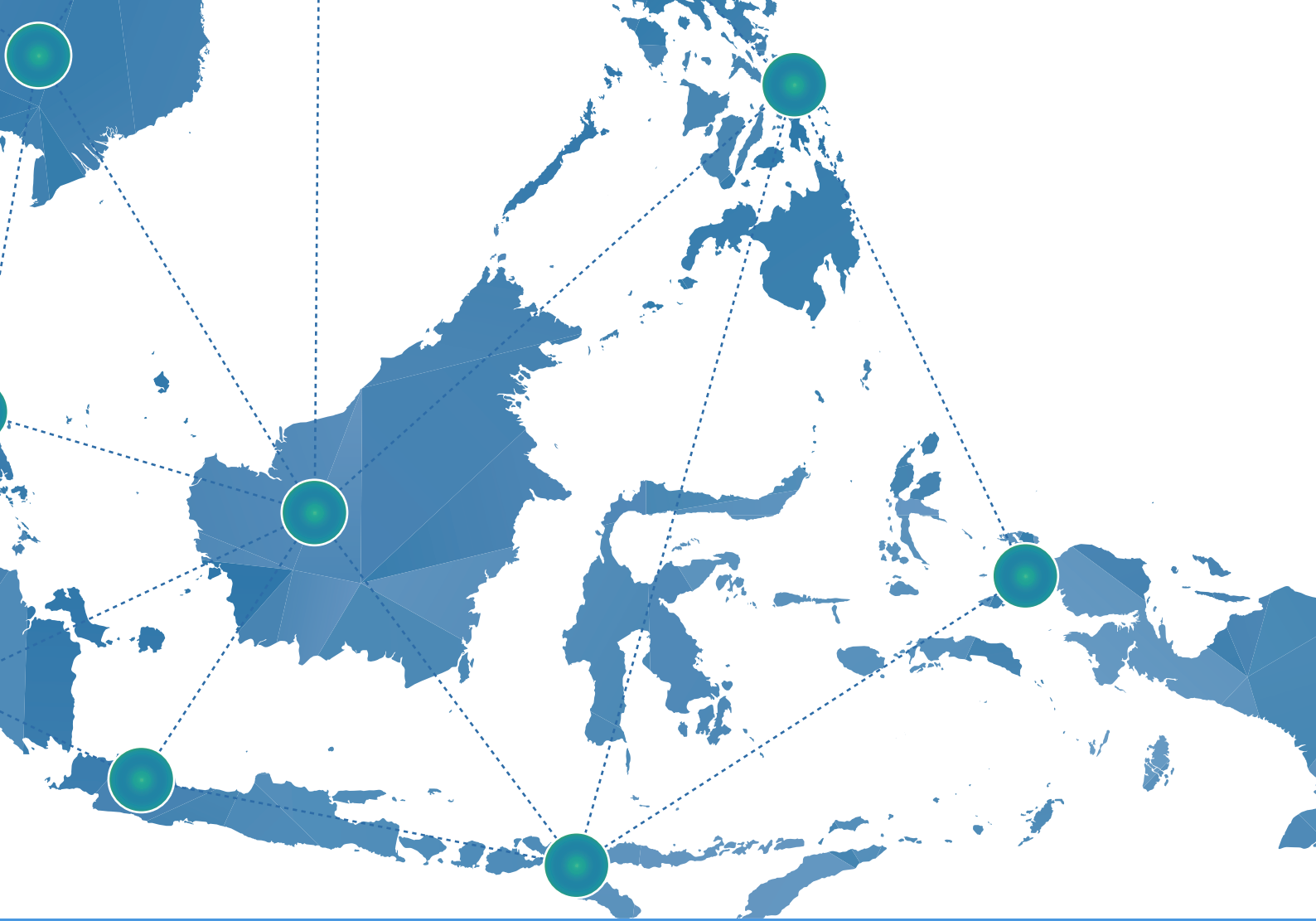


# TABLE OF CONTENTS



Disclaimer	2
Acknowledgements	2
List of Acronyms	3
Foreword	4
Background to the Proliferation Financing Threat	8
UNICRI's Response	10
Objectives and Approach of UNICRI's Project	10
Format and Content of the In-Country Visits	11
Proliferation Financing Threats in Southeast Asia	12
1. Proliferation Financing Threats from Procurement Schemes	14
2. Proliferation Financing Threats from Weapons of Mass Destruction Proliferation Networks	18
2.1 The Threat Posed by Non-State Actors	20
2.2 How Proliferation Financing Networks Threaten Southeast Asia?	22





3. Proliferation Financing Threats from Revenue-Raising Activities and Sanctions Evasion	23
3.1 Trade Sanctions evasion	24
3.2 Proliferation Financing in the maritime sector	26
3.3 Democratic People’s Republic of Korea Officials	27
3.4 Democratic People’s Republic of Korea Workers	28
3.5 Virtual assets	29
Challenges to Implementing Counter Proliferation Financing Regimes in Southeast Asia	31
What Can Be Done to Increase Awareness of Proliferation Financing-Related Risks?	32
Identified Priority Actions and Recommended Steps	39
The Way Forward	40
Annex	41

# BACKGROUND TO THE PROLIFERATION FINANCING THREAT

The proliferation of chemical, biological, radiological and nuclear (CBRN) weapons and their means of delivery represents one of the most pressing threats to international peace and security. Over recent years, the international community's concern for risk associated with financial products and services linked to the trade in proliferation-sensitive items has dramatically increased. This is mainly due to increasingly sophisticated evasion techniques, and the wide range of actors involved in proliferation activities, from state actors to complex networks of criminal enterprises, front companies, and professional intermediaries conducting operations on their behalf.

The proliferation financing (PF) threat is multifaceted and complex due to the different forms of potential financial support that can be provided to programmes that proliferate weapons of mass destruction (WMD) and their means of

delivery. The proliferation financing threat encompasses (i) trade finance services for the procurement of strategic goods, materials and technology destined for WMD proliferation programmes, (ii) funding through licit and illicit revenue-raising activities as well as (iii) any form of financial service or related technical assistance facilitating the provision of financial support in aid of WMD proliferation.

By denying the provision of funds and financial or other instrumental services (e.g., insurance services, legal and corporate advisory services) to proliferators or to their networks engaging in WMD proliferation-related activities, the international community aims to restrict the ability of malign actors to pursue their WMD malicious programmes. One of the greatest challenges to counter-proliferation financing (CPF) efforts is the limited capacity (or inability) of PF networks to adapt to the response mea-

asures adopted by the international community, especially in the case of state-sponsored WMD programmes. Consequently, as CPF efforts expand to cope with new and increasingly sophisticated tactics aimed at funding WMD proliferation, the scope of proliferation financing enlarges.

## RESOLUTION 1540 FROM 2004 UNTIL TODAY

The United Nations Security Council (UNSC) adopted resolution 1540 (2004) following attacks on 11 September 2001, commonly known as 9/11, in New York City and Washington DC and the discovery of Abdul Qadeer Khan's network supporting nuclear weapon and ballistic missile proliferation attempts across several jurisdictions. The UNSC's decision introduced a global approach to counter-proliferation financing, as opposed to the country-based approach where specific sanction regimes target WMD sta-



te-sponsored programmes.<sup>1</sup> Such a global approach calls upon all UN Member States to prohibit non-state actors from carrying out WMD proliferation-related activities as well as their financing.

Although state-sponsored programmes currently pose the greatest PF risks, WMD proliferation from non-state actors remains of concern. Against the backdrop of an increasingly unstable international security environment, on 30 November 2022, the UNSC unanimously extended the 1540 Committee's mandate for 10 years. The adoption of UNSC resolution 2663 (2022) demonstrated the international community's commitment to fight WMD proliferation by non-state actors.

## UNDERSTANDING THE EXPOSURE TO THE RISK OF PROLIFERATION FINANCING

The global reach of PF threats has been widely documented in numerous case studies involving jurisdictions located in different continents.<sup>2</sup> Yet, the level of proliferation financing risk is not homogenous across the globe; it varies according to several risk factors. Systemic opportunities and geographical proximity to the Democratic People's Republic of Korea (DPRK) have drawn particular attention to the Southeast Asia region. Since its establishment in 2009, the UN Panel of Experts of the 1718 Sanctions Committee<sup>3</sup> has reported on the tactics used by the DPRK in the region to pursue its WMD and

ballistic missile programmes, constantly adapting to more and more restrictive sanctions. In addition to the identification of global and regional threats, factoring in the national level analysis is equally key to understand the exposure to PF risks. A holistic analysis of elements such as the relevant national legal framework, the national economy or the financial sector, is critical to adopt effective mitigation measures. Therefore, national initiatives need a coordinated effort involving relevant competent authorities that encompass a wide range of players, including policy makers, prosecutors, law enforcement agencies, financial and security intelligence, customs and supervisory authorities over financial institutions and designated non-financial businesses and professions (DNFBPs).

1 Financial Action Task Force, "FATF Guidance on Counter Proliferation Financing", FATF, February 2018, pp. 3, 4.

2 See for example Jonathan Brewer, "Study of Typologies of Financing of WMD Proliferation, Final Report," Project Alpha, King's College London, 13 October 2017.

3 The Security Council Committee pursuant to resolution 1718 (2006) oversees the sanctions measures imposed by the Security Council on the DPRK.

# UNICRI'S RESPONSE

---



UNICRI produced this report with the aim to identify and highlight the main issues discussed at expert level meetings, including the perception of PF threats, case studies, challenges in addressing such illicit activities and mitigation measures. The report aims to lay the foundation for subsequent capacity-building initiatives.



From October 2022 to January 2023, UNICRI conducted workshops and consultations with relevant national authorities in three Southeast Asian jurisdictions, namely Cambodia, Lao People's Democratic Republic (PDR) and the Philippines, to raise awareness on CBRN proliferation financing risks and promote the development of solid counter PF regimes.



The consultations took place within the framework of the project "Strengthening capacities to identify and mitigate CBRN proliferation financing risks in Southeast Asia", funded by the Foreign, Commonwealth and Development Office of the United Kingdom. This report highlights the major PF threats posed to the Southeast Asian region, the challenges the three above-mentioned countries are facing in addressing CBRN proliferation activities and the priority actions that need to be taken in order to address them.

## OBJECTIVES AND APPROACH OF UNICRI'S PROJECT

This report is the result of a project by UNICRI that sought to improve understanding of chemical, biological, radiological and nuclear weapon proliferation financing risks, enhance awareness of and compliance with relevant international norms, and identify priority actions at the national and regional levels to increase countries' capacities to effectively tackle PF risks. This report consolidates findings from UNICRI's research and consultations. It is hoped that it will pave the way for follow-up initiatives

to address proliferation financing in the Southeast Asian region and globally. The report is structured in two main parts. The first presents an overview of the threats in Southeast Asia associated with the risk of exposure to proliferation financing, particularly regarding WMD procurement schemes, WMD proliferation networks, and revenue raising activities that evade non-proliferation sanctions programmes. The second part illustrates the proposed measures to mitigate the PF risk.



