Financing the Bomb with Blockchain

Understanding the Implications of Virtual Asset Use in Proliferation Financing Networks: A Case Study on North Korea

Financer la Bombe par la Blockchain

Comprendre les implications de l'utilisation des actifs virtuels dans les réseaux de financement de la prolifération: une étude de cas sur la Corée du Nord

A Thesis Submitted to the Division of Graduate Studies

of the Royal Military College of Canada

by

Ariel Burgess

In Partial Fulfillment of the Requirements for the Degree of

Master of Arts, War Studies

May 2026

Acknowledgements

First and foremost, my deepest gratitude to Dr. Christian Leuprecht for his mentorship, insight, and guidance throughout this process. I am extraordinarily fortunate to have been supervised by a scholar who is not only a leading expert in this field but also exemplifies the ideals of academia: a commitment to building communities of inquiry, collaboration, and collegiality. I am also incredibly grateful to the RMC War Studies Department, particularly Dr. Sarah Hill. Without her support, I would have lost faith in myself.

I also wish to acknowledge SSHRC and the Department of Defence. Through the CGS-M and MINDS scholarship programs, their support has made this thesis possible and significantly contributed to my educational development.

I am grateful to the following individuals who have supported me personally and professionally over the course of this work:

To Mikayla Ozga, Nicholas Donaldson, and Liam Burns for their insights and friendship.

To Justine Chaput, for her friendship, generosity, and example - your sisterhood is treasured.

To Jasmine Weir and Zachary Brooks, whose love, humor, and perspective have been a constant source of encouragement and have shaped me into the person I am.

To my horse, Rooster, for his steady presence in essential moments of peace, joy, and personal growth.

To my dog, Jaegar, for his unwavering companionship and dedication to our joint thesis writing/couch nap schedule.

To my family, for everything.

Abstract

This thesis argues that the expansion of proliferation financing into decentralized digital systems has altered both the structure and strategic logic of illicit finance, reducing the effectiveness of chokepoint and visibility-dependent counter-proliferation financing (CPF) mechanisms. To investigate this transformation, this study presents the first empirical dataset documenting virtual asset–enabled proliferation financing (VA-PF), tracking twelve cases of North Korean state-sponsored network operations. Utilizing the Democratic People's Republic of Korea (DPRK) as a critical case study, this research introduces the Virtual Asset Proliferation Risk Model (VA-PRM)—an adaptation of the Terrorist Resourcing Model—to systematically identify patterns, trends, and vulnerabilities within these networks.

It finds that by leveraging VAs, the DPRK has decoupled its proliferation networks from traditional institutional frameworks, collapsing previously distinct stages of asset acquisition and laundering into a single, fluid process. To evaluate the systemic consequences of this shift, this thesis introduces the original Enforcer/Shield/Challenger (E/S/C) framework. Grounded in international relations theory, this framework offers a tool for understanding how decentralized networks reshape global power relations and challenge state compliance with the implementation of current CPF regimes. This thesis concludes that virtual asset–enabled proliferation financing (VA-PF) fundamentally erodes traditional state oversight and incentivizes systemic shifts in the strategic behavior of actors operating within the global CPF architecture. Ultimately, this study addresses a critical gap in international security and illicit finance literature and offers directions for future empirical research as well as potential avenues for policy, enforcement capacity-building, and pre-emptive interdiction.

Résumé

Cette thèse soutient que l'expansion du financement de la prolifération vers les systèmes numériques décentralisés a modifié à la fois la structure et la logique stratégique de la finance illicite, réduisant l'efficacité des mécanismes de lutte contre le financement de la prolifération (LFP) dépendants de la visibilité et des points de contrôle. Pour étudier cette transformation, cette étude présente le premier ensemble de données empiriques documentant le financement de la prolifération par les actifs virtuels (FP-AV), en suivant douze cas d'opérations de réseaux parrainés par l'État Nord-Coréen. En utilisant la République Populaire Démocratique de Corée (RPDC) comme étude de cas critique, cette recherche introduit le Modèle de risque de prolifération des actifs virtuels (VA-PRM) — une adaptation du Modèle de ressourcement terroriste — afin d'identifier systématiquement les tendances, les modèles et les vulnérabilités au sein de ces réseaux.

Elle révèle qu'en tirant parti des actifs virtuels, la RPDC a découplé ses réseaux de prolifération des cadres institutionnels traditionnels, fusionnant des étapes auparavant distinctes de l'acquisition et du blanchiment d'actifs en un processus unique et fluide. Pour évaluer les conséquences systémiques de cette transition, cette thèse introduit le cadre original Exécuteur/Bouclier/Contestataire (E/S/C). Ancré dans la théorie des relations internationales, ce cadre offre un outil pour comprendre comment les réseaux décentralisés remodèlent les relations de pouvoir mondiales et remettent en question la conformité des États dans la mise en œuvre des régimes actuels de LFP. Cette thèse conclut que le financement de la prolifération par les actifs virtuels (FP-AV) érode fondamentalement la surveillance étatique traditionnelle et incite à des changements systémiques dans le comportement stratégique des acteurs opérant au sein de l'architecture mondiale de la LFP. En fin de compte, cette étude comble une lacune critique dans la littérature sur la sécurité internationale et la finance illicite, et propose des orientations pour de futures recherches empiriques ainsi que des pistes potentielles pour l'élaboration de politiques, le renforcement des capacités d'application de la loi et l'interdiction préventive.

Table of Contents

Chapter 1: Introduction

Despite decades of international sanctions and surveillance, the Democratic People's Republic of Korea (DPRK) has continued to expand the scale and sophistication of its nuclear weapons program. This persistence and complexity cannot be reduced to the failure of sanction regimes. It must be interpreted instead as a strategic adaptation to a hostile threat environment. The mechanisms by which proliferators generate, store, and transfer resources for nuclear development - collectively termed proliferation financing (PF) - have evolved alongside North Korea's strategic doctrine to incorporate virtual assets (VAs). This evolution has allowed the Kim regime to sustain an advanced weapons program despite formal isolation from the global systems of finance and trade. This exposes a fundamental misalignment in managing proliferation in the digital age that this thesis contends with: the world is trying to enforce old rules against an actor playing a new game.

1.1 Virtual Assets: The Transformative Opportunity in Proliferation Financing

Current counter-proliferation financing (CPF) regimes operate on an assumption of visibility: illicit flows, must, at some point, pass through regulated global economic structures. Accordingly, identification and interdiction mechanisms have relied upon chokepoint controls and measures such as sanctions, designed to intercept transactions at identifiable nodes and deter would-be proliferators by denial.[1] Such enforcement logic presumes that proliferators require

[1] Sonia Ben Ougrham-Gormley, "Banking on Nonproliferation," *The Nonproliferation Review* 19, no. 2 (2012): 255, https://doi.org/10.1080/10736700.2012.690963.

consistent access to legitimate financial systems, therefore their activities can be constrained through traditional regulatory and judicial frameworks.

This thesis challenges that assumption. While North Korea's cyber activities and cryptocurrency thefts are well documented, the degree to which VAs have been integrated into its PF structures remains underexplored. This study argues that VAs have become a central component of the DPRK's proliferation strategy, and that their adoption represents a structural transformation in the PF environment. VAs introduce a new dimension to the threat landscape. The emergence of new digital assets such as cryptocurrency fundamentally reshapes understandings of threat capability, intent, and offender opportunity to act on these. By nature of their existence in a compliance-resistant financial ecosystem, VAs enable value transfer outside the jurisdictional reach of conventional CPF frameworks.

This transformation is driven by the convergence of digital-enabled capabilities and proliferation success. As a result, the greatest danger posed to implementation of the counter-proliferation regime is not solely overt nuclear capability. Rather, this thesis hypothesizes states' adaptive and resilient financial architecture is equally as important as technological or nuclear capacity. The DPRK provides a critical stress test to analyze this dynamic: cyber-warfare, nuclear proliferation, and sanctions evasion have become increasingly symbiotic components of a broader geopolitical strategy. VAs provide the central enabling mechanism through which North Korea can advance its interests.

As the most persistently sanctioned state with an active nuclear weapons program, and a state with institutionalized illicit revenue generation, the DPRK embodies the conditions under

which VA-enabled PF (VA-PF) can thrive. Exclusion from global payment systems such as the Society for Worldwide Interbank Financial Telecommunication (SWIFT), a singular focus on weapons and technology development as a basis for economic and military growth, and an advanced cyber program have incentivized the development of novel proliferation strategies.

1.2 Thesis Statement & Research Questions

The current CPF regime is systematically undermined by two key factors: the political dynamics of state competition, and the regimes continued reliance on centralized financial chokepoints. This thesis contends that the DPRK's adoption of VA-PF constitutes a typological merger of theft and laundering, effectively decoupling proliferation networks from the institutional banking system. In doing so, the DPRK exposes the limits and vulnerabilities of both the utility of conventional CPF frameworks and wider vulnerabilities in international financial governance. Furthermore, VA-PF not only erodes existing regulatory efficacy but also reshapes the political dynamics of enforcement, shielding, and challenging that define the broader counter-proliferation landscape.

The research is guided by three central questions:

1. How does the DPRK's use of VAs function within its PF architecture?
2. How do VA-PF mechanisms interact with cyber capabilities and sanctions evasion strategies?
3. How does the integration of VAs alter the global CPF regime?

1.3 Intersection with Theoretical Debates

This thesis engages two theoretical debates in different fields. The first concerns the transformative potential for financial governance of illicit finance in the digital age: are VAs merely a new phase in established laundering practices, or do they represent a transformative shift? This research posits the latter, arguing that VAs merge two previously distinct stages of illicit finance - the generation of illicit proceeds and the laundering of those proceeds - into a single, fluid process. This merger fundamentally alters the detection and disruption calculus for VA-PF and other VA-enabled financial crimes, collapsing traditional stage-based categories that have long informed enforcement strategies.

The second debate concerns financial power dynamics in global security regimes. To evaluate how VAs reconfigure this landscape, the thesis introduces an original analytical framework via the *Enforcer, Shield, and Challenger* (E/S/C) model. Building on concepts from literature on weaponized interdependence, balancing and strategic shielding, and revisionist states, the E/S/C framework reconceptualizes how power is distributed within the CPF regime.

Through this framework, the thesis demonstrates that VAs redistribute enforcement power and efficacy among these actors. By merging theft and laundering into a single typology of financial behaviour, VA-PF rebalances relationships among Enforcers, Shields, and Challengers. In the ensuing system, regulatory control is diffused and deterrence weakened.

1.4 Contributions of the Research

This thesis makes four distinct but interrelated contributions. Empirically, it provides the first consolidated observation of state-sponsored PF involving VAs, generating a novel and methodologically replicable dataset analyzed through mixed methods. The study also introduces the Virtual-Asset Proliferation Resourcing Model (VA-PRM), an adapted version of the Terrorist Resourcing Model (TRM), which classifies and tracks VA-PF flows. This model enables visualization of value transfers within illicit networks and identifies liquidity conversion or off-ramping - the point at which virtual value becomes real-world currency - as the primary chokepoint in VA-PF, offering a novel methodological contribution. By applying the E/S/C framework, the thesis demonstrates that VAs reshape the enforcement landscape of PF, redistributing power among Enforcers, Shields, and Challengers. This reveals critical flaws in multilateral CPF frameworks at the United Nations (UN) and Financial Action Task Force (FATF) level. It further establishes a key theoretical contribution: that VA-PF merges early stages of money laundering into a unified process, complicating established understandings of illicit finance. Finally, the findings illuminate the adaptive architecture of VA-PF and its implications for counter-proliferation strategies, providing policy-relevant insights for recalibrating international regulatory structures to maintain regime effectiveness amid global financial transformation.

1.5 Thesis Structure

The chapters that follow are organized to ensure a logical flow from conceptual framing to empirical analysis and policy implications. First, Chapter 2 consolidates existing research on

PF, VAs, and international financial governance. It situates the study within key theoretical debates on deterrence, financial power, and digital transformation and introduces the E/S/C Framework. Finally, it reviews the extant literature on North Korea's proliferation and cyber strategies. Chapter 3 outlines the methodological approach, dataset construction, and analytic tools underpinning the research. Chapter 4 presents the descriptive findings of the empirical analysis, integrating quantitative data with qualitative case studies. This is followed by Chapter 5, which interprets the findings in relation to traditional methods of PF and broader patterns in financial crime, emphasizing the shift from chokepoint to liquidity control. Chapter 6 then explores the theoretical, policy, and strategic significance of VA-PF, considering its implications for sanction design and global governance. Finally, Chapter 7 synthesizes the major findings, reaffirms the stakes of the research, and outlines a future research agenda focused on the evolving nexus of cyber capability, finance, and proliferation.

In summary, this thesis views the DPRK as more than an anomaly. It is an early indicator of systemic change. Through analysis of the world's most sanctioned and adaptive proliferator, the study reveals how digital finance erodes the enforcement logic of existing regimes and accelerates a broader shift toward decentralized, compliance-resistant systems. The implications extend beyond North Korea, signaling a fundamental test for the durability of global counter-proliferation governance in the digital age.

Chapter 2: Literature Review

2.1 Definitions, Ideologies & The Current Counter-Proliferation Framework

Understanding the financial dimensions of proliferation is a necessary foundation for this thesis. PF sits at the intersection of security, economics, and law. It refers to how funds are raised, moved, and obscured to sustain programs linked to weapons of mass destruction (WMDs) and chemical, biological, radiological, and nuclear weapons (CBRNs).[2] For the purposes of this thesis, these weapons are all referred to under the umbrella terminology of a "nuclear program" in relation to the DPRK. This section establishes the conceptual, ideological, and institutional context that global counter-proliferation frameworks operate within. In doing so, it synthesizes the extant literature to identify structural limits of this system and set the stage to study how North Korea uses unconventional means to push the limits.

2.1.1 Institutional Foundations: The UN, the FATF & Multilateral Sanctioning

The international community has developed overlapping counter-proliferation regimes led primarily by the United Nations Security Council (UNSC) and the Financial Action Task Force (FATF). Each plays a distinct but interdependent role in CPF: the UNSC establishes binding sanctions to prevent material and technology transfers through resolutions known as UNSCRs, and monitors member compliance, while the FATF sets financial standards meant to

[2] Financial Action Task Force, *Complex Proliferation Financing and Sanctions Evasion Schemes* (Paris: FATF, June 2025), 8, https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/Complex-PF-Sanctions-Evasions-Schemes.pdf.

give UNSCRs operational effect, using a listing process to reward or punish varying levels of compliance.[3]

The FATF's working definition of PF has become the accepted international benchmark and is adopted here:

> 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.[4]

While the FATF's definition is useful in formulating international guidance and forms a strong basis for academic understanding of PF, there is no universally accepted definition or

---

[3] Johnathan Brewer, "The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation," *Center for a New American Security*, January 2018, 13, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/CNAS%20ProliferationFinance.pdf; Togzhan Kassenova and Bryan R. Early, *Countering the Challenges of Proliferation Financing* (Washington, DC: Center for a New American Security, July 2023), 11, https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/China_Use.pdf.

[4] Financial Action Task Force, *Combating Proliferation Financing: A Status Report on Policy Development and Consulation,* (Paris: FATF/OECD, 2010), 5, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Status-report-proliferation-financing.pdf.coredownload.inline.pdf.

binding legal standard.[5] This undermines cohesive enforcement efforts and hampers data collection.

2.1.2 The FATF's Standard-Setting Role & Its Operational Boundaries

The FATF is the primary intergovernmental body tasked with developing global anti-money laundering (AML) and counter-terrorism financing (CTF) standards.[6] As a standard setting-body, the FATF holds no enforcement or independent regulatory power. Instead, it relies on the political will of member states to implement its recommendations.[7] The FATF also maintains a system of blacklists and greylists, which, in theory, exerts indirect pressure on listed jurisdictions to comply by limiting their opportunity to engage with other member states.[8] The DPRK has been blacklisted since 2013 for its proliferation activities.[9]

---

[5] Nikos Passas, "Financial Controls and Counter-Proliferation of Weapons of Mass Destruction," *Case Western Reserve Journal of International Law* 44, no. 3 (2012): 749, https://files01.core.ac.uk/download/pdf/214077663.pdf; FATF, *Complex Proliferation Financing*, 8; Kassenova & Early, *Countering the Challenges,* 12-13.

[6] Louis de Koker, "Supporting the Combatting of Financing of Weapons of Mass Destruction with AI Technologies," in *Proceedings of Artificial Intelligence Governance Ethics and Law (AIGEL)* (Barcelona, Spain, 2022), 10, https://ceur-ws.org/Vol-3531/LPaper_02.pdf.

[7] de Koker, "Supporting the Combatting," 10; Kassenova & Early, *Countering the Challenges,* 11.

[8] Louis de Koker, "The FATF'S Combating of Financing of Proliferation Standards: Private Sector Implementation Challenges," in *Financial Crime and the Law*, Ius Gentium: Comparative Perspectives on Law and Justice, vol. 115, ed. D. Goldbarscht and L. de Koker (Springer, 2024), 129; Kassenova & Early, *Countering the Challenges,* 11.

[9] Benjamin Habib, "The Enforcement Problem in Resolution 2094 and the United Nations Security Council Sanctions Regime: Sanctioning North Korea," *Australian Journal of International Affairs* 70, no. 1 (2016): 55, https://doi.org/10.1080/10357718.2015.1095278; Financial Action Task Force, *Guidance on the Effective Implementation of Targeted Financial Sanctions Related to Proliferation of Weapons of Mass Destruction* (Paris: FATF/OECD, 2007), 2, https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-UNSCRS-Prolif-WMD.pdf

In 2012, FATF expanded its mandate to include PF, integrating it into broader financial integrity standards.[10] This mandate expansion is narrowly defined and operationally limited in application to CPF. Only two of forty total FATF recommendations are applicable.[11] Recommendation 7 - the primary PF-related standard - recommends states implement targeted financial sanctions (TFS) pursuant to relevant UNSCRs.[12] Recommendation 2 suggests that states need to develop CPF policies.[13] Importantly, these standards only apply to UNSC TFS related to named entities and individuals in the DPRK and Iran specifically, and do not extend to general activities listed in UN sanctions.[14] Beyond these two measures, PF has received little independent attention within the FATF framework with two exceptions.

First, the 2018-2019 US presidency of the FATF resulted in enhanced risk assessment and mitigation requirements related to TFS.[15] Member states and regulated institutions are now expected to assess PF risks and strengthen controls when elevated. While this reflects some recognition of upstream financial vulnerabilities, it remains unclear how effectively these

---

[10] de Koker, "FATF'S Combating of Financing," 124; c.f. Financial Action Task Force, *The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (Paris: FATF/OECD, 2012), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.

[11] Brewer, "Financing of Nuclear and Other Weapons," 4.

[12] FATF, *The FATF Recommendations*, 13.

[13] FATF, *The FATF Recommendations*, 10-11.

[14] de Koker, "FATF'S Combating of Financing," 130; Brewer, "Financing of Nuclear and Other Weapons," 4; de Koker, "Supporting the Combatting," 10.

[15] de Koker, "Supporting the Combatting," 11; c.f. Financial Action Task Force, *Guidance: Countering Proliferation Financing*, February 2018, https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Countering-Proliferation-Financing.pdf.coredownload.pdf.

measures will be applied.[16] Second, a 2008 FATF work (updated by Brewer et al. in 2017) produced a list of PF indicators based on case studies from the DPRK, Iran, Syria, Pakistan, and India.[17] At the time, this study was comprehensive. Even with the update, however, the list omits emerging methods such as *virtual currencies* (VCs). It focuses on conventional trade and materials flows that are often not uniquely associated with PF.[18]

The FATF can be seen as more of a compliance enhancer than a proactive regulatory innovator. Its standards reinforce existing UN sanctions rather than creating new-risk-based mechanisms.[19] As a result, the limited range of FATF work on PF is largely concerned with the financial elements of material transfers, rather than financial flows themselves, and depends on state-level interpretation and implementation.

2.1.3 The UN Sanctions Regime & Its Structural Limits

The UN sanctioning process is the cornerstone of multilateral counter-proliferation efforts. It operates through targeted sanctions that are designed to apply maximum pressure to elites and goals of the target regime while minimizing collateral damage to the broader

---

[16] de Koker, "Supporting the Combatting," 11.

[17] c.f. Financial Action Task Force, *Typologies Report on Proliferation Financing*, June 18, 2008, 14, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf; Johnathan Brewer, "Study of Typologies of Financing of WMD Proliferation," King's College London, Center for Science and Security Studies, Project Alpha, October 13, 2017. study-of-typologies-of-financing-of-wmd-proliferation-2017.pdf

[18] Brewer, "Study of Typologies," 14, 27.

[19] Brewer, "Financing of Nuclear and Other Weapons," 13.

population of the state.[20] These sanctions are designed to be escalatory, but retractable should the targeted regime comply with the demands of the UN.[21] Only two general Security Council resolutions - UNSCR 1540 (2004) and UNSCR 2325 (2016) - explicitly address financial measures related to PF, despite counter-proliferation being one of five primary goals of UN sanctions.[22] Both of these resolutions are limited in scope, focusing on broad obligations rather than detailed enforcement mechanisms.

Relevant sanctions against the DPRK amount to:[23]

- An embargo on supply of WMD program-related items
- A complete arms embargo that exempts small arms and light weapons supplied only through controlled channels after notification to the UNSC

---

[20] Ruediger Frank, "The Political Economy of Sanctions Against North Korea," *Asian Perspective* 30, no. 3 (2006): 11, http://www.jstor.org/stable/42704552.; Thomas J. Biersteker et al., "UN Targeted Sanctions Datasets (1991–2013)," *Journal of Peace Research* 55, no. 3 (2018): 405, https://www.jstor.org/stable/48595892; Risa A. Brooks, "Sanctions and Regime Type: What Works, and When?" *Security Studies* 11, no. 4 (2002): 6, https://doi.org/10.1080/714005349.; Christian von Soest, "How Authoritarian Regimes Counter International Sanctions Pressure," *German Institute for Global and Area Studies*, no. 336 (September 2023): 9, https://pure.giga-hamburg.de/ws/files/49014203/GIGA_WP_336.pdf.

[21] Henning Jessen, "Multilateral and Unilateral Sanctions Compliance and Challenges," in *Peace, Justice, and Strong Institutions*, ed. W. Leal Filho et al. (Springer, 2021), 570.

[22] Bafode Drame, Lisa Toler, and Susan Pepper, *Forensic Analysis of Terrorist Counter-Financing to Combat Nuclear Proliferation*, no. BNL-111867-2016 (Brookhaven National Lab, 2016), 4; Brewer, "Financing of Nuclear and Other Weapons," 3, 12; Jessen, "Sanctions Compliance," 574; Fabio Cozzi, "Will Blockchain Technologies Strengthen or Undermine the Effectiveness of Global Trade Control Regulations and Financial Sanctions?" *Global Jurist* 20, no. 2 (2020), 4, https://doi.org/10.1515/gj-2019-0047.

[23] For a more comprehensive overview of sanctions against the DPRK, see Arms Control Association, "UN Security Council Resolutions on North Korea," accessed January 14, 2025, https://www.armscontrol.org/factsheets/un-security-council-resolutions-north-korea; for an in-depth review of landmark UNSCRs, see Tricia Fisher and Daniel White, "Implementing UN Sanctions on Democratic People's Republic of Korea," *Old Dominion University Model United Nations Council Issue Brief*, 2025, 5-7, https://www.odu.edu/sites/default/files/2025/documents/SC%20North%20Korea%20Sanctions.pdf.

- A ban on luxury goods
- Freezes of assets owned or controlled directly or indirectly by persons or entities designated as being related to the DPRK's WMD/CBRN programs
- Prevention of member states from providing financial services to persons, assets, or resources that may contribute to the DPRK's WMD/CBRN program
- No new loan commitments for grants, foreign assistance, or loans to the DPRK except for humanitarian, developmental, or denuclearization purposes
- A variety of individual travel bans and asset freezes

This sanctions regime is designed to target specific entities, strengthen financial measures with regard to banking and financial services to the DPRK, restrict proliferation-related trade, and target elites that give legitimacy to government leadership.[24]

The standard process of passing and maintaining a UNSCR and levying a sanction can be briefly summarized in three steps. First, a resolution is brought by one or more members of the Security Council (sponsors) to the others.[25] It must receive a majority vote and cannot pass, even with a majority, if vetoed by any of the permanent members (P5): Russia, the United States (US), the United Kingdom (UK), France, or China.[26] Then, once passed, all 193 member states of the UN are responsible for implementing, enforcing, and complying with the terms of the UNSCR in

[24] Habib, "The Enforcement Problem," 58.

[25] United Nations Security Council, *Provisional Rules of Procedure of the Security Council*, UN Doc. S/96/Rev.7 (1982).

[26] United Nations, *Charter of the United Nations*, 26 June 1945, 1 UNTS XVI, art. 27 para. 3.

question.[27] Finally, a Panel of Experts may be established to report to the UNSC on compliance by both the sanctioned regime and all UN member states with all sanctions levied against the regime in question.[28]

Three primary points of weakness exist in this process. First, the veto power of the P5 routinely limits the adoption or expansion of sanctions where political interests or ideology conflict with implementation and enforcement requirements.[29] This has historically been the case when it comes to Russia (which has a history of exercising veto power) and China (which has a history of abstaining, often in implied support of Russian vetoes) in relation to sanctions against the DPRK.[30] Second, while sanctions are binding, the nature and extent of their implementation and enforcement depends on the national capacity and political will of member states, which varies across both time and jurisdiction, depending on a multitude of factors.[31] Divergent domestic priorities create an uneven patchwork of enforcement with regulatory gaps that proliferators can exploit. The third factor relates to the first; the continued mandate of a Panel of

---

[27] UN Charter, art. 25; art. 41.

[28] UN Charter, art. 29.

[29] Habib, 59.

[30] Ticha Ungboriboonpisal, "Efficacy of Economic Sanctions in the Face of Cryptocurrency," *New York University Journal of International Law and Politics* 55 (2022): 232, https://www.nyujilp.org/wp-content/uploads/2023/03/Comment4.pdf; Adérito Vincente, "United Nations Security Council Reform: The Question of the Veto Power," *United Nations Institute for Training and Research Multilateral Diplomacy Summer School–Student Papers*, 2013, 19-23, https://doi.org/10.13140/RG.2.2.26138.93121.; Federica D'Alessandra, "Conceptualizing Great Power Perpetrators," *Genocide Studies and Prevention: An International Journal* 18, no. 1 (2024): 153-154, https://ora.ox.ac.uk/objects/uuid:800e5170-39cc-485d-9985-1b1baf5b6024/files/rmp48sf11g; E. G. Ivanov and A. V. Solovyov, "The Erosion of the UN Security Council Sanctions Regime Against the DPRK," *Journal of International Analytics* 14, no. 1 (2023): 84, https://doi.org/10.46272/2587-814X-2023-14-1-67-81.

[31] de Koker, "Supporting the Combatting," 11; Jessen, "Sanctions Compliance," 578.