## IN-COUNTRY VISITS

UNICRI engaged with stakeholders and key authorities from Cambodia, Lao PDR and the Philippines (including relevant government ministries, financial intelligence units, central banks, law enforcement and state security agencies) to raise their awareness of proliferation financing and to enhance their understanding of priority measures to address such risks. Within this framework, UNICRI held national workshops and consultations in the three partner countries.

During the first part of the workshops, the experts from UNICRI presented on key PF concepts, including how to define proliferation financing. Having acknowledged the lack of an official definition, experts drew upon the working definition<sup>4</sup> developed by the Financial Action Task Force (FATF) in 2010:

*The act of providing funds or financial services which are used, in whole or in part, for 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 technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.*

The experts further elaborated on this definition to reflect the widening scope of proliferation financing since 2010. Without delving into a technical analysis of the definition of PF, the experts highlighted that (i) PF is not only the act of providing funds and financial services, but also the services necessary to execute PF schemes (legal assistance, accounting, etc.); (ii) the FATF's working definition of PF also includes the provision of other economic resources that may be used to obtain funds; and (iii) in addition to chemical, biological and nuclear weapons, UNICRI's initiative extended

the scope to radiological weapons due to the risks of radiological attacks (e.g. the dispersal of radioactive material or the use of radiation exposure devices). The experts delivered presentations on key concepts, followed by an overview of PF threats, typologies, international sanctions, international financial standards, trends and case studies. Subsequently, consultations were held with the national authorities, based on a specific reference document, to further improve the understanding of CPF-related issues, collect information on current challenges and to identify actions aimed at mitigating PF risks.

## REGIONAL EXPERTS' MEETING

After the in-country visits, UNICRI organized a regional experts' meeting at its headquarters in Turin, Italy, from 14 to 16 March 2023, to identify priority actions to address the current threats and to share good practices and lessons learned. The workshop was attended by key authorities involved in counter-PF efforts in the participating jurisdictions and beyond (including experts from the Financial Intelligence Unit in Malaysia, the Monetary Authority of Singapore and a PF expert from His Majesty's Treasury of the United Kingdom) as well as representatives of relevant international organizations and think tanks (including the PF specialist of the Group of Experts supporting the 1540 Committee, and PF experts from King's College London and the Royal United Services Institute (RUSI)).

The three-day workshop provided an overview of the main PF threats, including emerging trends, and a regional focus on the challenges and perception of PF risks. Moreover, the workshop discussed challenges faced by Member States' in Southeast Asia in addressing PF threats and capacity-building priorities in countering such financial crime.

<sup>4</sup> Financial Action Task Force, "Combating Proliferation Financing – A Status Report on Policy Development and Consultation", February 2010, p. 5.



# PROLIFERATION FINANCING THREATS IN SOUTHEAST ASIA

Southeast Asia is uniquely exposed to the DPRK's WMD proliferation ambitions. Geographically located in proximity to the DPRK, and characterized by extensive maritime borders, Southeast Asian countries are easily accessible to the North Korean proliferation networks. Moreover, the expanding trade and financial hubs in growing Southeast Asian economies, coupled with the interest in developing nuclear energy programmes and chemical and biotech industries, attract WMD proliferators, who seek to misuse the services and technical assistance provided to business operators to pursue criminal purposes. PF actors exploit the lack of advanced counter-proliferation financing regimes in some jurisdictions to operate undetected in the region. WMD procurement activities are often disguised as normal business operations, whose apparently legitimate nature complicates investigations.

In addition to the threat posed by the DPRK, Southeast Asian jurisdictions should also consider PF threats stemming from other countries deemed of proliferation concern, *in primis* Iran. As mentioned above,

the PF threat may be more or less significant based on certain factors, including trade data, business presence or diaspora. A specific assessment of a country's exposure to proliferation activities is necessary to gain awareness of the level of the PF risk coming from other countries variously involved in WMD proliferation. Some jurisdictions could deem necessary to assess the PF risks determined, for instance, by Syria's<sup>5</sup> implication in chemical weapons use on its territory.

The presence of violent non-state actors, including terrorist groups, in some parts of Southeast Asia elevates the risk of violent non-state actors also acquiring CBRN materials to cause instability and spread fear, which should not be underestimated. The potential of such actors to acquire and use chemical or radiological substances is a scenario that raises concern in the region. For example national authorities from Lao PDR who participated in UNICRI's awareness-raising event expressed concern about the risk of mining chemicals being diverted for criminal use.

---

5 Although not specifically subject to UNSC WMD-related resolutions (as in the case of the DPRK and Iran), some jurisdictions consider Syria a country of proliferation concern based on the reported cases of toxic chemical use in the Syrian Arab Republic between 2014 and 2015 (see [Executive Council Decision – OPCW-United Nations Joint Investigative Mechanism Reports on Chemical Weapons Use in The Syrian Arab Republic \(EC-83/DEC.5\) 11 November 2016](#)) and, more recently, the 7 April 2018 chemical attack in Douma (see the Organisation for the Prohibition of Chemical Weapons (OPCW) Investigation and Identification Team's third report, <https://www.opcw.org/media-centre/news/2023/01/opcw-releases-third-report-investigation-and-identification-team>)



# 1. PROLIFERATION FINANCING THREATS FROM PROCUREMENT SCHEMES

Several cases investigated and reported by the UN Panel of Experts represent procurement strategies by the DPRK involving the Southeast Asia region. The Glocom case – a front company for the DPRK entity Pan Systems Pyongyang (and its Singaporean partner Pan Systems Pte Ltd) linked to the DPRK intelligence agency Reconnaissance General Bureau – is illustrative of the dimension and complexity of the financial schemes adopted to distribute and procure dual-use items. Glocom operated in the sale of military communication equipment and systems using a global network extending to jurisdictions in Southeast Asia, namely Indonesia, Malaysia and Singapore, as well as to China and the Middle East. The components of the goods produced in factories in DPRK were procured from suppliers based in China and Hong Kong through two Malaysian front companies, International Golden Services Sdn Bhd and International Global Systems Sdn Bhd, and a support network of agents and other facilitators active in at least 10 jurisdictions.<sup>6</sup>

The conglomerate avoided detection of the financial transactions with the DPRK by employing alternative payment systems, including bulk cash transfers, use of the diplomatic privileges granted to the DPRK missions and ledger systems.<sup>7</sup> As reported by the UN Panel of Experts, the ledger system used in the Glocom case was operated by the Chinese financial institution Daedong Credit Bank.<sup>8</sup> On the procurement side, the front companies based in Malaysia and acting on behalf of Glocom opened several bank accounts whereby they initiated payments to multiple front companies based in Hong Kong that were destined for the network's suppliers.<sup>9</sup> By utilizing the network of bank accounts opened by Glocom and the *ad hoc* front companies that were financed with the earnings from Glocom's sales, the ledger system allowed for the money flow to circulate outside of the DPRK, detached from the actual beneficiaries.

---

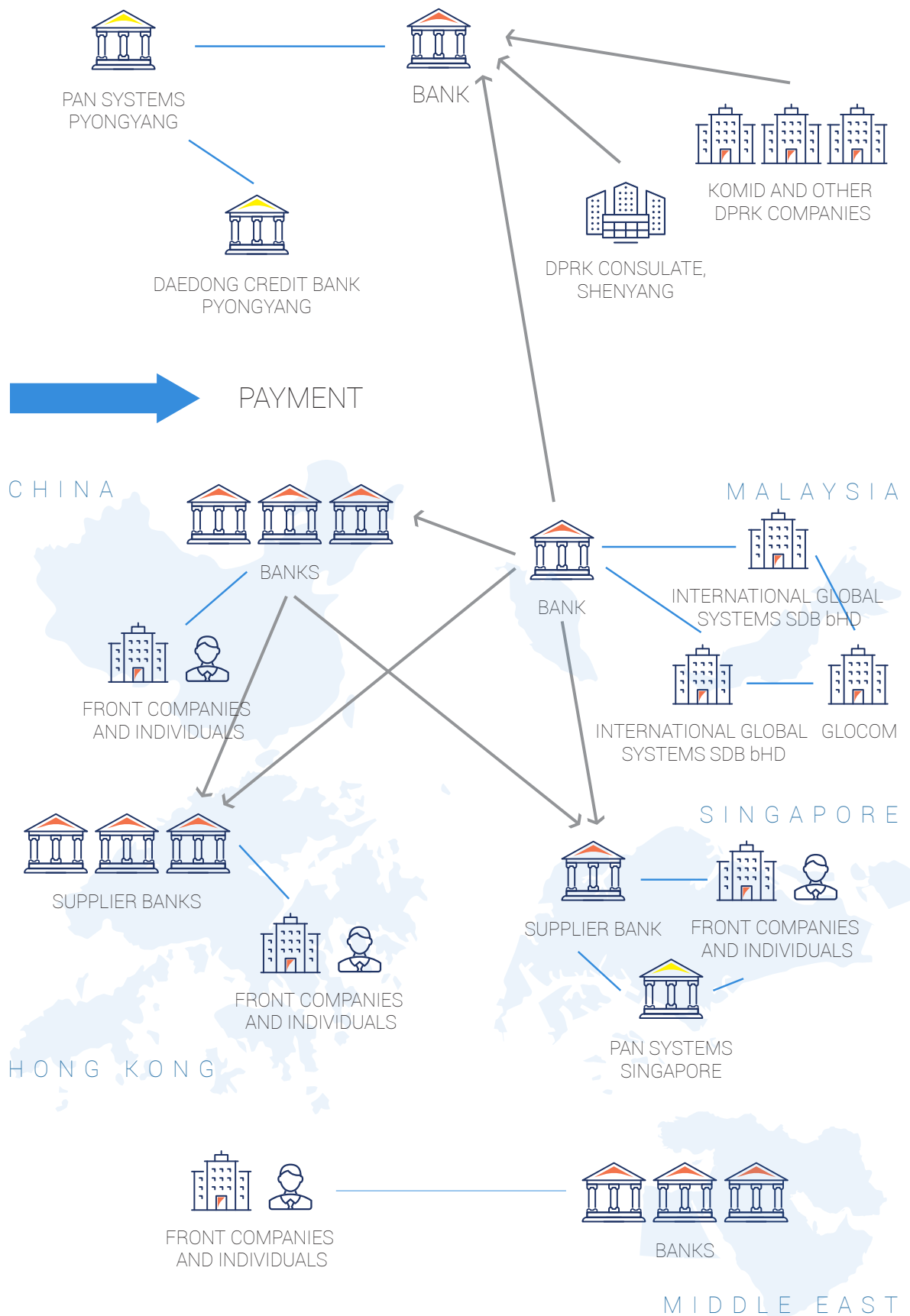
6 UN Security Council, "Final Report of the Panel of Experts Submitted Pursuant to Resolution 2276 (2016)", S/2017/150, 27 February 2017, pp. 34-37.