Experts is also subject to P5 veto power. At regular intervals, the UNSC votes on whether and how the work of a Panel of Experts will continue. At these points, members of P5 are able to invoke veto power to end the mandate.

The absence of the unified monitoring mechanism provided by a Panel of Experts can generate a compliance gap, minimizing attribution capability and identification of emerging trends, mechanisms, and actors in proliferation networks. In 2024, Russia exercised its veto power to end the Panel of Experts on the DPRK, which was responsible for linking North Korean cyber thefts to its nuclear and ballistic program developments.[32]

2.1.4 Summary: The Limits of Multilateral Sanctions & Standards

Together, the UN and the FATF form the backbone of the global CPF regime. Yet their mutual reliance on state-level enforcement, combined with a primary focus on financing related to material control – tracking production, trade, and institutional financial flows – has produced a system that is inherently oriented towards monitoring regulated and centralized channels. To fully understand the constraints created by this orientation, it is necessary to examine the specific modalities through which PF is carried out. The following section traces the traditional financing and laundering cycle before turning to the emerging literature on VAs and illicit finance to assess how scholarship currently understands their impact.

[32] Fisher & White, "Implementing UN Sanctions," 1; United Nations, "Security Council Fails to Extend Mandate for Expert Panel Assisting Sanctions Committee on Democratic People's Republic of Korea," press release, March 28, 2024, https://press.un.org/en/2024/sc15648.doc.htm.

2.2 Proliferation Financing: Traditional Modalities & the New Digital Frontier

This thesis contends that the movement of PF activities into decentralized digital systems has altered both the structure and strategic logic of illicit finance. To understand these changes, the thesis shall first establish how proliferators have historically raised, laundered, and deployed funds, and then evaluate current debates around the disruptive potential of VAs. This section examines the conventional three-stage PF cycle and core elements of laundering-based financial crime before turning to the emergence of VA ecosystems and their relationship to extant regulatory frameworks.

2.2.1 Understanding the Relationship of Proliferation Financing & Money Laundering

The literature consistently emphasizes that PF is a core enabling mechanism for proliferation; finances are often the most decisive limiting factor in proliferation networks.[33] PF is typically conceptualized as a three-stage cycle: fundraising, disguise & laundering, and procurement. First, funds are generated via domestic revenues or illicit streams (fundraising). These funds must then be concealed and integrated into the international financial system (disguise & laundering). Finally, these funds are used to acquire sensitive goods, materials, or technologies (procurement).[34] Historically, the DPRK has navigated this cycle through a variety of mechanisms, including exploiting state-owned enterprises in permissive jurisdictions, falsifying invoices and end-user certifications, false-flagged shipping, and trafficking via

[33] Drame, Toler, & Pepper, *Forensic Analysis,* 4.

[34] Brewer, "Financing of Nuclear and Other Weapons," 2.

diplomatic networks, all aimed at moving bulk cash value and illicit goods across borders to circumvent sanctions.[35]

This PF cycle mirrors the classic tripartite money-laundering (ML) sequence that underpins much of financial crime research: placement, layering, and integration.[36] A more expansive five stage framework conceptualized by Broome (2005), which adds generation and consolidation as initial stages, is also widely employed in ML analyses.[37] In either model, a predicate offense must exist for the ML sequence to initiate.[38]

At higher levels, recommendations from bodies such as the FATF highlight differences in ML and PF. While ML involves a wide range of actor types,[39] PF is predominantly state-driven (although limited evidence suggests that some non-state affiliated actors such as terrorist organizations have attempted to engage in proliferation-related activities).[40] As such, specific

---

[35] Drame, Toler, & Pepper, *Forensic Analysis,* 5; Habib, "The Enforcement Problem," 55; FATF, *Typologies Report*, 9-11.

[36] Mohd Yazid bin Zul Kelpi and Maruf Adeniyi Nasir, "Money Laundering: Analysis on the Placement Methods," *International Journal of Business, Economics and Law* 11, no. 5 (2016): 33-34, http://irep.iium.edu.my/65817/1/Analysis%20on%20placement%20methods.pdf; Fabian Maximilian Teichmann, "Recent Trends in Money Laundering and Terrorism Financing," *Journal of Financial Regulation and Compliance* 27, no. 1 (2019): 3, https://doi.org/10.1108/JFRC-03-2018-0042; Paul Gilmour et al., *Reexamining the PLI Model of Money Laundering* (The Institute of Money Laundering Prevention Officers, 2025),13, https://brianforensics.com/wp-content/uploads/2024/11/Institute-Report-Reexamining-the-PLI-Model-of-Money-Laundering.pdf.

[37] Gilmour et al., *Reexamining the PLI Model,* 20.

[38] Teichmann, "Recent Trends," 3; Gilmour et al., *Reexamining the PLI Model*, 9-10; Olha Maletova et al., "Predicate Offense in Money Laundering Cycle," *Cuestiones Políticas* 47, no. 71 (2023): 26-27, https://doi.org/10.46398/cuestpol.4179.01.

[39] Teichmann, "Recent Trends," 3.

[40] FATF, *Complex Proliferation Financing*, 11; FATF, *Typologies Report*, 2.

ML guidance often focuses on risk-based mechanisms, while rules-based approaches are recommended for PF.[41] Despite these recommendations, the minimal and somewhat vague guidance on CPF and slow adoption processes at the national level has resulted in the grafting of many CPF regulations onto existing risk-based AML frameworks.[42] However, these frameworks are not oriented to catch PF. Unlike in ML, which intends to conceal the origin and source of funds, PF transactions are primarily concerned with obscuring the end-use and final destination of funds and goods. Ergo, the efficacy of AML tools when applied to PF is limited.[43]

2.2.2 The Central Debate: Will Virtual Assets be Adopted by Proliferators?

Scholars have generally agreed that VAs have criminogenic attributes that make them attractive for purposes of financial crime. This agreement is grounded in an increasing recognition in international illicit political economics (IIPE) literature that cyber-enabled methods offer a key comparative advantage to criminals: reducing exposure to regulated financial systems, and consequently, to enforcement mechanisms.[44]

---

[41] Brewer, "Financing of Nuclear and Other Weapons," 4.

[42] Ougrham-Gormley, "Banking on Nonproliferation," 245.

[43] Ougrham-Gormley, 242, 245, 248.

[44] See, for example, Hamilton & Leuprecht 2024; Ariel Burgess, Rhianna Hamilton, and Christian Leuprecht, "Terror on the Blockchain: The Emergent Crypto-Crime-Terror Nexus," in *Financial Crime, Law, and Governance*, Ius Gentium: Comparative Perspectives on Law and Justice, vol. 116 (Springer, 2024), https://doi.org/10.1007/978-3-031-59547-9_9; Emma K. Macfarlane, "Strengthening Sanctions: Solutions to Curtail the Evasion of Sanctions Through the Use of Cryptocurrency," *Michigan Journal of International Law* 42, no. 1 (2021), https://doi.org/10.36642/mjil.42.1.strengthening; Kole Zellers, "Hacked! North Korea's Billion-Dollar Crypto Heisting Scheme," *Penn State Journal of Law & International Affairs* 12, no. 1 (2024), https://insight.dickinsonlaw.psu.edu/cgi/viewcontent.cgi?article=1369&context=jlia; United States Department of

However, whether this is true of PF is debatable. Scholars on one side argue that proliferators have little incentive to adopt VAs because existing illicit finance infrastructures are already effective at containing such a high-risk form of criminality. The risks of integrating new technology and difficulties associated with functionally employing it may offset potential gains.[45] By contrast, a smaller subset of scholarship argues that the attributes of VAs - borderless transfer, pseudonymity, and rapid value movement - shift the reward-risk calculus in favour of their adoption in PF networks.[46] Extant scholarship on both sides consistently frames VAs as tools that enhance or refine existing PF processes without considering their potential to alter the processes themselves.

The final hurdle in resolving this debate is lack of empirical evidence. Failure to resolve this obstacle has created a paradox: the lack of evidence simultaneously supports the prevailing view that VAs have not been and are unlikely to be widely adopted by proliferators, while undermining its certainty. Without systematic empirical study, such a conclusion is speculative. Absence of evidence is not evidence of absence, and the true scope and operational significance of VA-PF therefore remains uncertain.

2.2.3 Regulatory Responses to VAs: Revisiting the Limits of Multilateral Frameworks

the Treasury, *2024 National Proliferation Financing Risk Assessment,* (Washington, DC: 2024), https://home.treasury.gov/system/files/136/2024-National-Proliferation-Financing-Risk-Assessment.pdf.

[45] Brewer, "Financing of Nuclear and Other Weapons," 2.

[46] Summer Wright, "The Evolution of Sanctions Evasion: How Cryptocurrency is the New Game in Evading Sanction and How to Stop It," *International Journal of Law, Ethics, and Technology* 1 (2023): 116-19, https://doi.org/10.55574/vohs5203.

In response to the rising popularity of VAs, some regulatory guidance has been introduced. The primary guiding force is FATF Recommendation 15 (2019), which extends oversight to VAs and Virtual Asset Service Providers (VASPs).[47] This oversight is not specific to the CPF framework; instead, requirements for licensing and due diligence aim to integrate VA regulation into existing AML regimes.[48]

In practice, these measures reflect the same structural constraints that haunt the CPF regime: they are largely reactive, assume the presence of cooperative intermediaries who will abide by regulatory and licensing requirements, and rely on national-level implementation and enforcement.[49] Notably, the FATF's VA guidance is inherently limited by the scope of sanctions-related recommendations, as no UNSCRs thus far apply to cryptocurrencies.[50] Perhaps the most pressing limitation for this thesis is the reliance on state-led regulation. Differences in capacity, interpretation of norms, priorities, and incentive to comply create regulatory arbitrage: loopholes in both CPF and VA regulation frameworks for proliferators to exploit.[51] Understanding the dynamics that lead to regulatory arbitrage requires a theoretical lens that can account for both the institutional architecture of the CPF system and the strategic behaviour of

---

[47] c.f., Financial Action Task Force, *Horizontal Review of FATF Standards on Virtual Assets and Virtual Asset Service Providers* (Paris: FATF/OECD, 2024).

[48] Burgess, Hamilton, & Leuprecht, "Terror on the Blockchain," 213.

[49] United States Department of the Treasury, *2024 NPFRA,* 10.

[50] Ungboriboonpisal, "Efficacy of Economic Sanctions," 229.

[51] Ungboriboonpisal, 230; Macfarlane, "Strengthening Sanctions," 204; Zellers, "Hacked!," 275-276; Christoph Wronka, "Digital Currencies and Economic Sanctions: The Increasing Risk of Sanction Evasion," *Journal of Financial Crime* 29, no. 4 (2022): 1274, https://doi.org/10.1108/JFC-07-2021-0158.

states in relation to it. The following section develops an original framework that meets this need.

2.3 The E/S/C Framework & Shifting Power Dynamics in Non-Conventional PF

Limitations of the international CPF regime are not merely structural; they are fundamentally political and strategic, driven by divergent national interests and uneven distributions of power that shape state incentives to comply, resist selectively, or actively undermine regulatory mechanisms. Existing scholarship offers valuable insight into these dynamics, yet it often treats actors as either compliant or non-compliant, overlooking the spectrum of strategic interaction that shapes the efficacy of CPF. To address this gap, this section introduces the Enforcer, Shield, Challenger (E/S/C) framework as an original synthesis of existing theoretical strands concerned with power, coercion, and institutional constraint.

The E/S/C framework provides a lens to understand how different states work to uphold, exploit, or subvert international financial systems. Rather than assuming static roles, it emphasizes how actors reposition themselves in response to shifting geopolitical conditions and national priorities. These categories are viewed as existing on a shifting spectrum of behaviour within the international financial system. While this model can be applied broadly, it is particularly useful in accounting for strategic behaviour in cases where conventional control models are limited or contested, such as in the case of PF by the DPRK.

2.3.1 The Enforcer

The concept of a "system-anchoring enforcer," or a jurisdiction capable of translating international norms into enforceable compliance, is rooted in literature on weaponized interdependence, Great Power competition, and the Status Quo state. This literature, particularly that of weaponized interdependence, emphasizes that control over centralized financial infrastructure and cross-border clearing systems creates asymmetries of power. States with jurisdictional reach into these networks hold coercive leverage over actors that depend on them and can use that leverage to maintain their favourable positions in the international order.[52] This thesis refers to those with this leverage as *Enforcers:* those who not only comply with the CPF regime, but actively use their domestic legal, financial, and regulatory capacities to maximize its enforcement potential.

The United States is the paradigmatic example. Its dominant position within global finance – notably the primacy of the US dollar (USD) as reserve currency, regulatory influence over the SWIFT network, and heavy saturation of primary chokepoints in global financial flows – confers a unique degree of control.[53] Consequently, US financial regulators (i.e., the Department of the Treasury's Office of Foreign Assets Control (OFAC) and the Financial Crimes Enforcement Network (FinCEN)) function as de facto gatekeepers to the global financial

---

[52] See, for example, Henry Farrell and Abraham L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion," *International Security* 44, no. 1 (2019), https://doi.org/10.1162/isec_a_00351.; Barry Buzan, *People, States and Fear: The National Security Problem in International Relations* (Brighton: Wheatsheaf Books, 1983); William T.R. Fox, *The Super-Powers: The United States, Britain, and the Soviet Union—Their Responsibility for Peace* (New York: Harcourt, Brace and Company, 1944).