7 Ledger payments refer to transactions recorded in a ledger to keep track of the payments made and received. This system allowed DPRK entities to manage the financial inflows and outflows generated by illicit sale and procurement activities through a correspondent bank account held by front companies of DPRK entities, therefore keeping the money flowing outside North Korea.

8 Daedong Credit Bank was sanctioned by the UN Security Council on 2 March 2016 for providing financial services to DPRK sanctioned entities established in other jurisdictions, in some cases using deceptive financial practices.

9 UN Security Council, "Final Report of the Panel of Experts Submitted Pursuant to Resolution 2345 (2017)", S/2017/742, 5 September 2017, p. 23.





### EXAMPLE OF A PROLIFERATION FINANCING PROCUREMENT SCHEME

Source: Jonathan Brewer, "Study of Typologies of Financing of WMD Proliferation, Final Report," Project Alpha, King's College London, 13 October 2017, Case 7, p. 57.



The peculiar feature of proliferation financing and its core threat is that WMD proliferators mainly, but not exclusively, rely upon the international financial system to procure the specific goods, materials and technology that allow for the design, development or production of weapons of mass destruction and their means of delivery. Therefore, both export control mechanisms, aimed at countering WMD proliferation by closely monitoring the movement of proliferation-sensitive items and financial establishments, which not only facilitate payment processing for commercial transactions but also ensure the seamless transfer of goods through trade finance and insurance services, are interconnected in their efforts to counter proliferation.

Proliferation schemes are designed based on in-depth knowledge of the jurisdictions' structural and sectoral vulnerabilities. WMD proliferators are able to evaluate the chances of procuring goods by exploiting, for instance, looser police, customs or export controls

applied in transshipment hubs and free trade zones to conceal the final destination and detach end-user proliferators from the commercial transactions. These malicious actors also target jurisdictions with permissive corporate service environments characterized by weak financial controls or less developed compliance culture so that they may establish front and shell companies to obfuscate their identities and hinder investigations.

Procurement schemes are usually characterized by a dual route comprising the commercial transaction to deliver the strategic item and the financial transaction for the payment. They both pass through several jurisdictions, as WMD proliferators try to add layers of complexity to water down the controls. With regard to the delivery of the item, for instance, the manufacturer may be based in a jurisdiction different from the one of the suppliers, who, in turn, will ship it through one or more transit or transshipment countries to the purchaser, usually a shell or a front company acting on



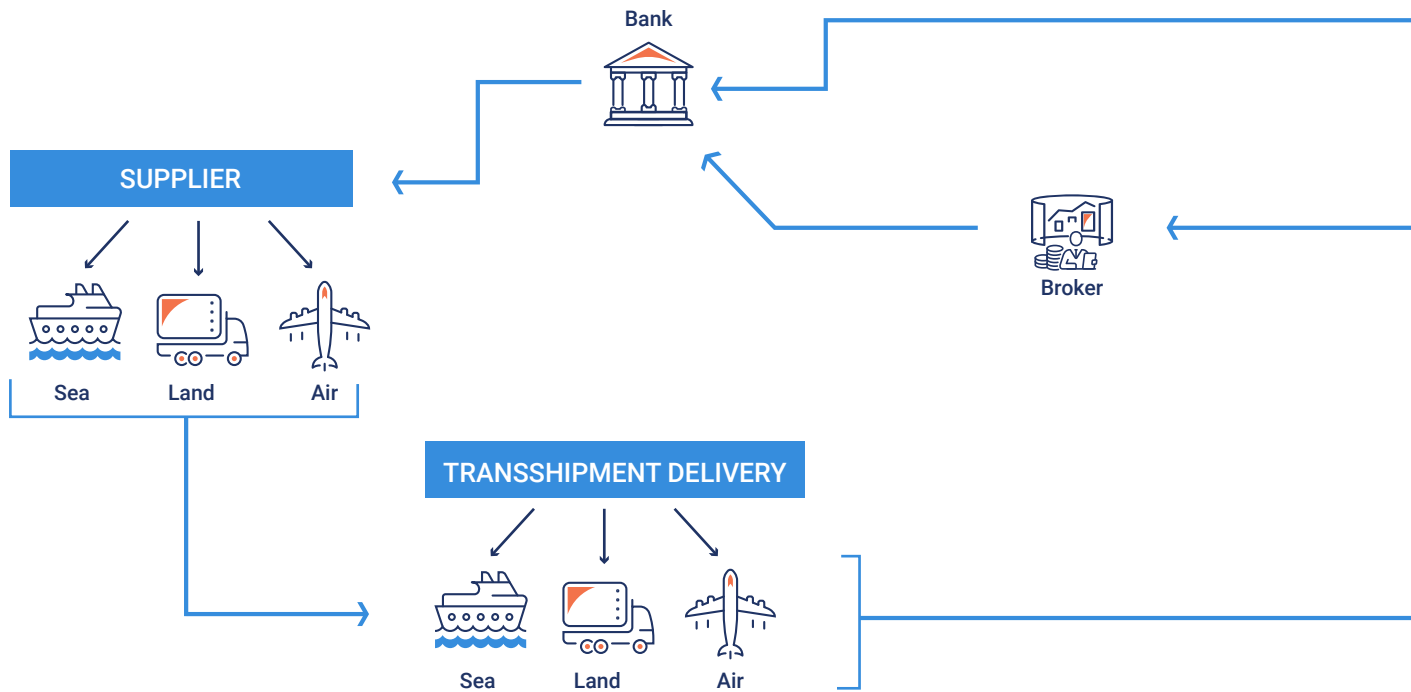
behalf of the WMD proliferators. The financial flow follows a different route through accounts held by shell companies established in offshore jurisdictions, where corporate structures are not disclosed.

A recent example of PF risk linked to a procurement scheme, which confirms the intertwined roles of export controls and CPF, concerns the transfer of radio control systems. In 2021, the Philippine export control authority, notably the Strategic Trade Management Office, denied the licence for the export of 1,760 Servos worth approximately US\$ 316,800 to another country believed to be a transshipment point to an ultimate end-user located in a country sanctioned by the UN Security Council. The denial followed the detection of red flags and further investigations on the end-user and the end-use. A first red flag that led to the application of the catch-all clause (a procedure requiring controls for WMD proliferation concern over items not included in the national control list) was the dual-use

nature of the goods: while the Servos are below the technical parameters defined in the dual-use goods list, they can be reengineered to be used in UAVs. A second red flag was the unusual large quantity of the items ordered. From the financial side, the payment raised concerns as it came from the broker, possibly with the aim of dissociating the end-user's identity from the transaction.

Moreover, the exporter had previously transferred similar items to Yemen and Syria (and possibly to Iran) for application in UAVs, while the directors and the secretary of the end-user performed the same roles in companies under investigation and enforcement measures by the US. Finally, the end-user claimed to be affiliated with an academic institution in Country Y. However, when the Philippine authorities reached out for confirmation, the university in Country Y denied any affiliation with the company.

## 2. PROLIFERATION FINANCING THREATS FROM WEAPONS OF MASS DESTRUCTION PROLIFERATION NETWORKS



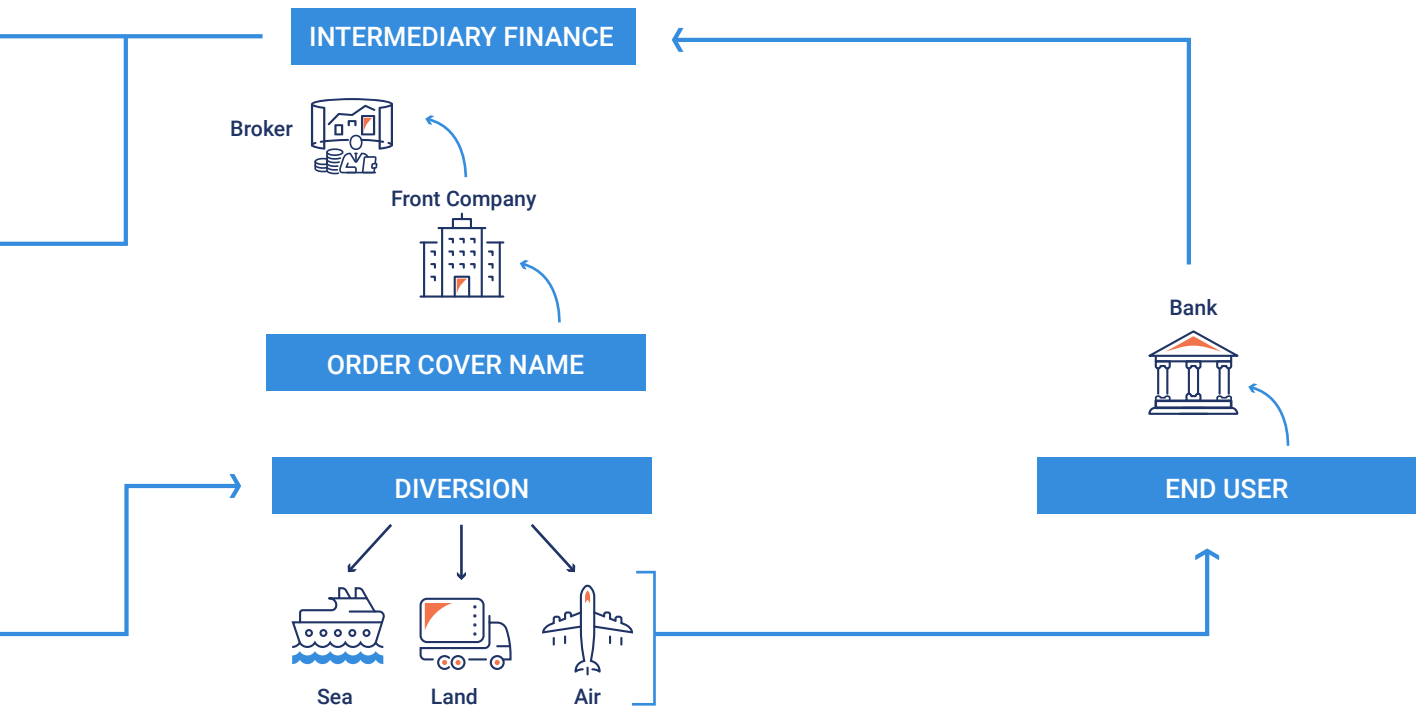
### EXAMPLE OF A PROLIFERATION FINANCING NETWORK

The United Nations Security Council has adopted resolutions<sup>10</sup> imposing targeted financial sanctions (TFS) on entities and individuals engaged in or providing support for programmes related to weapons of mass destruction and ballistic missiles. At the national level, TFS against WMD proliferators, including PF actors, translate to further obligations to financial and business operators. Member States shall implement such obligations for establishing asset freezing mechanisms and prohibiting the provision of any funds, financial assets or economic resources to or for the benefit of the designated entities and individuals. With the implementation of targeted financial sanctions, the UNSC has tried to financially isolate actors involved in WMD

proliferation-related activities by denying them access to the international financial system. What is more, by assuming that the funds, financial assets, economic resources or related services provided to designated individuals or entities would be used to carry out WMD proliferation-related activities, targeted financial sanctions have expanded the scope of proliferation financing.

While proliferation financing may be the financial crime traditionally identified with certain “activities” covered by operative paragraph 2 of UNSCR 1540 (2004), PF TFS shift the focus to the “actors”. Procurement schemes for WMD programmes originate from WMD proliferators and their support structures. UNSC resolutions im-

10 See for example, UNSCRs 1718 (2006), 1737 (2006), 1747 (2007), 1929 (2010), 2087 (2013), 2270 (2016).



sing targeted financial sanctions have identified individuals and entities actively operating in the DPRK and Iran’s WMD and ballistic missiles programmes. Therefore, TFS put the main “nodes” of the proliferation networks on the map, whose immediate extensions are represented by people they control or who act on their behalf, as well as entities they either directly or indirectly own or control.

WMD proliferators and their immediate extensions, for instance in the form of shell companies or agents acting on their behalf, seek to develop a support structure to gain access to international trade and the international financial system. The development and the operation of such structures represent a PF threat

to different economic operators that become involved in WMD proliferation schemes (see figure above). By engaging in transactions, directly or indirectly, with WMD proliferators, the network of financial institutions, brokers, freight forwarders, legal consultants, accountants, and so on, provides proliferators with the resources and services necessary to pursue their programmes.

As we move from the “nodes” to the “tails” of the network, the support structure progressively features more private entities operating for their own profit and with less or no connection with the state. These support structure components often fall within the definition of non-state actors.

## 2.1 THE THREAT POSED BY NON-STATE ACTORS

UNSC resolution 1540 (2004) defines a non-state actor as any “individual or entity, not acting under the lawful authority of any State in conducting activities which come within the scope of this resolution.”<sup>11</sup> The grave concerns expressed in the resolution relate to two different threats from non-state actors: on the one hand, the threat of illicit trafficking, which refers also to economic operators wittingly or unwittingly participating in WMD procurement schemes, as shown in the previous figure; on the other hand, the threat of terrorists and terrorist groups pertains to violent non-state actors engaging in WMD proliferation-related activities. With the objective of making profits, criminal organizations engage in illicit activities by assisting or acting on behalf of WMD proliferators, or by independently attempting to steal sensitive material (e.g. radiological substances) to resell directly to WMD proliferators or to black markets.

It is worth noting that criminal organizations facilitating illicit deliveries of hundreds of thousands of barrels of oil to the DPRK fall within the definition of non-state actors.<sup>12</sup> The International Atomic Energy Agency (IAEA) Incident and Trafficking Database (ITDB) recorded unauthorized events involving nuclear and radiological material reported by the 142 participating States between 1993 and 2021. Despite only 2 per cent of the total 3,982 cases being related to trafficking or malicious use,<sup>13</sup> the risk of non-state actors supplying WMD proliferators or directly using such material should not be overlooked.<sup>14</sup> Past examples of non-state actors engaging in chemical and biological weapons programmes include the Aum Shinrikyo cult in Japan,<sup>15</sup> or, more recently, Islamic State in Iraq and the Levant (ISIL, also known as Da’esh) in Iraq and Syria.<sup>16</sup>

11 UN Security Council, Security Council resolution 1540 (2004), 28 April 2004, S/RES/1540 (2004), p. 1, [https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F1540\(2004\)&Language=E&DeviceType=Desktop&LangRequested=False](https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F1540(2004)&Language=E&DeviceType=Desktop&LangRequested=False) (last access 23.03.2023).

12 Christian Davies, Primrose Riordan, Chan Ho-him, “Inside North Korea’s oil smuggling: triads, ghost ships and underground banks”, Financial Times, London, 23 March 2023, available at <https://ig.ft.com/north-korea-oil-smuggling/> (last access 27.07.2023).

13 ITDB 2022 Factsheet, [itdb-factsheet.pdf \(iaea.org\)](itdb-factsheet.pdf(iaea.org)) (last access 23.03.2023).

14 Moreover, it is worth noting that some countries do not report to the ITDB, therefore the data recorded do not fully represent the size of the risk.

15 For more information on the cult’s financing and procurement activities see Parachini, John, Aum Shinrikyo in Aptitude for Destruction, Vol. 2, RAND Corporation, 2005, pp. 27-29.

16 UNITAD report on investigative progress regarding ISIL crimes in Iraq <https://press.un.org/en/2022/sc15127.doc.htm> (last access 31.03.2023).



International partners have supported jurisdictions in their efforts to strengthen security measures to prevent the acquisition of sensitive and weaponizable material and technology by terrorist groups. For example, in Southeast Asia, the Department of State's Global Threat Initiatives assisted the Philippine government in building capacity due to the presence of terrorist groups, such as the Abu Sayyaf Group, in the south of the country.<sup>17</sup> The UN also recently sanctioned ISIL (Da'esh) in Southeast Asia.<sup>18</sup>

The financing of WMD proliferation-related activities by terrorists stands at the intersection of the financing of terrorism and the financing of WMD proliferation. Since legislation on the financing of terrorism developed at an earlier stage, jurisdictions often cover the financing of WMD proliferation by violent non-state actors with the legislation combating the financing of terrorism. However, norms to combat the financing of terrorism (CFT) do not address the PF threat stemming from non-violent non-state

actors, as the activities of the latter are not driven by a terroristic purpose. In addition to the binding UN targeted financial sanctions for all Member States, some jurisdictions have autonomously adopted sanctions programmes on WMD non-proliferation. While there is no international requirement for the implementation of thematic sanctions programmes on WMD non-proliferation by UNSCR 1540 (2004), unilateral TFS function as national measures for the prohibition of the financing of WMD proliferation-related activities.<sup>19</sup>

By imposing unilateral targeted financial sanctions on individuals and entities, jurisdictions autonomously prevent the designated subjects from acquiring the financial resources to pursue activities related to WMD proliferation. Therefore, unilateral TFS strengthen the overall effectiveness of counter-proliferation financing efforts, especially when they are widely implemented, both as a disruptive tool and as a source of information on the financial flows.<sup>20</sup>

17 Bureau of Counterterrorism, US Department of State, "Country Reports on Terrorism 2019" and "Country Reports on Terrorism 2020", available at <https://www.state.gov/reports/country-reports-on-terrorism-2019/> ; <https://www.state.gov/reports/country-reports-on-terrorism-2020/> (last access 23.03.2023).

18 On 27 January 2023, the UN Security Council Committee approved the addition of the Islamic State East Asia Division to its ISIL (Da'esh) and Al-Qaida Sanctions List of individuals and entities subject to the assets freeze, travel ban and arms embargo, <https://press.un.org/en/2023/sc15186.doc.htm> (last access 23.02.2023).

19 Note 4, Annex 2, pp. 34 – 37.

20 The US sanctions programme on WMD non-proliferation is particularly impactful for its extraterritorial reach. Non-US persons engaging in transactions with subjects designated by the US risk incurring US secondary sanctions, even if there is no *nexus* between the transaction and the US jurisdiction. US secondary sanctions may compromise access to the US financial system, and therefore the US dollar, or may even comprise the business continuity of the sanctioned entity.



## 2.2 HOW PROLIFERATION FINANCING NETWORKS THREATEN SOUTHEAST ASIA

As mentioned, sanctions evasion and WMD procurement schemes are plans created by WMD proliferators for the illicit movement of goods as well as for the illicit flow of money through *ad hoc* networks. PF actors establish companies or other forms of legal entities or legal arrangements in different jurisdictions to obscure the identity of end-users/beneficiaries as well as the end-use of apparently licit transactions and businesses. For instance, networks may include front companies operating as trading companies or shell companies established to open bank accounts in jurisdictions with weaknesses in their national counter-PF regimes or the private sector. Any financial or advisory service provided to such PF actors constitutes proliferation financing.

The UN Panel of Experts assisting the 1718 Sanctions Committee reported in the past a significant DPRK presence throughout Southeast Asia. Such a presence was detected mainly in the form of agents and front companies for DPRK manufacturers in trade hubs or jurisdictions with more advanced dual-use goods sectors and in the form of accounts in banks based in financial hubs, not to mention the presence of conglomerates linked to the DPRK that are active in several continents and in several economic sectors.<sup>21</sup> The reported assistance to entities linked to the DPRK, such as with company registration and the opening of bank accounts by nationals, illustrates a pattern of sanctions evasion to move funds across jurisdictions or pay suppliers through local partners.

While DPRK proliferation networks appear to be by far the greatest PF threat to Southeast Asia, other proliferation financing activities may be carried out by the Iranian proliferation<sup>22</sup> network, supported by the Iranian business presence, as well as by terrorists or terrorist groups present in some areas of the region. In conclusion, WMD proliferation networks represent themselves a PF threat to Southeast Asian jurisdictions and are instrumental to other proliferation financing activities, including revenue-raising and WMD procurement.

21 For example, Malaysia-Korea Partners (MKP) Group of Companies. See UN Security Council, "Final Report of the Panel of Experts Submitted Pursuant to Resolution 2345 (2017)", S/2018/171, 5 March 2018, pp. 71, 72.

22 Iran's recent advancements in uranium enrichment in defiance of the thresholds agreed under the Joint Comprehensive Plan of Action, and the growing restrictions on the IAEA's ability to monitor potential diversion activities raise concerns on a new nuclear-threshold state (see David Albright, Sarah Burkhard, and Spencer Faragasso, "Updated Highlights of Comprehensive Survey of Iran's Advanced Centrifuges", 1 December 2022, <https://isis-online.org/isis-reports/detail/Dec-2022-updated-highlights-of-survey-of-irans-advanced-centrifuges/>).