[53] Brewer, "Financing of Nuclear and Other Weapons," 2; Cozzi, "Blockchain Technologies," 10; United States Department of Treasury, *2024 NPFRA*, 8; Farrell and Newman, "Weaponized Interdependence," 52.

system.[54] This is reflected by international assessments: for example, the FATF has identified the US as the only jurisdiction with explicit requirements for financial institutions to detect and interrupt PF.[55]

The US approach to CPF illustrates how the Enforcer operates. Measures enacted under authorities such as the *North Korea Sanctions and Policy Enhancement Act* (2016) and executive powers under the *International Emergency Economic Powers Act* (IEEPA) authorize asset freezes, service prohibitions, technology transfer restrictions, and secondary sanctions against third-party facilitators.[56] The 2016 designation of North Korea as a "primary money laundering concern" under section 311 of the *USA PATRIOT Act* significantly curtailed the DPRK's access to US dollar-clearing systems.[57] In practice, this pressured international financial institutions to exclude DPRK-linked entities from global payment networks to avoid counterparty risk.[58] While the tempo and diplomatic posture of enforcement has varied by US presidential administration,

---

[54] Cozzi, "Blockchain Technologies," 6; Farrell & Newman, "Weaponized Interdependence," 52.

[55] Brewer, "Financing of Nuclear and Other Weapons," 14.

[56] Katherine Kirkpatrick et al., "Virtual Currency in Sanctioned Jurisdictions: Stepping Outside of SWIFT," *Journal of Investment Compliance* 20, no. 2 (2019): 41, https://doi.org/10.1108/JOIC-04-2019-0019.; c.f. Office of Foreign Assets Control, "North Korea Sanctions Program," United States Department of the Treasury, November 2, 2016, https://ofac.treasury.gov/media/9221/download?inline.; United States Government Publishing Office, "North Korea Sanctions and Policy Enhancement Act of 2016," https://www.govinfo.gov/content/pkg/COMPS-11985/pdf/COMPS-11985.pdf.

[57] Bruce E. Bechtol Jr., "North Korean Illicit Activities and Sanctions: A National Security Dilemma," *Cornell International Law Journal* 51, no. 1 (2018): 79-80, https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=1913&context=cilj; Victor Cha and Lisa Collins, "Treasury Department Designates North Korea Under Section 311," *Center for Strategic and International Studies*, June 1, 2016, https://www.csis.org/analysis/treasury-department-designates-north-korea-under-section-311.

[58] Bechtol Jr., "North Korean Illicit Activities," 87.

the underlying logic of systematic CPF enforcement has remained consistent since its consolidation during the Obama-era.[59]

In sum, Enforcers are state actors with the capacity to convert their structural financial privilege into operationalized compliance pressure. Maintaining international norms benefits the Enforcer: they maintain their privileges, which in turn provide leverage over other states in the international community. Such leverage can be amplified or diminished by actions of other state actors.

2.3.2 The Shield

While an Enforcer seeks to maximize the reach and impact of CPF frameworks, other state actors aim to moderate or bypass these efforts, which creates regulatory asymmetries that proliferators can exploit. This thesis defines these actors as *Shields***.** This archetype is based on international relations literature on balancing and shielding.[60]

Shields work to balance formal obligations to the international community with the pursuit of their own objectives, which may be subject to limitations created by those formal obligations. Like Enforcers, they look after their own interests in the international system.

---

[59] Bechtol Jr., 77; Vincent Koen and Jinwoan Beom, "North Korea: The Last Transition Economy?," *Organization for Economic Co-operation and Development Working Paper No. 1607*, 2020, 19, https://one.oecd.org/document/ECO/WKP(2020)15/en/pdf.

[60] See, for example, Stephen M. Walt, *The Origins of Alliances* (Cornell University Press, 1987); Kenneth N. Waltz, *Theory of International Politics* (Addison-Wesley, 1979); Cheng-Chwee Kuik, "Getting Hedging Right: A Small-State Perspective," *China International Strategy Review* 3, no. 2 (2021): 301, https://doi.org/10.1007/s42533-021-00089-5.

However, unlike Enforcers, they do not inherently asymmetrically benefit or derive power from their position within the current global financial system, and may seek to change certain conditions of it without necessarily overturning it entirely or directly confronting Enforcers. Their actions are covert; implementing the letter of regulations but not their full spirit or exercising soft power influence to mitigate regulatory pressure indirectly.[61]

In the case of the DPRK, China exemplifies the Shield.[62] Since 2000, it has been North Korea's largest trading partner, particularly in the energy sector, supplying an estimated 90% of North Korean oil imports.[63] Stable relations with the DPRK support multiple Chinese policy objectives. North Korea acts as a geopolitical buffer along China's border against US and South Korean military presence, and as an ideological buffer that limits Western influence in the region.[64] Although China formally participates in UN and FATF frameworks, it has historically

[61] In relation to this behaviour and the China/DPRK relationship, see D'Alessandra, "Great Power Perpetrators," 170; Ivanov and Solovyov, "Erosion of the UN Security Council," 92, 96; Peter Harrell, Elizabeth Rosenberg, and Edoardo Saravalle, *China's Use of Coercive Economic Measures* (Washington, DC: Center for a New American Security, June 2018), 10, 48, https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/China_Use.pdf.; Frida Lampinen, "Russia-DPRK Relations: Implications for the UNSC's Mandate," *Institute for Security and Development Policy Issue Brief*, February 9, 2024, 4, https://www.isdp.eu/wp-content/uploads/2024/02/Brief-Frida-Feb-9-2024-final-.pdf.; Stephen Blank, "The North Korean Factor in the Sino-Russian Alliance," *Korea Economic Institute of America*, July 29, 2019, 38, https://keia.org/wp-content/uploads/2020/05/kei_jointus-korea_2019_1.2.pdf.; Christopher Twomey, "Explaining Chinese Foreign Policy toward North Korea: Navigating between the Scylla and Charybdis of Proliferation and Instability," *Journal of Contemporary China* 17, no. 56 (2008), https://doi.org/10.1080/10670560802000167.

[62] c.f. the concept of soft revisionism in relation to China from Kai He et al., "Rethinking Revisionism in World Politics," *The Chinese Journal of International Politics* 14, no. 2 (2021), https://doi.org/10.1093/cjip/poab004.

[63] Bechtol Jr., "North Korean Illicit Activities," 89; Koen and Beom, "The Last Transition Economy?," 24-25.

[64] Bechtol Jr., 89; Ivanov and Solvyov, "Erosion of the UN Security Council," 90; Blank, "The North Korean Factor," 36; Giwoong Jung et al., "Why Russia and China Advocate Korean Peace-Unification Public

implemented these measures selectively or kept enforcement passive.[65] Consequently, China's economic and financial networks serve as principal conduits for the DPRK's illicit revenue: sanctioned entities frequently transfer funds through Chinese intermediaries, shell companies, and small regional banks.[66] Combined, this relationship manifests an asymmetric system of dependence in which China exerts strategic leverage over the DPRK.[67]

Shields can also exercise diplomatic influence to reaffirm economic or political shielding efforts. China, for example, has positioned itself as a mediator between North Korea, the US, and the broader international system, as its centrality in negotiations such as the Six-Party Talks demonstrates.[68] This duality illustrates the Shield's goal: by moderating international pressure on proliferators, Shields can simultaneously protect their strategic interests, retain influence over targeted actors, and gatekeep progress on international goals with relative impunity by maintaining plausible deniability.

Diplomacy?," *Journal of International Relations* 26, no. 2 (2023): 245, https://www.kci.go.kr/kciportal/landing/article.kci?arti_id=ART002964296.

[65] Bechtol Jr., "North Korean Illicit Activities," 91; Brewer, "Financing of Nuclear and Other Weapons," 12-13; Ungboriboonpisal, "Efficacy of Economic Sanctions," 232; Kassenova & Early, *Countering the Challenges,* 20; D'Alessandra, "Great Power Perpetrators," 186-169.

[66] Bechtol Jr., "North Korean Illicit Activities," 63, 66.

[67] Harrell, Rosenberg, and Saravalle, *China's Use of Coercive Economic Measures*, 10; Twomey, "Chinese Foreign Policy,"; Ivanov & Solvyov, "Erosion of the UN Security Council," 92; Blank, "The North Korean Factor," 46.

[68] William J. Perry, "Proliferation on the Peninsula: Five North Korean Nuclear Crises," *The Annals of the American Academy of Political and Social Science* 607 (2006): 84; Nuclear Threat Initiative, "Six-Party Talks," Inventory of International Nonproliferation Organizations and Regimes, Center for Nonproliferation Studies, May 24, 2012, https://media.nti.org/pdfs/6ptalks_1.pdf.; Twomey, "Chinese Foreign Policy," 411-413.

2.3.3 The Challenger

Grounded in literature on rogue, revisionist states, and non-compliant states, as well as Power Transition Theory,[69] *Challengers* are defined as states that may actively and intentionally undermine CPF regimes. They engage in these efforts as part of broader activities aimed at revising, weakening, or replacing the current international order.[70] Unlike Shields, Challengers are openly non-compliant and directly counter Enforcers through mechanisms such as political obstruction and direct facilitation. Russia and the DPRK itself are primary examples of this archetype.

Historically, Russia has sometimes functioned as a Shield, aligning publicly with Enforcers on denuclearization and CPF while selectively permitting sanctions to be breached.[71] Since 2017, however, Russia has increasingly operated as a Challenger in relation to the DPRK, using its P5 veto powers to block UN measures aimed at strengthening and expanding sanctions

[69] While Power Transition Theory positions Challengers as those with asymmetric or growing material wealth (GDP, military size), this thesis believes the concept of a Challenger is applicable and extendable to the financial and cyber domains. Rather than the transition culminating in conventional conflict, the transitions in this case are envisioned as culminating in wars of attrition - for example, over financial architecture - using asymmetric tactics. c.f. A. F. K. Organski, *World Politics* (Alfred A. Knopf, 1964), esp. Part Two.

[70] See, for example, Randall L. Schweller, "Bandwagoning for Profit: Bringing the Revisionist State Back In," *International Security* 19, no. 1 (1994): esp. 80, https://doi.org/10.2307/2539149.

[71] Lampinen, "Russia-DPRK Relations," 2-3; Fisher and White, "Implementing UN Sanctions," 3; Ivanov & Solvyov, "Erosion of the UN Security Council," 93.

against North Korea.[72] In 2024, Russia escalated, effectively single-handedly terminating the UN Panel of Experts on the DPRK by vetoing the continuation of its mandate.[73]

The DPRK is also a Challenger by virtue of its deliberate proliferation behaviour,. In seeking to revise or extricate itself from the global norms restricting nuclear proliferation, the DPRK directly contravenes CPF frameworks and associated sanctions regimes, propped up by the activities of other Challengers such as Russia.[74]

Both state activities erode structural authority of the bodies and frameworks that underpin the current international order to advance their own interests. This erosion generates a feedback loop within the CPF system: measures imposed by Enforcers to deter or contain behaviour by Challengers may provoke further non-compliant or evasive action by reinforcing their motivation to resist or challenge the international order. Under the E/S/C framework, this system of mutually reinforcing polarity is referred to as the *Resistance-Amplification Cycle*.

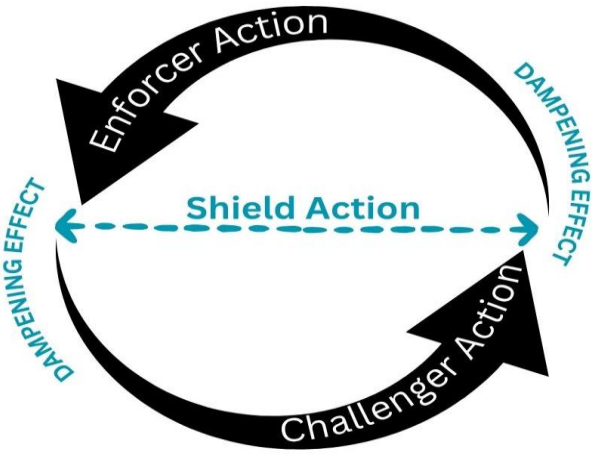
---

[72] Ungboriboonpisal, "Efficacy of Economic Sanctions," 232; Kassenova & Early, *Countering the Challenges,* 20; Lampinen, "Russia-DPRK Relations," 4; D'Alessandra, "Great Power Perpetrators," 153.

[73] de Koker, "Private Sector Implementation Challenges," 131; Fisher and White, "Implementing UN Sanctions," 1; United Nations, "Security Council Fails to Extend Mandate."

[74] Blank, "The North Korea Factor," 38; Andrea Berger, "A House Without Foundations: The North Korea Sanctions Regime and Its Implementation," *Royal United Services Institute Whitehall Report* 3, no. 17 (June 2017): 14, https://static.rusi.org/201706_whr_a_house_without_foundations_web.pdf

Figure 1: The Resistance-Amplification Cycle



2.3.4 The E/S/C Framework: Culminating Insights & Unresolved Questions

The E/S/C framework is derived from the strategic logic that underpins contemporary work on proliferation, sanctions, financial statecraft, and the political economy of global finance. The E/S/C framework reveals shared structural assumptions that can be conceptualized in terms of three archetypes - Enforcers, Shields, and Challengers - whose strategic behaviour is shaped by, and act upon, the international financial system. Table 1 summarizes these roles, their sources of power, primary actions, and underlying rationale.