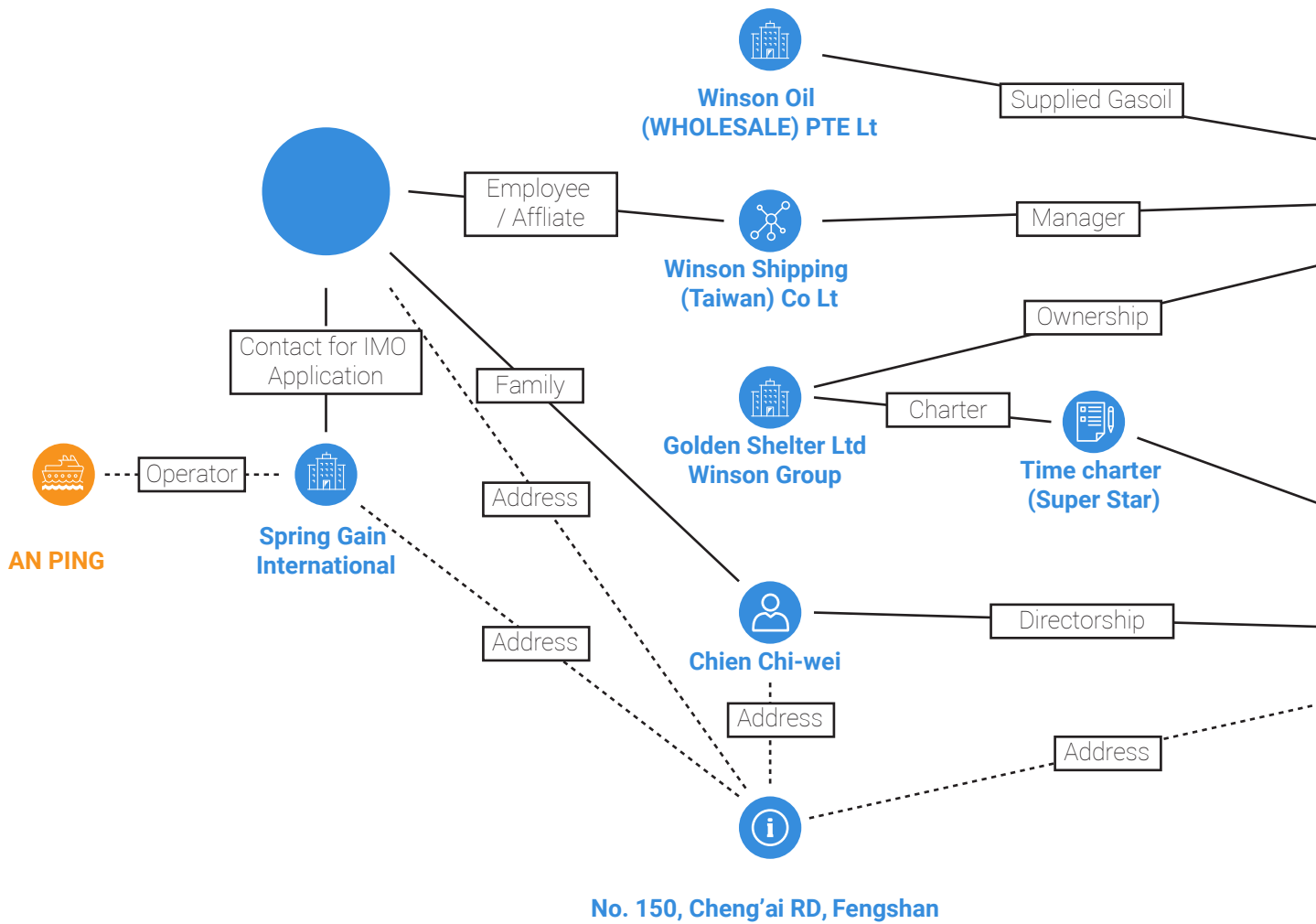
### 3. PROLIFERATION FINANCING THREATS FROM REVENUE- RAISING ACTIVITIES AND SANCTIONS EVASION

Over time, the UN Security Council's sanctions programme on the DPRK has evolved in response to the new evasion tactics. New developments in international sanctions have therefore further expanded the typologies that fall within the definition of proliferation financing. Although different from the original concerns more strictly related to the procurement of sensitive items, these sanctions have been adopted with the purpose of stopping the provision of funds, financial and other related services to the DPRK WMD programmes.

Nuclear weapons and ballistic missiles programmes require vast resources that countries are not always able to cover with the state budget, hence the need to raise funds through external sources and to access the international financial system. Since the first nuclear weapon test in 2006, the Security Council has progressively limited the DPRK's access to financing by imposing targeted financial sanctions on WMD proliferators and their networks, by imposing restrictions in certain key economic sectors and by prohibiting relevant forms of financial support and financial services through activity-based sanctions. Nevertheless, the DPRK has been able to keep the money flowing into its WMD programmes through sophisticated sanctions evasion tactics as well as other illicit means, including illicit cyberactivity.



### 3.1 TRADE SANCTIONS EVASION



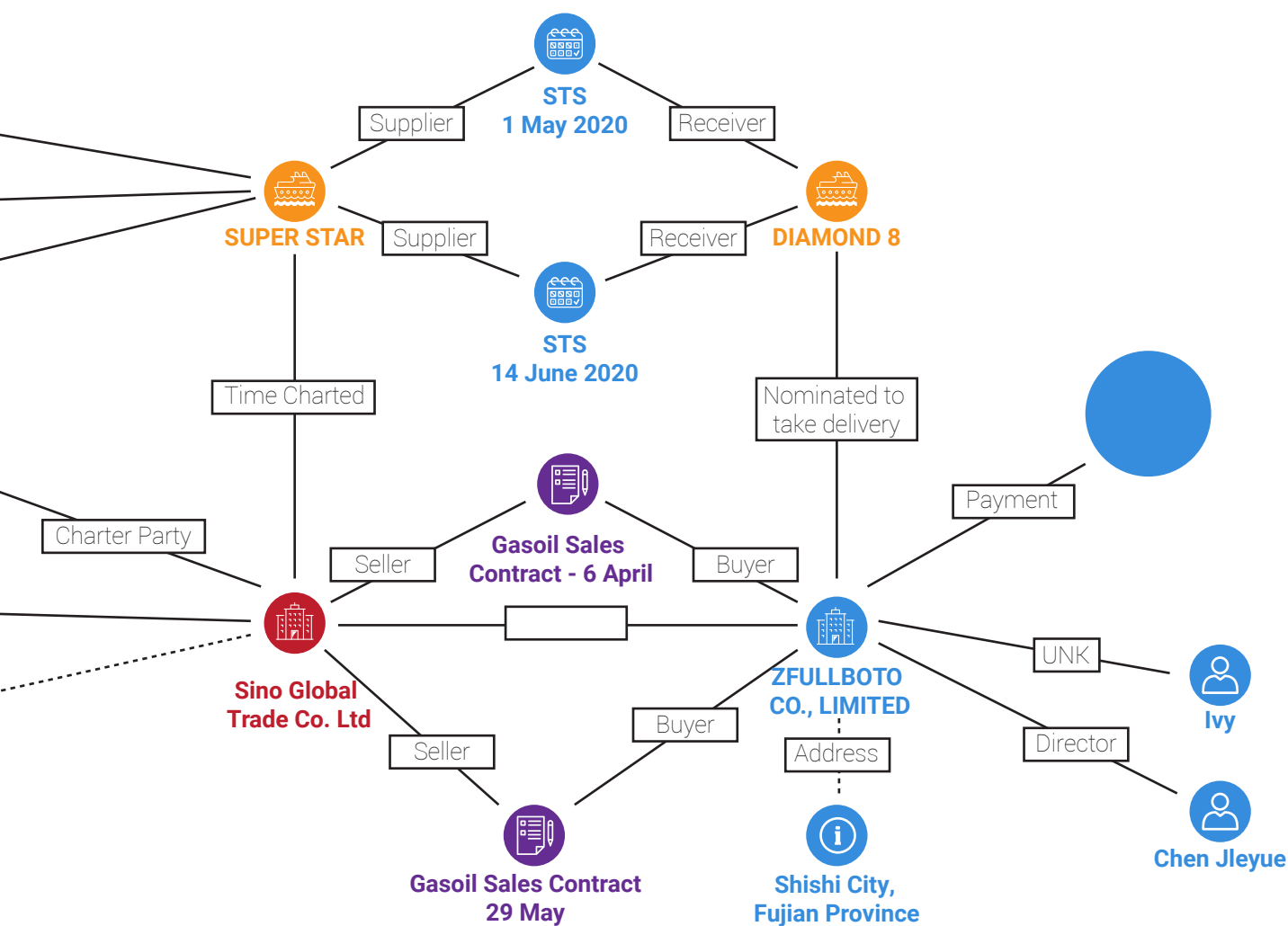
Source: UN Security Council, Final Report of the Experts Submitted Pursuant to Resolution 2569 (2021), S/2021/777, 8 September 2021, p. 50

Sectoral sanctions imposed on the DPRK represent restrictions imposed on the DPRK's economy. These sanctions have a dual purpose: to prevent the transfer of any good, material or technology that could contribute to the national WMD programmes; and to reduce DPRK incomes from exports to prevent the accrual of revenues presumably destined for WMD proliferation.

While these trade-related sanctions are not strictly financial *per se*, their implementation is key to counter-proliferation financing efforts to the extent that their violation may contribute to the financing of the DPRK WMD programmes.

The breach of the sanctions prohibiting the import or procurement of certain items from the DPRK, including non-sensitive goods, such as seafood, wood or textiles, is considered to be direct financing of the DPRK WMD programmes, as the payments are deemed as a source of foreign currency that the DPRK government might invest into the development of nuclear weapons or ballistic missiles.

On the export side, more intuitively, the UN Security Council has prohibited Member States from transferring goods, materials or technology that could be employed at any stage of the WMD development pro-



grammes, including dual-use goods, coal, iron, crude oil or steel. It goes without saying that the provision of financial and other related services for the evasion of trade sanctions also constitutes proliferation financing activities, as they indirectly contribute to the advancement of DPRK WMD programmes.

As sanctions regimes have expanded, evasion techniques have become more sophisticated, defying due diligence efforts from the region's traders and banks. The UN Panel of Experts reports that its investigations

on sectoral sanctions violations led them to networks of foreign traders scattered across the globe, involving, among others, the Southeast Asia region.<sup>23</sup> Investigations revealed cases of illicit fuel procurement by the DPRK through networks of entities based in Southeast Asia, such as the entities linked to the Singapore-headquartered Winson Group. A major oil trader and high-seas bunkering service provider, the group is one of the key nodes for the DPRK's oil procurement. It was involved in sanctions violation through the ship-to-ship transfers of oil carried out by the vessels Super Star and Diamond 8.

23 UN Security Council, "Final Report of the Panel of Experts Submitted Pursuant to Resolution 2345 (2017)", S/2018/171, 5 March 2018, p. 22.



## 3.2 PROLIFERATION FINANCING IN THE MARITIME SECTOR

Satellite imagery and information provided by Member States show that the DPRK has been violating trade restrictions imposed by the UN Security Council mainly by breaching the cap on the import of refined petroleum products and the export of sanctioned commodities, such as coal or sand. Maritime import-export operations are carried out through sophisticated tactics involving vessels – e.g. ship-to-ship transfers, misuse of automatic identification systems, false documentation – and corporate structures aiming to obfuscate the management or ownership of the vessels.

Featuring as director or shareholder of the company owning or operating a vessel engaged in sanctions violation exposes to proliferation financing risk, as does providing the services required to operate a vessel: from insurance services to crew services, to vessel classification or certification. Ship registration is a requirement under international law and the country of registration, or flag state, determines the nationality of the vessel, which is then allowed to sail internationally. Ship registries certify the compliance of vessels with specific standards for navigation. The provision of these forms of technical assistance to designated vessels or to vessels linked to designated entities or

individuals becomes instrumental to the illicit trade and therefore to the DPRK revenue-raising.

As reported by the UN Panel of Experts on the DPRK, in the past, such illicit practices also involved Southeast Asian jurisdictions. For instance, in 2012, the *Jie Shun*, a vessel trafficking arms manufactured in the DPRK, was registered under the Cambodian flag, with DPRK officials and crew certified by the Cambodian Maritime Administration.<sup>24</sup> More recently, the FATF's regional body Asia Pacific Group (APG) reported two cases<sup>25</sup> of Filipino nationals linked to vessels, which respectively delivered coal and refined petroleum, involved in a large number of financial transactions not reconcilable with their business activities. In one case, publicly available sources show that a Filipino national was the director of a company owning, managing and operating a vessel implicated in the delivery of refined petroleum products to the DPRK in April 2020. Financial investigations revealed that the Filipino national made cash deposits for more than \$5 million between 2005 and 2019, an amount not justifiable considering his business and which approximately equals his total debit, raising the concern that the account had served to manage the inflows and outflows from illicit activities.

24 The vessel was de-flagged in August 2016. See UN Security Council, "Final Report of the Panel of Experts Submitted Pursuant to Resolution 2276 (2016)", S/2017/150, 27 February 2017, pp. 30, 31.

25 Asia/Pacific Group on Money Laundering, "APG Yearly Typologies Report. Methods and Trends of Money Laundering and Terrorism Financing", July 2021, pp. 74, 75.

### 3.3 THE ROLE OF DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA OFFICIALS



DPRK diplomats, and more generally DPRK official representatives, have played a pivotal role in the pursuit of the national WMD programmes. Through a diplomatic presence in almost 50 jurisdictions and the abuse of the immunities and privileges guaranteed by the Vienna Convention on Diplomatic Relations, DPRK government officials, including representatives of sanctioned public companies, have both directly evaded sanctions and supported sanctions evasion efforts.<sup>26</sup>

While in 2013 the Security Council already acknowledged the threat from DPRK official representatives, calling upon Member States “to exercise enhanced vigilance,”<sup>27</sup> it was only in 2016 that the UN body decided that Member States must reduce the number of staff at DPRK missions and limit the number of bank accounts to one per mission and one per diplomat/consular officer.<sup>28</sup> DPRK diplomatic presence in a country requires the hosting jurisdiction to raise vigilance levels due to the role played by official representatives in facilitating WMD proliferation activities. The network of official representatives exposed jurisdictions to multiple PF threats, including WMD procurement, WMD proliferation networks and DPRK revenue-raising. Southeast Asia makes no exception.

For instance, in 2017, the UN Panel of Experts reported that the designated DPRK financial institution Tanchon Commercial Bank assigned two of its representatives to Viet Nam, disguised as diplomats.<sup>29</sup> Moreover, the September 2017 report reveals the Malaysia Korea Partners Group of Companies case, the Malaysian-DPRK joint-venture operating in the procurement of coal, undertaking business with a DPRK national based in Malaysia, who, after the revocation of their work permit, remained in Malaysia using a diplomatic passport issued by the DPRK.<sup>30</sup> Also in 2017, a DPRK diplomat was expelled from Myanmar after the UN Panel of Experts’ investigations revealed that he was acting on behalf of the designated DPRK entity Korea Mining Development Trading Corporation (KOMID).<sup>31</sup>

Another peculiar case involving the DPRK intelligence agent Kim Chol Sok shows how the apparatus in Pyongyang managed to enter Cambodia’s business environment, setting up hotels, casinos, restaurants and bars, and to operate such businesses undetected until mid-2020. Investigations by the national authorities revealed his other identity, Sok Kha, and his false documents, including a Cambodian diplomatic passport that he had used to register as director of a company with an active bank account.<sup>32</sup>

26 Daniel Salisbury, “From Missions to Missiles. The Role of North Korea’s Diplomatic Corps in Sanctions-Busting”, Royal United Services Institute, London, November 2022.

27 UN Security Council, Security Council resolution 2094 (2013), 7 March 2013, S/RES/2094 (2013), p. 5.

28 UN Security Council, Security Council resolution 2321 (2016), 30 November 2016, S/RES/2321 (2016), p. 4.

29 UN Security Council, “Final Report of the Panel of Experts Submitted Pursuant to Resolution 2276 (2016)”, S/2017/150, 27 February 2017, p. 57.

30 Note 7, pp. 24, 25.

31 Note 19, p. 43.

32 UN Security Council, “Final Report of the Panel of Experts Submitted Pursuant to Resolution 2569 (2021)”, S/2022/132, 1 March 2022, p. 76.



### 3.4 DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA WORKERS

In December 2017, the UNSC called upon Member States to repatriate DPRK nationals working abroad within 24 months to limit access to foreign currency by the DPRK through remittances. Consequently, by December 2019, Member States expelled DPRK workers based in their jurisdictions. Nonetheless, the UN Panel of Experts reported that in 2021 DPRK nationals were still employed in several jurisdictions across the globe, including in the Southeast Asian region, allegedly active in the fields of information technology, medicine, construction and catering.<sup>33</sup> Geographical proximity and more favourable entry conditions facilitate DPRK nationals' staying in some areas of Southeast Asia.

Geographical proximity, borders shared entirely with neighbouring countries and relatively easier access for DPRK nationals to the country make Lao PDR particularly susceptible to being a host state for DPRK workers. After the expiration of the December 2019 deadline, Lao PDR reported that all 28 nationals of the DPRK had been repatriated.

Similarly, the UN Panel of Experts is investigating two cases of DPRK nationals working in Cambodia for two DPRK entities, active despite being deregistered by the authorities in December 2019. In February 2022, the Cambodian authorities again deregistered the DPRK entities disguised under different identification details.<sup>34</sup>

33 UN Security Council, "Final Report of the Panel of Experts Submitted Pursuant to Resolution 2627 (2022)", S/2022/668, 7 September 2022, p. 73.

34 Note 29, pp. 73, 74.



### 3.5 VIRTUAL ASSETS

Arguably, the most concerning emerging trend in PF risk is the exploitation of virtual assets by PF actors. The potential for anonymity and untraceability in cryptocurrency transactions and the lack of oversight and regulation have paved the way for a flourishing criminal business, which has become a key source of income for the DPRK. Since 2016, the DPRK has been focusing on advancement in the cyber sphere to illegally raise and move funds.<sup>35</sup> These hacking operations have involved both fiat currencies and cryptocurrencies.<sup>36</sup>

However, the latter have recently offered a much more fruitful means of raising revenues while circumventing the international financial system, therefore evading financial restrictions. Pyongyang seized this opportunity by training groups of cybercriminals linked to the national intelligence agency Reconnaissance General Bureau, a governmental entity involved in conventional arms trade and designated by the UN Security Council.

35 UN Security Council, "Final Report of the Panel of Experts Submitted Pursuant to Resolution 2407 (2018)", S/2019/171, 5 March 2019, p. 48.

36 For instance, in 2016, in the infamous Bangladesh Bank cyber heist was executed by members of the DPRK 'Lazarus Group'. The hackers attempted to transfer USD 951 million of foreign reserves from the Bangladesh Bank's account at the Federal Reserve Bank in New York to accounts in the Philippines.



According to the 2023 Crypto Crime report by Chainalysis,<sup>37</sup> a blockchain data provider, 2022 was “the biggest year ever for crypto hacking”, with \$ 3.8 billion stolen from cryptocurrency businesses, of which \$ 1.7 billion was taken by DPRK-linked hackers. Almost 60 per cent of the DPRK groups’ illicit proceeds were sent to mixers to be laundered. Mixers are service providers that blend cryptocurrencies from different transactions to conceal the parties in exchange for a fee. Designed to protect financial privacy, mixers have been abused for money-laundering purposes.

In March 2022, the Ronin network, the blockchain network used by the popular game Axie Infinity, was hacked by the DPRK Lazarus Group, who exploited a vulnerability with the bridge that connected the Ronin network to the main Ethereum network.<sup>38</sup> Part of the stolen funds were sent to the virtual currency mixer Blender, which pooled them together with other funds, applying a certain algorithm. The obfuscated funds were then sent to different wallet addresses, some of them owned by Lazarus Group hackers or affiliated entities.

While virtual assets and virtual asset service providers (VASPs) are spreading across Southeast Asia, the thre-

at of PF actors using financial institutions and VASPs to raise, move or to exchange cryptocurrencies is of growing concern. Some Southeast Asian jurisdictions, such as Malaysia and Viet Nam, were among those targeted by the cybercriminals.<sup>39</sup>

The development of the virtual assets industry also found favourable conditions in Lao PDR: while the surplus in production of hydroelectric power paves the way for profiting from mining and trading digital currencies, the restrictions on cryptocurrencies imposed in China left the space for Vientiane to seize a market share. At the end of 2021, Vientiane launched its first crypto-mining operations, authorizing six companies to mine and trade cryptocurrencies. Therefore, after protracted discussions on regulation and security, the first trading platforms began to operate licensed by Bank of the Lao PDR.<sup>40</sup> However, the plan to expand this business, and thus the incomes generated by crypto-mining, exposes virtual asset service providers to the threats of DPRK cyberattacks. For instance, the potential for greater income in the Lao crypto mining industry represents a revenue-raising opportunity for DPRK cybercriminals specialized in cryptojacking, that is the practice of hacking devices to mine for cryptocurrencies.

37 Chainalysis, “The 2023 Crypto Crime Report”, February 2023, pp. 60, 61. The report can be found here: <https://go.chainalysis.com/2023-crypto-crime-report.html>.

38 Note 32, p. 76.

39 UN Security Council, “Final Report of the Panel of Experts Submitted Pursuant to Resolution 2464 (2019)”, S/2019/691, 30 August 2019, pp. 109, 110.

40 John Reed, “Laos pushes into crypto as it authorises mining and trading”, Financial Times, London, 16 September 2021, available at <https://www.ft.com/content/3a820200-0128-42b3-be6c-f5abd6381efa> (last access 23.03.2023).





# CHALLENGES TO IMPLEMENTING COUNTER PROLIFERATION FINANCING REGIMES IN SOUTHEAST ASIA

This part of the report looks at general challenges when implementing a national CPF regime, as well as implementation challenges specific to Southeast Asia. These emerged during the in-country workshops and the consultations in Turin with the competent national authorities from the Philippines, Lao PDR and Cambodia. The sections below also summarize the measures discussed to address the specific challenges, with the objective of identifying priority actions and paving the way for further capacity-building initiatives.