Table 1: Summary of Archetypes in the E/S/C Framework

Archetype	Description	Relevant Example	Primary Action	Theoretical Grounding	Representative Quote
Enforcer	Actively use their domestic legal, financial, and regulatory capacities to maximize CPF enforcement potential	USA	Sanctions	Weaponized interdependence, Great Power competition, Status Quo states	"Specifically, states with political authority over the central nodes...through which money, goods, and information travel are uniquely positioned to impose costs on others." [75]
Shield	Aims to balance formal obligations to the international community with the pursuit of their own objectives	China	Selective compliance	Strategic non-enforcement, balancing, shielding	"Actors may perceive the structure that constrains them and understand how it serves to reward some and penalize others...to say that the structure selects means simply that those who conform to accepted and successful practices more often rise to the top and are likelier to stay there."[76]
Challenger	Actively and intentionally undermine CPF regimes as part of broader activities aimed at revising, weakening, or replacing the current international order	Russia; the DPRK	Direct circumvention/ intentional obstruction	Revisionist statecraft	"But staying in place is not the primary goal of revisionist states. They want to increase, not just preserve, their core values and improve their position in the system. These goals cannot be achieved by simply ensuring that everyone else does not gain relative to them. They must gain relative to others."[77]

[75] Farrell & Newman, "Weaponized Interdependence," 45.

[76] Waltz, *Theory of International Politics,* 92.

[77] Schweller, "Bandwagoning for Profit," 87.

When these relational logics become explicit, a shared structural assumption becomes visible across both academic literature and CPF regulatory practice: states and proliferators are theorized as acting within a stable, bounded financial system whose architecture of monitoring, intermediation, and enforcement remains fundamentally intact. Even when discussing subversion or adaptation, the system itself is treated as the fixed stage upon which strategic behaviour unfolds.

By mapping these dynamics relationally, the E/S/C framework makes this implicit assumption apparent. All three archetypes presuppose the continued centrality of legacy financial infrastructure and their chokepoint-dependent mechanisms of control. The framework also makes visible the dynamic interplay between these roles. The Resistance–Amplification Cycle illustrates how interactions among the three archetypes are mutually reinforcing: Enforcers provoke adaptive responses from Challengers,[78] which in turn shape subsequent enforcement strategies, while Shields mediate and modulate the effects of both, dampen escalation, and stabilize system-wide outcomes (Figure 1). These interactions stabilize power relations when conflict occurs, ensuring the CPF system remains intact even when stressed. In this sense, the framework does more than classify actor roles; it clarifies the conceptual boundaries that

[78] Theoretical grounding for this form of state interaction can be found in Schweller, "Bandwagoning for Profit," esp. 105.

structure the PF literature. It shows not only what the literature explains, but also what it is not built to see.

This systemic tension gives rise to several critical research gaps. First, it highlights the limitations of traditional theories of financial statecraft, which assume that global value transfers must pass through centralized chokepoints. Consequently, current scholarship lacks the conceptual tools to analyze decentralized value transfer infrastructure that operates outside chokepoint-based control. This is compounded by the way CPF processes treat shielding and challenging as variations of the same form of resistance, despite the literature recognizing that they arise from distinct strategic logics. This lack of distinction obscures how financial resistance to CPF may be structured and coordinated differently by different actors. Finally, these gaps are underpinned by a static system assumption in most CPF scholarship, which models adaptation as iterative (sanction leads to evasion leads to countermeasure). By assuming that proliferators continue to operate within the same financial order even when evading enforcement, the CPF challenge is framed as an issue of capacity and enforcement. There is little consideration as to whether the underlying structure of control may itself be deteriorating.

Taken together, these gaps indicate that both the literature and the CPF regime share the same epistemological constraint: they are designed to interpret change *within* the global financial system, and by extension the CPF system, and not *changes to* those systems. This is precisely the challenge posed by VAs. VA-PF does not merely introduce new methods of evading sanctions inside the existing architecture of financial control; it creates the possibility of moving value outside that architecture altogether. It transforms a fixed stage into a dynamic one, retaining the

interested actors without clarifying the roles or relationships among them under these changed conditions.

Thus, the E/S/C framework is not only a typology. Its central contribution is that it repositions the analytical vantage point of PF research. By modeling the relational distribution of enforcement capacity, shielding leverage, and system-disruptive activity, the framework shifts analysis away from discrete enforcement outcomes and toward the structural configuration of financial power itself. This allows scholars to examine transformations to the architecture of financial control rather than just tactical adaptations occurring within it.

From this perspective, the limitations identified above cannot be resolved by more data, improved monitoring, or enhanced regulatory coordination. They are products of assumption internal to the system: the belief that proliferators, enforcers, and intermediaries will continue to rely on a financial environment where chokepoint control remains structurally determinate. The rise of decentralized, cyber-enabled value transfer challenges this assumption directly, introducing pathways of value movement that may no longer depend on the system by which enforcement has historically operated.

Accordingly, this thesis does not simply assess whether proliferators are adopting VAs or whether such adoption is effective. It uses empirical evidence to show how VA-PF reconfigures the relational dynamics of financial power composition. It demonstrates that VAs may represent a transformation in the architecture of financial control, altering the conditions of CPF and by extension actor behaviours and possible outcomes of interactions within the CPF framework, rather than a tactical adaptation occurring within it.

2.4 The DPRK as a Critical Case Study[79]

Having established that existing proliferation finance scholarship and enforcement practice are structured according to a system-internal logic, the next step is to examine the practical limits of this logic. The DPRK provides the most analytically valuable case for examining these limits. No other state has faced such sustained financial isolation while simultaneously maintaining, expanding, and modernizing a strategic weapons program.[80] In this respect, the DPRK is not simply another case of PF; it is a stress test of the durability and adaptability of the global financial control regime itself.

The DPRK case provides an opportunity to examine how long-standing enforcement and policy frameworks function under conditions of maximum constraint. It also illustrates both the technical feasibility and strategic logic of VA-PF while offering an analytical window into PF practices that may already be emerging elsewhere below detectable thresholds.

2.4.1 Ideology, Governance, & State-Based Criminality: Complicating Deterrence

The DPRK's strategic posture is shaped by two primary doctrines: j*uche* and s*ongun*. These doctrines collectively justify optimized allocation of resources to the military and nuclear

[79] The DPRK represents both a least-likely (for nuclear program survival under complete economic isolation) and most-likely (for VA-PF) critical case. c.f. Xhimi Hysa, "Critical Case," in *The SAGE Encyclopedia of Research Design*, 2nd ed., ed. Bruce B. Frey (SAGE Publications, 2022), https://doi.org/10.4135/9781071812082.n130.

[80] Wright, "The Evolution of Sanctions Evasion," 16; Anderson, "North Korea's Nuclear Ambitions," 624; Ivanov & Solvyov, "Erosion of the UN Security Council," 89.

sectors, cementing regime survival and nuclear deterrence as foundational imperatives of the state.

Juche, or "self-reliance," serves dual ideological and political functions for the North Korean state. It highlights regime autonomy, centralization of power, and control over political, military, and economic resources.[81] Externally, *juche* is grounded in realist assumptions of international relations: the state exists in an anarchic system where survival depends on independent capability and credible deterrence. Under such an interpretation, nuclear weapons cease to be mere strategic assets and instead serve as a guarantee against external coercion.[82] The long-term presence of US military forces on the peninsula, combined with decades of diplomatic tension and sanctioning, continually reinforces this existential threat perception. This incentivizes the accumulation of nuclear capability as the ultimate mechanism of survival for the Kim dynasty.[83]

Songun, or "military-first," is a complementary policy that asserts the primacy of the armed forces in governance, resource allocation, and ideological direction.[84] The synthesis of

---

[81] See Grace Lee, "The Political Philosophy of Juche," *Stanford Journal of East Asian Affairs* 3, no. 1 (2003), https://time.com/wp-content/uploads/2014/12/korea1.pdf.

[82] Drame, Toler, & Pepper, *Forensic Analysis,* 3; Anderson, "North Korea's Nuclear Ambitions," 622, 631; Scott D. Sagan, "Why Do States Build Nuclear Weapons?: Three Models in Search of a Bomb," *International Security* 21, no. 3 (1996): 57-58, https://doi.org/10.2307/2539273.; Jacques E. C. Hymans, "Assessing North Korean Nuclear Intentions and Capacities: A New Approach," *Journal of East Asian Studies* 8 (2009): 265, https://dornsife.usc.edu/jacques-hymans/wp-content/uploads/sites/323/2023/09/Hymans_JEAS_North_Korea_article.pdf.

[83] Hymans, 265; Habib, "The Enforcement Problem," 52.

[84] Stephan Haggard and Marcus Noland, "Sanctioning North Korea: The Political Economy of Denuclearization and Proliferation," *Asian Survey* 50, no. 3 (2010): 545, https://doi.org/10.1525/as.2010.50.3.539.

juche and *songun* elevates nuclear weapons from a strategic instrument to a cornerstone of state function.[85] Resources, labour, and scientific expertise are preferentially allocated to the nuclear sector via the military, even as other sectors of the economy remain underdeveloped or in crisis, embedding both as central elements of state survival and regime legitimacy.[86] This centrality is affirmed by the endurance of the nuclear program in the face of international sanctions, famine, and economic shrinkage.[87] Further, the framing of the DPRK's nuclear project as an existential imperative of the Kim family's legitimacy is leveraged to justify political insulation, which is derived through the mutually reinforcing *juche* and *songun* doctrines.[88] Contrary to typical expectations of regime failure in similar dictatorship models, the survival of the Kim dynasty suggests a political system so tightly controlled by the leadership that the core military mission – in this case, nuclear power – persists even under extreme pressure. This aligns with broader academic findings on neo-patrimonial and sultanist regimes that suffer deeply from bureaucratic dysfunction yet are successful at maintaining high-priority sectors.[89]

Such entrenchment negates non-proliferation efforts: denuclearization would require a fundamental reorganization of the North Korean governance model and political identity.[90]

---

[85] Kevin Gray and Jong-Woon Lee, "Following in China's Footsteps? The Political Economy of North Korean Reform," *The Pacific Review* 30, no. 1 (2017): 60-61, https://doi.org/10.1080/09512748.2015.1100666.

[86] Frank, "Political Economy of Sanctions," 17; Zellers, "Hacked!," 280-281; Sagan, "Why Do States Build Nuclear Weapons?," 74; Koen & Beom, "The Last Transition Economy?," 9.

[87] Koen & Beom, 7.

[88] von Soest, "Authoritarian Regimes," 15.

[89] von Soest, 11; Hymans, "North Korean Nuclear Intentions," 274.

[90] Anderson, "North Korea's Nuclear Ambitions," 634.

Counter-proliferation thus carries the burden of managing the DPRK nuclear program, yet this entrenchment still imposes a significant barrier: the regime is willing to bear extraordinarily high costs for a capability it views as an existential imperative, so sanctions result in a "rally-round-the-flag" effect rather than incentivizing compliance.[91]

Increasing deterrence efforts have coincided with the ideological developments of j*uche* and s*ongun*. As sanctions have intensified, the DPRK has been unable to reciprocate traditional, high-volume foreign trade. This has spurred a shift in governance structures via a substitution effect, where traditional economic activity has been replaced by illicit, state-sanctioned activities.[92] This is best demonstrated by the bureaucratic inclusion of Office 39 in the 1970s. A notorious criminal bureau thought to derive revenue from large-scale criminal enterprises (i.e., arms and narcotics trafficking), Office 39 is functionally a laundering machine for the North Korean state.[93] After being blacklisted by the FATF in 2013 and a severe economic recession, the black-market exchange rate became a basis for domestic transactions in North Korea, which marked a decisive shift to a black and grey-market supported shadow economy.[94] In combination with the continuation of a governance model that has formalized laundering for revenue, such a

---

[91] Frank, "Political Economy of Sanctions," 17; Habib, "The Enforcement Problem," 51-52; Haggard & Nolan, "Sanctioning North Korea," 23; von Soest, "Authoritarian Regimes," 12.

[92] von Soest, 11-12; Frank, "Political Economy of Sanctions," 20; Bechtol Jr., "North Korea Illicit Activities," 94.

[93] Bechtol Jr., 58; Jenny Jun, Scott LaFoy, and Ethan Sohn, *North Korea's Cyber Operations: Strategy and Responses* (Center for Strategic and International Studies, 2015), 54, https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf.

[94] Koen & Beom, "The Last Transition Economy?," 14-15.

dynamic can be understood as state-based criminality.[95] The adoption of such a model forms a mandate for illicit revenue generation at the state level.

2.4.2 The Resulting Mandate for Illicit Revenue Generation

The shift to illicit revenue generation is thus an existential necessity. This necessity is highlighted by the vast resource disparity within the state: estimates show that the level of preferential funding the military receives puts per capita asset costs for military personnel at an approximate 8:1 ratio compared to non-military personnel. By way of comparison, estimates for the US, which has the largest military in the world, is 5:1.[96] Such extraordinary spending requires a reliable, sanctions-proof source of currency. As sanctions closed off traditional banking access (e.g., removal from SWIFT), the need for an un-censorable financial mechanism became acute. This imperative accelerated the development of two key, non-traditional PF channels. First, *Proliferation Exportation*, where North Korea cemented its role as a proliferator, exporting nuclear-related materials and expertise to other states, particularly in the Middle East and Africa, using diplomatic and commercial channels as revenue nodes.[97] The second, and more relevant

---

[95] Bechtol Jr., "North Korean Illicit Activities," 58, 60-61, 94; Frank, "Political Economy of Sanctions," 20; Perry, "Proliferation on the Peninsula," 85-86.

[96] Charles Wolf, Jr. and Kamiljon T. Akramov, *North Korean Paradoxes: Circumstances, Costs, and Consequences of Korean Unification* (Santa Monica, CA: RAND Corporation, 2005), 14, https://www.rand.org/pubs/monographs/MG333.html.