Countering proliferation financing is an endeavour compounded by inherent challenges, including the lack of an official and generally accepted definition of PF, and the complexity in identifying its scope due to its cross-cutting and dynamic nature.

The lack of an official definition of proliferation financing hinders a coordinated international effort in countering the financial crime, therefore providing margins of manoeuvre to WMD proliferators in those jurisdictions where proliferation financing is perceived as a more limited phenomenon. Thus, the lack of a PF definition may prevent harmonization among legal frameworks and, more generally, among national CPF regimes, not to mention the hurdles it creates to international cooperation.

Proliferation financing intersects different matters, such as export controls, international sanctions and WMD non-proliferation. Although it might be challenging for the national authorities in charge of these different areas to coordinate and share information, siloed approaches are likely to fail to prevent PF activities. Similarly, a static approach would soon become obsolete due to the evolving nature of proliferation financing. New forms of financial support expand the range of PF threats. As noted in the Glacom case (see above, Procurement

Schemes), in addition to the international financial system, PF actors are increasing the use of alternative payment systems, including bulk cash transfers, ledger systems, bartering, the use of gold and precious metals and, most importantly, the use of virtual assets to raise, move and use funds. More recently, challenges to the current world order and the extensive use of financial sanctions are indirectly prompting efforts to design new parallel systems, which might represent opportunities for malign actors, including WMD proliferators.

With respect to more practical aspects, the detection of PF activities presents numerous challenges due to the ostensible legitimacy of the transactions, the technical knowledge required to identify dual-use goods and the intricacy of WMD proliferation networks. The transactions often involve indirect parties not detected by sanctions screenings and frequently implicate dual-use goods items traded in licit commercial transactions. However, despite the appearance of legitimacy, the multi-layered ownership structures, possibly featuring shareholders based in less transparent jurisdictions, might in fact hide UN-designated entities or end-user beneficiaries.

Moreover, although classifying the export of dual-use goods as a risk factor helps assess the transaction, identifying the good is complex, as it requires technical knowledge of the items featured in the control lists. However, there is not always a qualified expert to identify the good due to a limited number of trained professionals.

The following sections identify tools to address some of the above-mentioned inherent challenges and the specific ones observed in the countries that participated in UNICRI's project, namely Cambodia, Lao PDR and the Philippines.

# 1. LEVEL OF AWARENESS OF PROLIFERATION FINANCING-RELATED RISKS

In November 2022, UNICRI conducted the first awareness raising workshop on proliferation financing in Lao PDR. Altogether 25 experts from different agencies participated in the two-day event. While some participants learnt of PF for the first time, the leading authorities in counter-proliferation financing, namely the Anti-Money Laundering Intelligence Office (AMLIO), showed an understanding of the illicit financial activity that reflected the FATF's narrow definition of PF risk, notably the risk related to the breach, non-implementation, or evasion of UN Security Council's targeted financial sanctions on the DPRK and Iran. Moreover, as explained by Lao experts in the workshop in Turin, the limited awareness of WMD proliferation and the differences between CFT and CPF represents a challenge to an effective national CPF system.

In Cambodia, UNICRI's presentation and questions from the reference documents triggered discussions on PF threats and cases, from which an uneven level of awareness emerged among competent national authorities. Cambodia's February 2019 high-level political commitment with the FATF and the APG included a plan of reforms, which, among other objectives, was aimed at "establishing a legal framework for implementing UN sanctions related to targeted financial sanctions for PF and providing training to strengthen the skills of competent authorities to implement targeted financial sanctions for PF".<sup>41</sup> While FATF acknowledged the progress achieved hitherto, Cambodia's endeavours have been mainly directed at completing this plan. Therefore, the understanding of PF that emerged from the consultations was mostly linked to UN targeted financial sanctions on entities and individuals designated under WMD non-proliferation programmes.

Since February 2019, several international partners have supported Filipino authorities through awareness-raising events, workshops and training on coun-

ter-proliferation financing, and assistance in drafting an *ad hoc* bill on CPF and its implementing rules. Thus, there seems to be a good understanding of PF, which is also attributable to knowledge and expertise developed in export controls, as demonstrated by the above-mentioned case of catch-all clause for the export of 1,760 Servos (see above, Procurement Schemes). Nonetheless, in the Philippines, PF is still a relatively new topic to some authorities.

## WHAT CAN BE DONE TO INCREASE AWARENESS OF PROLIFERATION FINANCING-RELATED RISKS?

During the workshop in Turin, countries discussed several forms of training<sup>42</sup> that could help resolve the challenges linked to a limited understanding of PF and its related areas. In particular, all three participating countries requested training on PF-related international sanctions compliance (or re-training on new trends); Lao PDR and Cambodia requested training on the PF legal framework; and Cambodia asked for support with outreach and communication strategies. These more general trainings would be targeted at members of inter-agency mechanisms, supervisory authorities, prosecutors, and law-enforcement authorities.

Moreover, the Philippines and Cambodia highlighted the importance of having more specific training for reporting entities on the identification of suspicious transactions, as well as more targeted training regarding detection, investigation and prosecution of proliferation financing activities.

With regard to the preferred form of training delivery, the participating countries indicated the "Train the Trainers" (TTT) model, either at the national or regional level, as a more sustainable approach.

41 FATF, Jurisdictions under Increased Monitoring - 21 October 2022, <https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoring-october-2022.html#:~:text=When%20the%20FATF%20places%20a,as%20the%20%E2%80%9Cgrey%20list%E2%80%9D>. (last access 23.02.2023).

42 For a more detailed overview of the pressing capacity-building needs, refer to the Annex of the report.

# RISK

LOW



HIGH



## 2. UNDERSTANDING EXPOSURE TO PROLIFERATION FINANCING RISKS

While raising awareness of the existence of proliferation financing risk represents the first step, the path towards adopting and implementing a CPF regime requires overcoming challenges such as: 1. defining PF and its scope; 2. understanding who are the PF actors or what are the PF activities that may threaten the jurisdiction, as well as the domestic weaknesses and the contextual factors that may attract PF networks; 3. strategizing a common response through the effective allocation of resources; and 4. adjusting to the evolution of PF threats and the global security landscape.

The production of a proliferation financing national risk assessment (PF-NRA) is pivotal to the counter-proliferation financing effort because the document results from reflections on PF. These reflections can be more general, such as the concept of PF as an illicit phenomenon, and more specific, such as how PF risk can affect the jurisdiction undertaking the assessment. Furthermore, the PF-NRA process requires a concerted approach, which deconstructs any previous siloed approach, therefore paving the way for institutionalized cooperation.

PF national risk assessments also outline the legal frameworks the countries have in place to address some or all of the aspects of proliferation financing, therefore highlighting possible legal gaps. Thus, these documents establish the premises for the adoption of specific legislative approaches by competent national authorities, ranging from amendments to the legislation and/or regulation in place to passing a comprehensive piece of legislation on CPF. Having a legal definition of

PF dissolves any ambiguities on the financial crime and facilitates harmonization among different pieces of legislation, therefore limiting PF actors' exploitation of uneven understandings of PF. Additionally, it fosters international cooperation in CPF.

At the time of the in-country workshops,<sup>43</sup> none of the partner countries had published their proliferation financing national risk assessment (PF-NRA) as per FATF's Recommendation 1. However, the Philippines has since initiated the PF risk assessment process with the assistance of the EUP2P Export Control Programme and King's College London, as presented at the experts' meeting in Turin in March 2023. Seventeen government agencies will undergo the risk assessment process and define mitigation strategies. The Philippines requested support in the review of the draft PF-NRA and in the follow-up phase on the implementation of the recommendations.

During the regional expert's meeting in Turin, both Cambodia and Lao PDR requested support in drafting their PF-NRA. The assistance needs range from providing advice more generally on a methodology to more specific support on preparatory meetings (e.g. introducing proliferation financing, defining scope and stakeholders) or regular calls to consult with experts throughout the process. Furthermore, Cambodia affirmed it would benefit from sharing good practices with experts from other countries, whereas Lao PDR focused more on the review of the draft PF risk assessment as well as assistance in the follow-up phases (e.g. implementation and outreach).

43 In-country workshops were held between October 2022 and January 2023.



### 3. EFFECTIVE INTER-AGENCY COOPERATION AND COORDINATION

The cross-cutting nature of proliferation financing, the ostensibly legitimate character of the transactions and the sophisticated tactics adopted by PF networks make the prevention, detection and response to the illicit financial activities challenging for the competent authorities, usually operating in their specific remit. The information obtained by a single agency may not be sufficient to build a PF case. Even if an agency detected suspicious activities, identifying the network and disrupting the illicit financial flows related to WMD proliferation could be hampered by a lack of knowledge and capabilities, which may reside in other agencies.

This makes the establishment of an inter-agency framework for cooperation, coordination and information-sharing crucial for an effective CPF regime. Although existing frameworks on anti-money laundering (AML) and counter-terrorism financing (CFT) may

also be suitable for CPF, peculiar features of the latter should be considered in the composition of inter-agency mechanisms, particularly the export control, sanctions and wider WMD non-proliferation dimensions. Similarly, in those jurisdictions where WMD counter-proliferation systems are in place, the PF element could be integrated in the relevant structures.

As stated above, the PF-NRA drafting process triggers inter-agency cooperation, which may represent the basis for establishing an actual inter-agency framework in compliance with FATF's Recommendation 2. Such a process highlights the need for information exchange with agencies operating in specific domains, for example in export controls, customs, and implementation of UN restrictive measures on the DPRK and Iran<sup>44</sup> or of UNSCR 1540 (2004). This mechanism can be implemented through specific legislation or regulation defi-

44 UNSCR 2231 (2015), endorsing the Joint Comprehensive Plan of Action (JCPOA), terminated the UN sanctions programme on Iran, but retained targeted financial sanctions on individuals and entities (see UNSCR 2231 (2015) paragraph 6(c) of Annex B) and established a limited number of restrictive measures, including on financial services related to nuclear technology.



ning cooperation, coordination and processes balancing information sharing and legitimate issues of data protection, both at policy level and at operational level.

In the three countries participating in UNICRI's project, existing inter-agency mechanisms have been used to discuss PF-related issues. The forms of inter-agency mechanisms in place reflect the different understanding of PF. In the Philippines, the National Security Council – Strategic Trade Management Committee deals with several aspects of proliferation financing, including strategic trade control and implementation of restrictive measures on the DPRK and Iran.<sup>45</sup>

During the experts' meeting in Turin, Lao authorities presented the inter-agency frameworks in place on AML/CFT, CBRN counter-proliferation, and dual-use goods. They requested assistance with the establishment of a PF specific inter-agency mechanism and the creation of related informational material (e.g. handbooks, leaflets) to circulate internally. Similarly, Cambodian authorities, building on the framework established by the June 2020 AML/CFT Law, together with the June 2020 CPF Law,<sup>46</sup> underlined the challenge of implementing an effective PF inter-agency coordination mechanism. Consequently, they requested assistance in establishing a sub-committee competent on proliferation financing.

45 It should be stressed that, after the end of the UNICRI initiative, the Philippines expanded the powers and functions of the inter-agency National AML/CFT Coordinating Committee (NACC) by adding the development of CPF policies and implementation of the CPF strategy to the NACC's mandate. The Philippines also created a specific Proliferation Financing Sub-Committee within the NACC tasked, among other things, with the development, and implementation of action plans on PF detection, investigation and prosecution.

46 The June 2020 Laws established the National Coordination Committee, which, more generally, sets out policies and coordinates and monitors the implementation of relevant targeted financial sanctions. More specific provisions on the National Coordination Committee can be found in the Sub-Decree no. 160 ANK.BK on The Organization and Functioning of The National Coordination Committee on Anti-Money Laundering and Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction.



## 4. INVOLVING THE PRIVATE SECTOR

---

The private sector plays a key role in proliferation financing. Banks and gatekeepers<sup>47</sup> are not the only businesses exposed to PF networks; other economic sectors involved in WMD procurement schemes are also at risk: strategic goods manufacturers, operators in the maritime industry, insurance companies, the defence sector, money or value transfer services, and virtual asset service providers. As a first line of defence, the private sector should be the first to detect suspicious activities and trigger further investigations.

Thus, after the inter-agency mechanism, a second dimension of CPF cooperation is represented by the contributions that the public and private sectors can provide to each other: financial institutions report suspicious transactions and activities, share analysis on trends and inform the supervisory authorities of their own risk assessments; at the same time, the supervisory authorities, with the support of other relevant agencies, assist the private sector by providing training, guidance, best practices, red flags and any information useful to direct the private sector's CPF efforts.

To further enhance the existing public-private partnership mechanism, the Monetary Authority of Singapore plans to introduce a digital platform called COSMIC

(Collaborative Sharing of ML/TF Information and Cases) The platform will enable financial institutions to share information on customers to detect and deter money laundering, terrorist financing and proliferation financing.

As a first step, a legislative framework has been established to govern the transfer of data, and ensure that the information is shared only for AML/CFT/CPF purposes and that it is shared in a proportionate manner to enable timely risk assessment and mitigation actions to be taken. This initiative seeks to address information gaps which exist as financial institutions can only see their own transactions. Criminals have exploited such information gaps through the use of networks of front or shell companies across different financial institutions to conduct illicit activities. Such an initiative – which was highlighted by a representative from the Monetary Authority of Singapore at the expert-level workshop in Turin – raised interest from other participating countries in having a similar platform aimed at detecting risk indicators in customers' accounts.

However, the implementation of public-private cooperation presents some challenges. The Anti-Money Laundering Council (AMLC) and the Strategic Trade Mana-



gement Office (STMO) are two authorities leading the CPF efforts in the Philippines that are active in outreach initiatives (e.g. awareness forums, sectoral information sessions, targeted outreach, online training). These authorities stressed the challenge of sensitizing the whole range of economic operators that might be involved in PF activities, not only financial institutions and DNFBPs, but others such as exporters, brokers or freight forwarders.

For this reason, the Philippines requested support to improve outreach activities through initiatives aimed at raising awareness and sharing best practices in the above-mentioned sectors and to assist with the acquisition of the technology, enabling the enhancement of public-private cooperation based on the model of the COSMIC digital platform. Additionally, since competent authorities ensured that information sharing does not pose a compatibility issue with other provisions (e.g. on confidentiality or data protection), Philippine authorities requested assistance in the production of informational materials and media outreach to encourage the participation of smaller financial institutions in the mutually beneficial public-private cooperation efforts.

One of the points of Cambodia's commitment with the FATF and the APG was raising awareness of PF in the private sector, in particular the banking sector. From the discussions in Phnom Penh and the experts' meeting in Turin, it emerged that approximately 800 representatives from financial institutions and 2,000 participants from DNFBPs have attended workshops on proliferation financing and on the PF Law since 2022. National authorities have also disseminated information on the CPF Law through media outlets and social media. However, limited understanding of PF among stakeholders, lack of resources and scarce public awareness still hold Cambodia back from an effective CPF system. As a result, experts from Cambodia requested assistance with awareness raising and best practice sharing events for national authorities on CPF public-private cooperation.

Lao PDR's limited human resources and infrastructure in CBRN counter-proliferation and illicit trafficking stressed the importance of raising awareness on CPF public-private cooperation, also through training for national authorities engaging with particular sectors and requesting relevant informational material (e.g. handbooks and leaflets).



## 5. INTERNATIONAL COOPERATION

---

A key challenge to the detection and disruption of PF networks is represented by the transnational nature of proliferation financing, whose schemes, as mentioned above, involve multiple jurisdictions, both from the perspective of the commercial transactions and the financial transactions. Therefore, although not explicitly required by relevant UNSC resolutions or PF-specific FATF recommendations, international cooperation on proliferation financing is crucial to countering PF activities. This cooperation begins with a collaborative attitude towards the international and regional organizations that are monitoring and assisting the effective implementation of the obligations stemming from relevant international instruments and investigating cases of international sanctions breaches or evasion.

Equally, information exchanges facilitate the reconstruction of the “mosaic transactions” which are designed by WMD proliferators and operated through their transnational networks. These “mosaic transactions” add layers of complexity and hamper the detection, possible investigation and prosecution of their procurement schemes. Information exchanges between countries allow the competent authorities to piece together more elements of these complex schemes, aiding their detection and investigation. Other cataly-

sts for international cooperation are a shared understanding of what PF is and the harmonization of legal frameworks and procedures.

However challenging, this objective can be achieved through regional initiatives aimed at bringing together stakeholders from different jurisdictions to discuss, with the support of independent subject matter experts, the general understanding of PF as well as specific best practices and cases. Participation in PF-related regional and international training and capacity-building workshops is critical to acquiring knowledge and expertise, in addition to building a common network to counter PF threats. Yet, it is important to consider the financial challenges and limited resources available to join these international initiatives, as highlighted by national authorities from Lao PDR.

As confirmed by the workshop in Turin, multilateral settings facilitate awareness raising and sharing of best practices. Hence, regional-specific events, as well as more advanced training sessions on the different dimensions of proliferation financing, such as international financial standards and sanctions implementation, will enhance regional cooperation among competent authorities, significantly strengthening countering proliferation financing in Southeast Asia.



# IDENTIFIED PRIORITY ACTIONS AND RECOMMENDED STEPS

Despite being one of the most exposed regions to proliferation financing risks, Southeast Asia has the potential to play a pivotal role in the disruption of DPRK proliferation financing schemes. It can also use its position and growing international clout to counter proliferation financing risks associated with PF threats from other countries of proliferation concern and from domestic threats. The development of solid counter-PF regimes across the region can compromise the DPRK's access to significant sources of revenue as well as the goods, materials and technology required for its WMD programmes. However, the complexity of this issue, compounded by regional challenges, risks hindering the effectiveness of counter-PF initiatives. Therefore, based on countries' challenges and requests reported above, the following priority actions have been identified:

- Participate in international, regional and national training related to counter-proliferation financing activities and international norms to develop a broader and more coherent understanding of PF and in tailored activities to build national authorities' and relevant professionals' CPF capabilities;
- Draft a dedicated risk assessment on proliferation financing to become aware of a country's exposure to the PF risks and consequently to adopt the necessary mitigation measures, including national measures to implement PF-related international obligations;
- Build on the current inter-agency frameworks and develop an *ad hoc* PF specific mechanism or a PF specific sub-committee to an existing counter-proliferation committee to share information, co-operate, and co-ordinate CPF efforts;
- Enhance public-private cooperation and outreach initiatives through the distribution of informational material and the use of media channels and other technological means (e.g. digital platforms) to involve as many stakeholders as possible and to address the limited awareness level of PF in the private sector; and
- Participate in regional CPF initiatives to learn about the transnational PF dimension, PF network tactics and to develop a CPF network based on mutual assistance through best practice sharing and collaboration in CPF efforts.

1



PF Training

2



Draft a  
PF-NRA

3



Establish an  
interagency  
framework

4



Enhance  
public-private  
cooperation

5



Participate  
in regional  
CPF initiatives



## THE WAY FORWARD

On 28 April 2023, UNICRI was awarded a second grant to further enhance the capacities of Cambodia, Lao PDR and the Philippines to address proliferation financing risks through the effective identification and investigation of PF schemes and procurement networks. This follow-up phase has recently started and will encompass regional training on: (i) international standards and sanctions; (ii) financial intelligence collection and investigation techniques; as well as the development, publication and dissemination of guidelines for the private sector on the timely identification of red flags of suspected PF activities. It is also worth noting that UNICRI is enhancing efforts to sensitize the international community on the threat posed by proliferation financing and is levera-

ging any relevant platform – within and beyond the UN – to spotlight this issue. As part of these ongoing efforts, UNICRI (with the support of the UK) was instrumental in ensuring the commitment from the Italian Ministry of Foreign Affairs in having counter-proliferation financing as one of the key priorities at the 2024 Presidency of the Global Partnership.

UNICRI is also trying to establish a solid, comprehensive programme on counter-proliferation financing consisting of activities that can be implemented globally and considers pressing capacity-building needs. Indeed, to date, assistance on this matter has been fragmented, and a full-fledged, UN-led initiative with global breadth is currently missing.

# ANNEX

PRIORITY NEEDS IN TERMS OF TECHNICAL ASSISTANCE/CAPACITY BUILDING THAT EMERGED AT THE WORKSHOP IN TURIN, ITALY FROM 14 TO 16 MARCH 2023.

Country	Topic	Target audience
All three countries	Sanctions compliance*	Governmental agencies and private sector
All three countries	Collection/analysis of financial intelligence*	Governmental agencies
All three countries	Investigation/prosecution of PF*	Governmental agencies
All three countries	Suspicious transactions, PF typologies and red flags*	Governmental agencies and private sector
Cambodia and Lao PDR	Legal frameworks	Governmental agencies
All three countries	Good practices from other Member States*	Governmental agencies and private sector
All three countries	National risk assessment (methodology, review, follow-up phase)	Governmental agencies and private sector
All three countries	Regular awareness workshops	Private sector
All three countries	Drafting of handbooks/guidelines/leaflets	Private sector
The Philippines	Digital platforms to improve public-private cooperation	Private sector and governmental agencies
Cambodia	Establishing or enhancing (existing) inter-agency committees (or sub-committees)	Private sector and governmental agencies

\*These issues will be tackled through the implementation of Phase II of the project.





**unieri**

United Nations  
Interregional Crime and Justice  
Research Institute