[97] Perry, "Proliferation on the Peninsula," 84; Haggard & Nolan, "Sanctioning North Korea,"14; Stephen Blank, "Russia's Proliferation Pathways," *Strategic Insights*, December 2008, 3, https://apps.dtic.mil/sti/pdfs/ADA517404.pdf.; Bechtol Jr, "North Korean Illicit Activities," 76, 78; Daniel Salisbury, "Spies, Diplomats and Deceit: Exploring the Persistent Role of Diplomatic Missions in North Korea's WMD Proliferation and Arms Trafficking Networks," *Asian Security* 17, no. 3 (2021), https://doi.org/10.1080/14799855.2021.1942848.

adaptation to this thesis, is *Cyber-Enabled Fundraising*, which involves investing in state-sponsored cyber capabilities to generate revenue, leading to the rise of VAs as a new pillar in the regime's progress towards autarky.[98] Of these strategies, the rapid development of state-sponsored cyber capability is the more resilient and scalable means of generating non-traditional currency.

2.4.3 The Rise of State-Based Cyber Criminality

The increasing global popularity of VAs has provided the DPRK with a uniquely suitable channel for sanctions-resilient financing that is highly compatible with cyber capabilities. VAs are borderless, pseudonymous, and function outside traditional correspondent banking. That makes them particularly valuable for a state excluded from the global financial system.[99] Prior to its dissolution, the UN Panel of Experts consistently concluded that cyber-derived VA revenue contributes directly to the DPRK's WMD program. They linked cyber operations to physical supply chain procurement.[100]

---

[98] Wright, "The Evolution of Sanctions Evasion," 16; Macfarlane, "Strengthening Sanctions," 200; Zellers, "Hacked!," 200, 268; Barney Warf, "The Hermit Kingdom in Cyberspace: Unveiling the North Korean Internet," *Information, Communication & Society* 18, no. 1 (2015): 115, https://doi.org/10.1080/1369118X.2014.940363.; United States Department of Treasury, *2024 NPFRA,* 10; Stephanie Kliene-Ahlbrandt, "North Korea's Illicit Cyber Operations: What Can Be Done?," *38 North*, February 2020, 1-2.

[99] Frank, "Political Economy of Sanctions," 30; Haggard & Nolan, "Sanctioning North Korea," 22; Wronka, "Digital Currencies," 1272, 1274; Ungboriboonpisal, "Efficacy of Economic Sanctions," 222.

[100] Macfarlane, "Strengthening Sanctions," 214; Vacusta, "Sanctions Evasion and Virtual Assets," 55; Kliene-Ahlbrandt, "North Korea's Illicit Cyber Operations," 1-2; Zellers, "Hacked!," 266; c.f. United Nations Security Council, *Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)*, S/2024/221 (New York: United Nations, March 7, 2024), esp. 60, https://undocs.org/S/2024/221.

Evidence suggests that the DPRK has invested heavily in building a sophisticated cyber apparatus capable of generating, moving, and converting value outside of the regulated financial system. These capabilities are primarily housed within the Reconnaissance General Bureau (RGB), a North Korean military intelligence agency that works in coordination with Office 39.[101] Under the RGB, the DPRK employs a large force of cyberwarfare specialists deployed both within the DPRK and abroad in permissive environments such as China, Russia, and various parts of Southeast Asia.[102] Estimates indicate that as many as 6,000 cyber-warfare personnel are currently employed by the RGB.[103] They are trained in state-run institutions such as the Pyongyang University of Automation and the Automated Warfare Institute (Moonshin Dong Military Academy).[104] The most well-known group of such specialists, Lazarus, has been implicated in dozens of high-profile cyberattacks targeting financial institutions and cryptocurrency exchanges globally.[105]

---

[101] Wright, "The Evolution of Sanctions Evasion." 16; Jun, LaFoy, & Sohn, *North Korea's Cyber Operations*, 5-6.

[102] David Carlisle and Kayla Izenman, "Closing the Crypto Gap: Guidance for Countering North Korean Cryptocurrency Activity in Southeast Asia," *Royal United Services Institute Occasional Paper*, April 2019, 8, https://static.rusi.org/20190412_closing_the_crypto_gap_web.pdf.

[103] Carlisle and Izenman, 8; Zellers, "Hacked!," 282.

[104] Warf, "The Hermit Kingdom," 115; Carlisle & Izenman, "Closing the Crypto Gap," 8.

[105] Carlisle & Izenman, 8; Kliene-Ahlbrandt, "North Korea's Illicit Cyber Operations," 12; Bogdan Vacusta, "Sanctions Evasion and Virtual Assets: Implications for National Security," *Strategic Impact* 87, no. 2 (2023): 50, 57, https://doi.org/10.53477/1842-9904-23-11.

State investment in the development of this cyber infrastructure has been significant; a 2009 estimate reports that the regime allocated $56 million to cyberwarfare that year.[106]. While the DPRK does not release official figures, the Bank of Korea and US State Department estimate the regime's gross domestic product (GDP) to have been between 24.7 and 24.8 billion dollars in 2008, based on gross national income (GNI) figures.[107] The overall allocation of GDP to cyber capability can therefore be estimated at 0.22%. This is four times the intensity of US federal cyber spending during the same period, which accounted for approximately 0.05% of its GDP in 2009.[108] Furthermore, while the DPRK's overall defence budget during this period was estimated at 30% of its GDP,[109] compared to 4.3% in the US,[110] their respective internal allocations to cyber were strikingly similar: approximately 1.2% in the US, and 0.7% in the DPRK. This proportional commitment is significant given the massive disparity in absolute numbers. To put

---

[106] Warf, "The Hermit Kingdom," 116.

[107] Note that in the case of North Korea, nominal GNI is treated as interchangeable with GDP, despite them measuring different economic activities. GNI measures the total income earned by a nation's people and businesses, regardless of where it is earned, while GDP measures the total value of all final goods and services produced within a country during a given period. Because North Korea's economy is deeply isolated and has little inflow of foreign direct investment, their nominal GNI is considered an effective way to estimate GDP. c.f.; Byung-Yeon Kim, *Unveiling the North Korean Economy: Collapse and Transition* (Cambridge: Cambridge University Press, 2017), esp. 35–42.

[108] Office of Management and Budget, *Fiscal Year 2009 Information Technology Budget Overview and Update* (Washington, DC: The White House, 2008), 4, https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/omb/assets/egov_docs/FY09_IT_Budget_Rollout.pdf.; World Bank, "United States," World Bank Open Data, accessed March 13, 2026, https://data.worldbank.org/country/united-states

[109] Chung-in Moon and Sangkeun Lee, "Military Spending and the Arms Race on the Korean Peninsula," *Asian Perspective* 33, no. 4 (2009): 82, http://www.jstor.org/stable/42704693.

[110] Sam Perlo-Freeman et al., "Military Expenditure," in *SIPRI Yearbook 2010: Armaments, Disarmament and International Security* (Oxford University Press, 2010), 203, https://www.sipri.org/sites/default/files/SIPRIYB201005A.pdf.

it in perspective, the DPRK's entire annual cyber budget during this period was just under half of the cost of a single US F-22 Raptor (which had a flyaway cost of $140 million in 2009); by contrast, the US's cyber budget could have purchased more than 50.[111]

Prioritization of cyber capability has continued to align with state spending patterns. Education reforms since 2017 have expanded instruction in computer science, information security, robotics, and applied mathematics, while national science and technology expenditures increased by 8.7% in 2019.[112] By investing in the cultivation of domestic technical expertise, the regime has insured a steady supply of skilled personnel for its cyber programs. For a relatively minimal capital outlay, the DPRK has established a cyber supply chain that can continuously manufacture high-value assets at a fraction of the cost of traditional one-time purchases of military hardware. This strategic prioritization of asymmetric capability has yielded a massive return on investment, providing the regime with a low-overhead, high-impact tool for sanction circumvention.

The scale of VA revenue generated through DPRK cyber operations is staggering and escalating. Between January 2017 and September 2018, the regime was linked to an estimated $571 million in stolen crypto assets; between 2019 and November 2020, $316 million; in 2021

---

[111] U.S. Government Accountability Office, *Defense Acquisitions: Assessments of Selected Weapon Programs*, GAO-09-326SP (Washington, DC, 2009), 9, https://www.gao.gov/assets/gao-09-326sp.pdf.; Maya Carlin, "The Air Force Built 195 F-22s Instead of 750 and Destroyed the Tooling to Make More - Now China has Exactly the Air Force the Raptor was Designed to Defeat" *19FortyFive*, March 2026, https://www.19fortyfive.com/2026/03/the-air-force-built-195-f-22s-instead-of-750-and-destroyed-the-tooling-to-make-more-now-china-has-exactly-the-air-force-the-raptor-was-designed-to-defeat/.

[112] Koen & Beom, "The Last Transition Economy?," 34; Zellers, "Hacked!," 282.

roughly $400 million; and nearly $1 billion in just the first quarter of 2022.[113] In 2022, the Lazarus Group alone was found responsible for the theft of approximately 1.7 billion USD in VAs – an amount exceeding the DPRKs total annual export in goods in 2020 (an estimated $142 million USD).[114] Blockchain analytics indicate that over 40% of all illicit crypto flows in 2022 originated from activity tied to sanctioned entities. That figure is dominated by actors linked to North Korea.[115]

Generating revenue through VAs for the nuclear program is not limited to crypto-theft: the DPRK also conducts cryptocurrency mining and cryptojacking operations, the full scale of which is impossible to gauge.[116] Cyber capability is thus central to North Korean PF.

2.4.4 The DPRK as a Diagnostic and Predictive Case Study for VA-PF

The most significant threat posed by proliferators such as the DPRK is not limited to their weapons programs, but to the adaptive, resilient financial architecture that sustains them. The DPRK's state-directed criminal apparatus represents the most developed form of PF currently observable, operating at scale and a level of coordination that few other states can match. Precisely because North Korea is so heavily monitored, the fact that its VA-enabled financing

---

[113] Zellers, "Hacked!," 266.

[114] Vacusta, "Sanctions Evasion and Virtual Assets," 53.

[115] Vacusta, 51.

[116] Carlisle & Izenman, "Closing the Crypto Gap," 16; Ungboriboonpisal, "Efficacy of Economic Sanctions," 220; Kliene-Ahlbrandt, "North Korea's Illicit Cyber Operations," 13; Adrian Corobana, "Financial International Sanctions and Cryptocurrencies: Challenges and Solutions," *European Business Law Journal* 1, no. 1 (2023): 77, https://doi.org/10.24818/EBLJ/2022/1/1.06.

networks continue to function demonstrates the resilience of these methods under the highest possible enforcement pressure. As such, the DPRK does not represent an outlier. Rather, it represents the upper bound of the risk profile. If a system this extensively surveilled can develop stable VA-based financing channels, then less-scrutinized states are likely to adopt them earlier, more quietly, and with fewer observable traces.

In this sense, the DPRK functions as a canary in the coal mine. It illustrates both the technical feasibility and strategic logic of VA-PF. It offers a window into practices that may already be emerging elsewhere but have not yet reached a detectable threshold. Conversely, understanding the points at which DPRK networks remain vulnerable provides a strategic foundation for preemptive interdiction. If the most advanced case can be disrupted, then diffusion across the rest of the VA-PF adoption spectrum can theoretically be curtailed or prevented. Studying the DPRK, therefore, allows this thesis to analyze VA-PF not as a speculative future risk, but as an active system of practice whose dynamics can inform both predictive monitoring and policy intervention.

The DPRK is not simply an exercise in case selection. It examines the limits of the existing order as a basis upon which future directions for enforcement can be built. This sets the stage for the subsequent chapters, which examine how VA-PF restructures actor dynamics and enforcement logic within the global financial system.

Chapter 3: Methodology

This chapter outlines the research design and analytic strategy used by this thesis to address the central debate in scholarship around VA-PF: are VA's being adopted by proliferators? It does so by addressing the empirical evidence paradox discussed in the previous chapter. To accomplish this, the thesis collates legal cases of DPRK PF involving VAs into a systematic dataset called the North Korean Virtual Asset-Proliferation Financing Dataset.

No pre-existing, replicable methodology is capable of capturing and analyzing cyber-enabled revenue networks, VA accumulation, and subsequent laundering activities. To address this gap, this thesis adapts and extends the established Terrorist Resourcing Model (TRM).[117] The resulting framework, referred to as the Virtual Asset Proliferation Resourcing Model (VA-PRM), was developed for this study but is theoretically applicable to other analyses of VA-PF.

The remainder of this chapter explains the rationale and novelty of this approach, the case selection process and inclusion criteria, addressed the limitations of the method, and discusses the analytic strategy used to interpret the dataset.

3.1 Methodological Innovation

This research makes three distinct methodological innovations. First, it produces the first replicable methodology designed to systematically capture the use of VAs within PF networks.

[117] The TRM was introduced in Christian Leuprecht et al., "Tracking Transnational Terrorist Resourcing Nodes and Networks," *Florida State University Law Review* 46 (2019): 314, https://www.fsulawreview.com/wp-content/uploads/2022/08/TRANSNATIONAL-TERRORIST-RESOURCING-.pdf.

The framework integrates variables that account for decentralized financial infrastructure (i.e., virtual currency exchanges (VCE)) alongside those associated with conventional financial systems. In doing so, it contributes to closing a significant empirical gap in PF and AML research. Second, the thesis demonstrates that resource-based network tracing models are transferrable between different types of financial crimes. It adapts the TRM, which was originally designed for TF research, to PF. Although modified and extended, the core elements and logic of the TRM remain intact. Ergo, network-centric analysis remains applicable and adaptable to different forms of illicit finance research, which extends the analytic utility of the TRM. Finally, this thesis offers the first structured, codified dataset of VA-PF networks linked to the DPRK. This methodological baseline enables future comparative study, risk modeling, and development of data-driven enforcement strategies.

3.2 The TRM & VA-PRM

The Terrorist Resourcing Model (TRM), developed by Leuprecht et al. (2019), is an empirically replicable framework in illicit finance research that is designed to trace the acquisition, aggregation, movement, and deployment of resources across transnational financial crime networks. The model operates through a five-stage, nonsequential coding process consisting of acquisition and exchange, aggregation of resources, movement of resources, transmission to terrorist organization, and purpose of resources.[118] Its analytic strength lies in modeling the flow of resources across networks, rather than focusing on individual transactions.

[118] Leuprecht et al, "Terrorist Resourcing Nodes," 315-319.

This makes its logic inherently transferable to other network-based financial crimes, including PF. Slight modification and expansion were required because VA-PF diverges from terrorist financing in three significant ways.

First, the TRM is designed to evaluate resources that were initially generated within and subsequently diverted through the regulated financial system. This limited its application to VAs, which may or may not intersect with the regulated financial system. The VA-PRM resolves this by expanding the set of variables to accommodate key elements of decentralized financial movement, such as virtual currency exchanges.

Secondly, the TRM concludes with the conversion of funds for an operational deployment (e.g., executing a terrorist attack).[119] PF does not necessarily culminate in the execution of an event or specific outcome. Instead, it is characterized by the accumulation of enabling capability. Because the TRM is interested in the deployment of financial resources, it codes variables such as terrorist attack dates and victims. These metrics are not applicable to PF. Instead, the VA-PRM reconceptualizes these coding metrics to account for cyber-enabled predicate offenses, such as cyber thefts and cyber attacks. This decision is grounded in the literature linking DPRK cyber operations to WMD financing, as noted in the previous chapter. It allows the dataset to examine the scale, sophistication, and effectiveness of cyber operations and their resulting impacts on the proliferation networks they fund.

[119] Leuprecht et al., 318.

Finally, to accommodate these divergences, the VA-PRM modifies the operational boundaries of the variables used in the last two stages of the TRM and expands the first. First, variables related to the transmission of funds to a terrorist organization are reconceptualized as the transmission of funds to a regime (reflecting the state-based nature of DPRK PF). Second, the purpose of resources is defined in two ways: as being for the DPRK nuclear program broadly, and as the point at which value becomes available for procurement use, rather the moment of a specific purchase. Finally, the acquisition stage is expanded to include coding of a predicate offense.[120]

3.3 Criteria for Source Collection & Case Inclusion

Cases reviewed in this thesis were sourced from government documents, such as Department of Justice press releases, OFAC designations, and Treasury Department actions. Source collection was completed in two stages: first by searching electronic legal databases and publicly accessible government databases, including OFAC, The Department of Treasury website and archives, the Department of Justice website and archives, LexisNexis, and CanLII; and then by scanning secondary and grey literature sources, including scholarly journals, private sector reports, government publications, law enforcement bulletins, and news articles. A preliminary literature review developed a list of key terminology which was deployed in the collection process, including "proliferation," "WMD," "money laundering," "North Korea,"

[120] For a full list of variables employed, see Appendix A.

"virtual currency," "cryptocurrency," "coin," "token," "financing," and "sanctions". These terms ensured that cases selected met the following basic inclusion criteria:

1) Transnational or cross-border in nature
2) Attributed to or identified as involving actors linked to the Kim dynasty
3) Included VCs

Approximately 25 cases were initially collected. After further review to ensure all inclusion criteria had been satisfied, 12 cases remained viable and 11 were coded in the final dataset.[121] The remaining cases were excluded because they failed to meet one or more of the inclusion criteria upon closer inspection.

The 12th case included two related filings and could not be coded because it lacked sufficient information about financial transactions. Although excluded from the coded dataset, these filings provided useful qualitative insights that warranted inclusion in the study and are thus introduced and discussed as a single case study in chapters 4 and 5. One other case that is included in the coded dataset contained unique characteristics that could not be fully captured in the coding process. It is also examined qualitatively as a second case study in chapters 4 and 5. These two cases were selected for qualitative study over others only because they contained anomalies that could not be accounted for by the coding instrument.

[121] For a full list of selected cases, see Appendix B.

3.4 Limitations of the Method & Data

The reliance of this method on publicly accessible legal and government documents has several inherent limitations.

3.4.1 Jurisdictional, Language, and Source Bias

All cases reviewed in this thesis were sourced from North American and European jurisdictions. This trend is explained by two primary factors: first, cases from rule-of-law jurisdictions, which are predominantly North American and European, make up the overwhelming majority of publicly accessible court documents. Second, these jurisdictions, particularly the US, play an outsized role in maintaining global sanctions and financial regulation frameworks. They thus have established structures to identify, attribute, and account for financial crimes. This jurisdictional focus, while practical to access data, may bias the scope and type of financial activity captured in the dataset. Additionally, the dataset relies exclusively on English-language legal and regulatory sources. Relevant investigations in other jurisdictions may therefore be underrepresented if they are not accessible in English, or if translations could not be located through the English-language databases used to source cases.

Furthermore, limiting the dataset to court records means excluding other sources like grey literature, investigative journalism, and private blockchain analytics reports. While this reinforces the geographic limits of the data, legal documents were chosen for three practical reasons.

First, the Terrorist Resourcing Model (TRM), which the VA-PRM is derived from, is designed to be compatible with legal sources. Changing the VA-PRM to include other types of material would require extensive methodological modification to ensure the data remains reliable and replicable. This restructuring was not feasible given the resources and time available for the study, but is recommended as a path for future development of the methodology.

Second, each alternative source has its own inherent disadvantages. Grey literature may have a much shorter temporal lag than other sources but is prone to circular reporting, and details provided are often hard to verify independently. Private blockchain analytics reports are published less frequently and often focus on overall trends and technical granularities rather than specific case details; even when they do look at activities perpetrated by a specific network, private companies may only see the small part of the transaction their services touched. Additionally, a vast majority of these alternative sources are for-profit entities with their own commercial interests to consider. Publicly accessible court documents, by contrast, offer a high threshold of verifiability, and present a strong option for citation tracing and replicability.

Finally, court documents are unique in that they serve as a partial record of state action. Because CPF is primarily a state-driven effort, court records can provide unique insight into the specific context the study is interested in. For these reasons, the trade-off involved in using court documents over other sources was deemed acceptable.

3.4.2 Legal, Regulatory, & Temporal Constraints

Data availability is inherently limited by the regulatory scope and the temporal lag of legal frameworks. PF is not only understudied but also unevenly regulated. Network

identification and subsequent legal actions are constrained by the scope of existing financial regulations and enforcement practices. That existing regulations around VAs are relatively new and not yet widely adopted across jurisdictions amplifies this constraint.

Furthermore, no cases of PF involving VAs can exist prior to 2009 (the introduction of the first VC).[122] The scope is further reduced by the time required to develop regulation, conduct enforcement, compile evidence, and formally bring a case to court. This limiting factor is evident in the data; the oldest identified case involved illicit activities beginning in 2015. This same factor applies inversely to recent cases. A hack of a major exchange may occur, but legal documents detailing the financial networks associated with it will not be disclosed until months or years later. As a result, analysis of the data is limited to past, successfully prosecuted networks.[123] Similarly, given the nature of the content, it is possible that cases of PF may intersect with classified intelligence operations and therefore be inaccessible to the public. Some proliferation networks may therefore remain absent from the public record, even if they have been detected and disrupted.

Additionally, due to the lack of specific legal accountability mechanisms related to crypto-crime, charges brought against actors in VA-PF networks are generally related to other criminal activities (e.g., money laundering, conspiracy), rather than the illicit use of VAs itself.

---

[122] Macfarlane, "Strengthening Sanctions," 201.

[123] See, for example, the ByBit Exchange hack of 2025, which has been widely attributed to the Lazarus Group but could not be included in the datatset due to lack of applicable legal documentation. Kara Struckman and Madison Binder, "The Bybit Heist: What Happened & What Now?," Wilson Center, March 31, 2025, https://www.wilsoncenter.org/article/bybit-heist-what-happened-what-now.

As a result, certain details relevant to the full financial network may be formally omitted from the legal document. That may exclude an otherwise relevant case.

Restriction of the data primarily to US jurisdictions introduces a similar confounding factor. Some of the findings - particularly the "opaque middle" discussed in Chapter 5—may reflect what prosecutors are legally required to name to secure a conviction or indict a case, rather than illustrating a realistic picture of network structure. However, from a different perspective, this still provides valuable insight into the limits of the tools available to prosecutors. This opacity can be interpreted as a feature of enforcement and prosecution structures rather than a characteristic of the illicit networks themselves, highlighting a different but closely related problem.

3.4.3 Dual-Use Ambiguity

A final, persistent limitation is the ambiguity of dual-use goods: goods that can be used for illicit proliferation but also have legal uses.[124] It is difficult to determine the ultimate purpose for which a dual-use good is procured; consequently some portion of proliferation activities and acquisitions is inherently unidentifiable.[125] While the heavy sanctions regime imposed on North Korea has restricted most dual-use goods, and records of sanctions violations offer some insight, these records often lack the detail necessary to code the network. As a result, currently

[124] Brewer, "Financing of Nuclear and Other Weapons," 2; Passas, "Financial Controls," 758-759.

[125] Passas, 758-759; Brewer, "Financing of Nuclear and Other Weapons," 3.

identifiable proliferation activities represent only a portion of actual proliferation by the DPRK. Nonetheless, these cases give us a window which we did not have before.

3.4.4 Analytic Strategy

The TRM is designed to be compatible with Social Network Analysis (SNA), which is a means of quantitatively evaluating relationships within a given network, and analyzing them comparatively. Analysis using this method is a goal for future research. At this point, the dataset itself is entirely novel. Other analytic methods are, therefore, better suited to producing initial, foundational insights that can ground future inquiry. This thesis employs basic statistical analysis accomplished through structured query language (SQL), in combination with qualitative comparative analysis. The results from both will also be interpreted through the E/S/C Framework introduced in the previous chapter. While it does not guide the data coding or interpretation process, it provides an additional analytical lens to interpret findings.

Chapter 4: Observations

This chapter presents empirical observations derived from mixed-methods analysis of the North Korean Virtual Asset-Enabled Proliferation Financing Dataset, including two qualitative case studies. This section focuses on the patterns and trends that emerged from the dataset. First, the networks involved a mixture of regime-linked actors and recipients, with certain actors recurring across multiple cases. Second, financial intermediaries and victims were often geographically concentrated in a few select regions. Third, cyber-enabled theft and cryptocurrency laundering acted as the primary mechanisms for generating and moving funds within networks. Finally, the variety of VAs employed was diverse, and very few fiat currencies were used. The following chapter provides an analytical discussion of these observations.

4.1 Dataset Patterns, Trends, & Observations

4.1.1 Actors & Attribution

Several consistent trends are evident in the composition of actors across the dataset. In total, approximately 262 total actors were coded, representing a mixture of regime-linked entities, investors, financial intermediaries, recipients, exchanges, and victims. Table 2 summarizes the distribution of these actors according to type, national attribution, and degree of identification. It distinguishes among the total number of actors, the total number linked to a specific country, and those explicitly named in the legal documents. This allows for a clearer picture of actor composition within the coded PF networks. There is no guarantee that "named" individual actors are identified by their government name, and these actors may be identified by

pseudonyms. Some identified actors were entities, companies, or groups, and not individuals. Some actors were attributed to a country, or named, but not both.

Table 2: Statistical Overview of Actor Types by Degrees of Attribution Identification

Actor Type	Total Actors	Total Attributed to Country	% of Total Actors Attributed to Country	Total Identified, Excluding Unnamed/ Unknown	Total Identified by Name & Attributed to Country	Total % of Actors Attributed to Country & Named
Investor	23	8	34.78%	12	7	30.43%
Recipient	18	10	55.56%	8	8	44.44%
Bank	35	35	100.00%	12	12	34.29%
Virtual Currency Exchanges	25	4	16.00%	6	0	0.00%
Financial Intermediaries	88	42	47.73%	34	15	17.05%
Victims	57	47	82.46%	34	12	21.05%
Regime Affiliates	16	16	100.00%	15	15	93.75%

The qualitative data across cases shows a regular recurrence of actors. Unsurprisingly, Office 39, the RGB, and the Lazarus Group are identified throughout the data, primarily as investors and recipients, although occasionally they also function as financial intermediaries. Many individual actors were also repeatedly identified. Notably, Tornado Cash (a mixer) and Sim Hyon Sop (a facilitator) appeared several times across different cases, with Sop even being

charged in two separate cases. Identical wallet addresses, emails, and IP signatures were also reused across cases.

4.1.2 Geographic Distributions

Multiple geographic patterns were also evident in the dataset. 25 countries and 28 sub-national regions were collectively represented across the dataset. The following figures provide visual representations of this data, illustrating total geographic occurrences across the dataset variables.

Figure 2: Total Dataset Occurrences by Sub-National Region

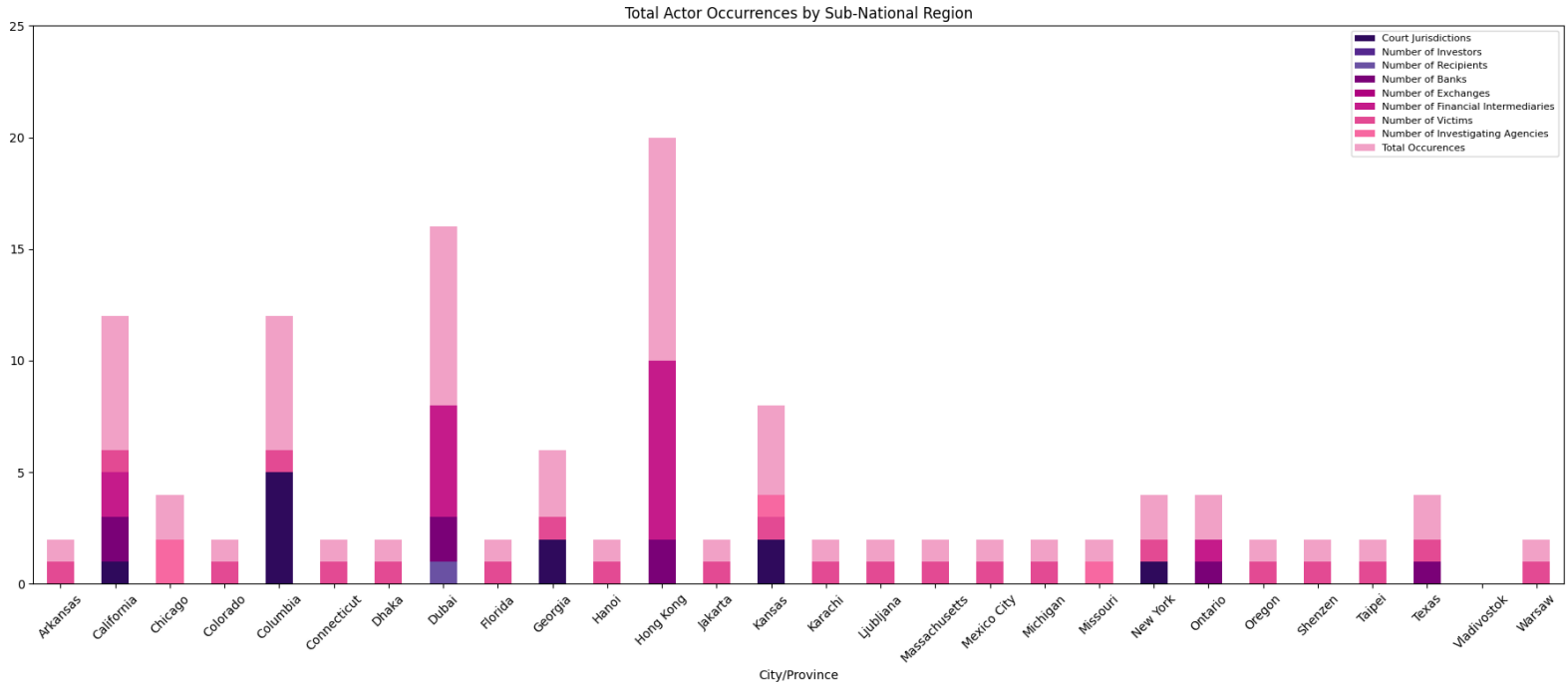
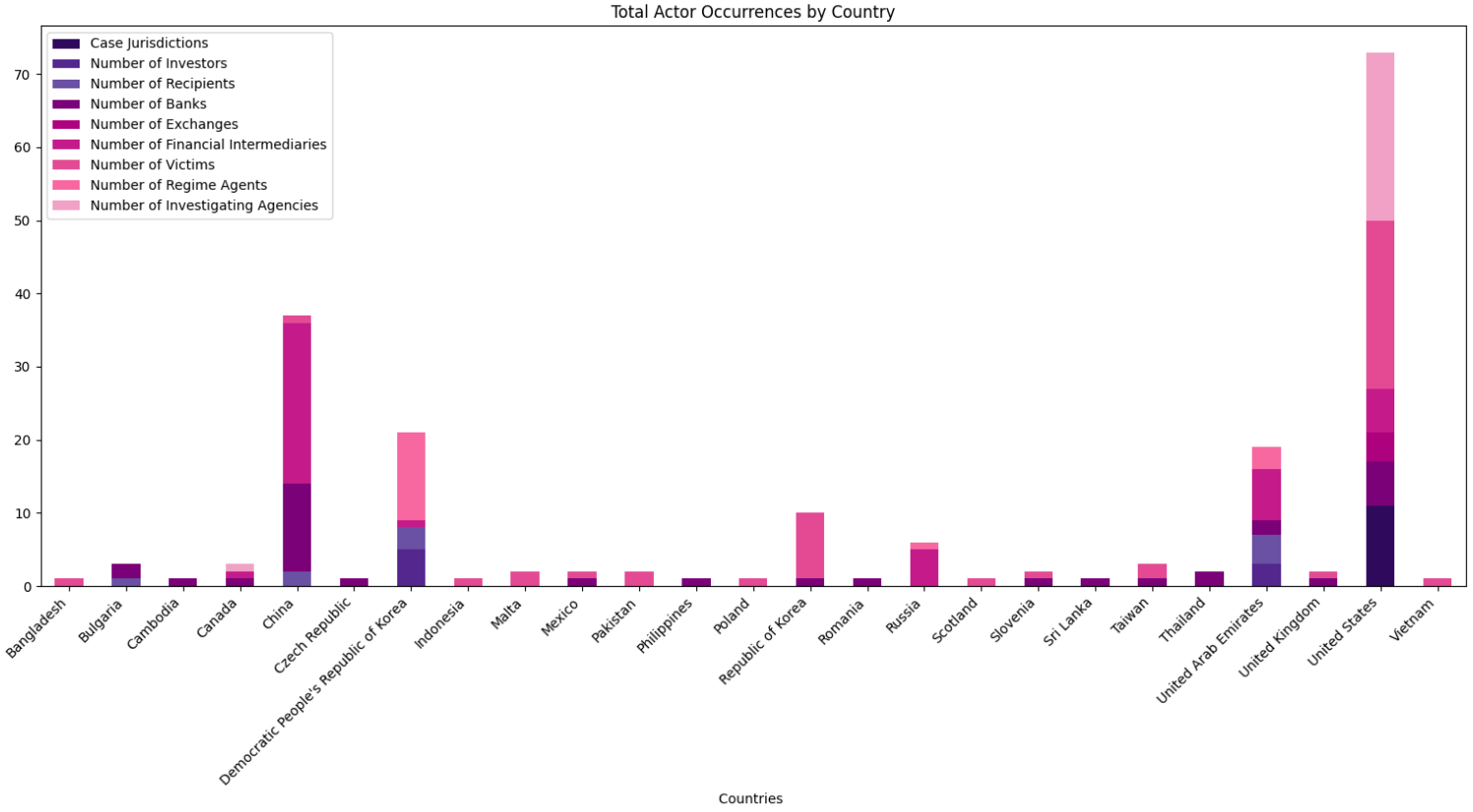


Figure 3: Total Dataset Occurrences by Country



The most interesting findings are:

- Financial intermediaries were disproportionally concentrated in China (22), followed by the United Arab Emirates (7), and the US (6)
- Only one financial intermediary in the dataset was attributed to the DPRK
- Hong Kong and Dubai emerged as the most frequently reoccurring sub-national nodes
- Russia and Russian-interest zones in the Eastern European sub-region only appear in the dataset once
- Most banks identified were located in China (12), with the second most in the US (6)
- Victims of cyber-attacks linked to monetary investments in the PF networks were primarily based in the US (23) and South Korea (9)
- The DPRK had the highest number of attributed investors (5)
- The United Arab Emirates had the highest number of attributed recipients (4)
- All cases were from US jurisdictions, with the most being from the District of Columbia (5)

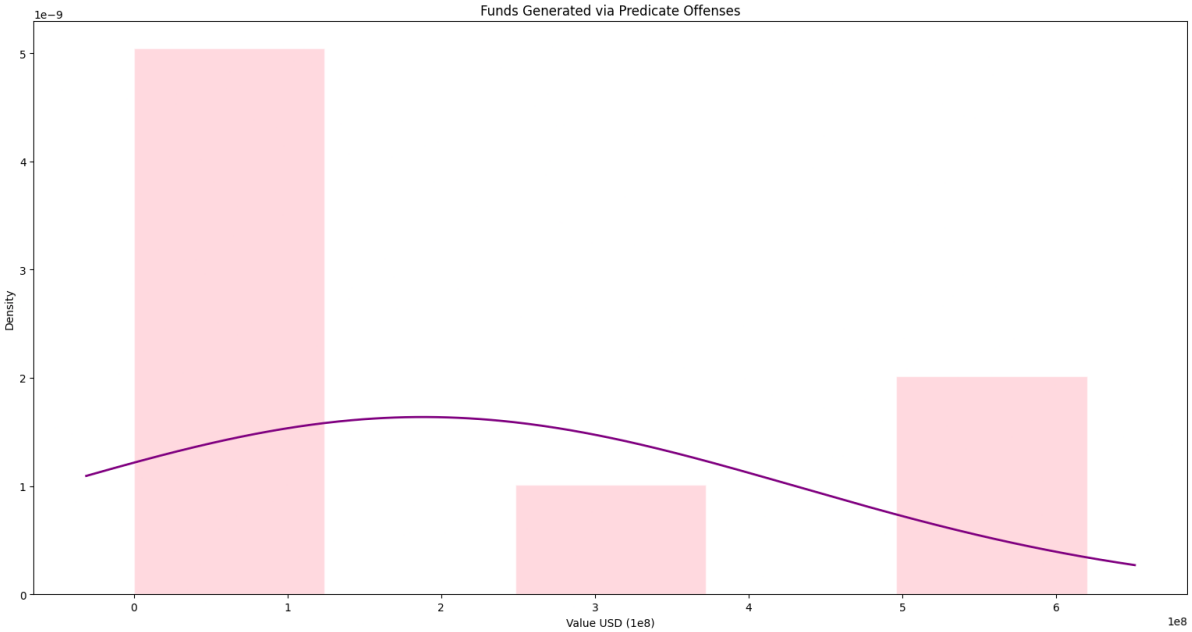
4.1.3 Procurement Patterns & Predicate Offenses

The data shows that procurement of funds by the coded PF networks was predominately achieved through organized cyber-operations. Although some cases were linked to one or two specific incidents, others involved funds from more than a dozen operations spanning several years. Many of these operations were accomplished through sophisticated small-scale intrusions, particularly spearfishing and business-email compromises. Others employed high-impact tactics such as WannaCry ransomware. In most cases, attacks caused substantial financial losses,

routinely reaching millions. Often, attackers had persistent access to victim systems prior to making a single, sweeping cash-out. In at least one instance, adversaries exfiltrated both funds and sensitive data from government and defence contractors. The most commonly recurring financial mechanism in the dataset was cryptocurrency laundering, an umbrella term that refers to the conversion of one VA into another.

Across the dataset, the mean loss per case was approximately $188.1 million USD, with a standard deviation of $243.6 million USD. This wide variance reflects the extreme volatility and variable scale of predicate offenses across the dataset, where a subset of high-impact breaches significantly skewed the overall average.

Figure 4: Funds Generated via Predicate Offenses



4.1.4 Currencies

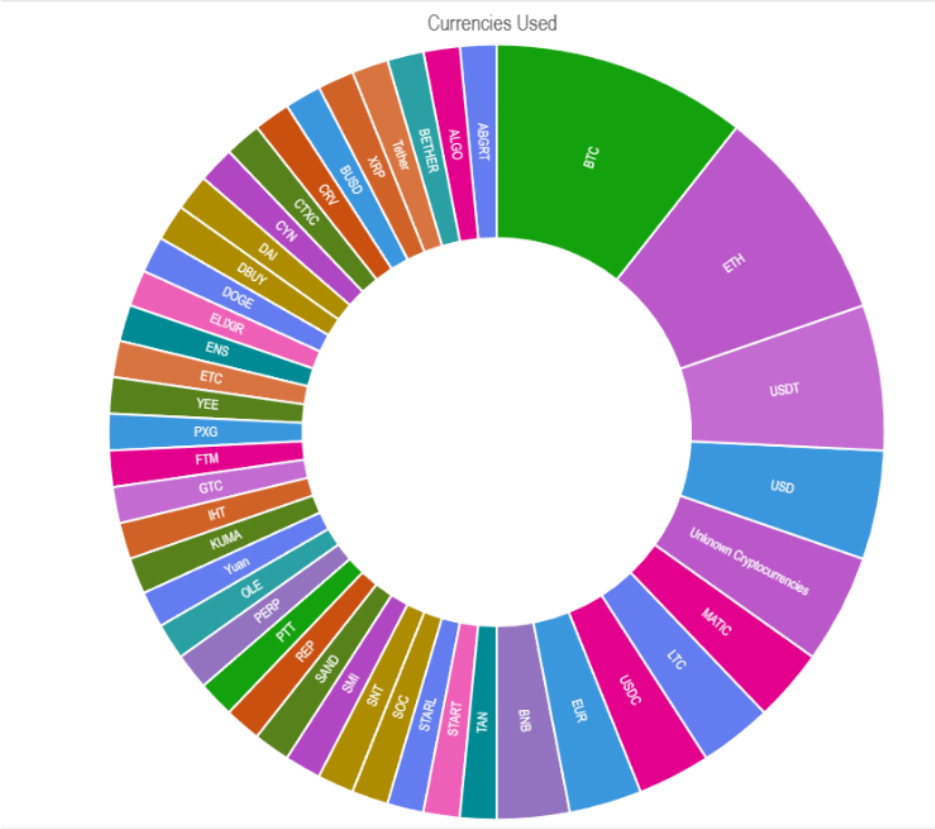
67 currencies were identified in the dataset. 44 were distinct. Of the distinct currencies, 41 were virtual, and three were fiat. Per Table 4, VCs accounted for 93% of total distinct currencies and 91% of total occurrences.

Table 3: Overall Currency Distribution in Dataset by Currency Type

Total Currencies - Fiat vs VCs	Percentage of Total Distinct Currencies	Percentage by Total Occurrences
VCs	93.18%	91.04%
Fiat	6.82%	8.96%

Per Figure 5, Bitcoin, Ethereum, and Tether were the most common currencies that appeared in the data. Most other currencies only appeared once, and a number of these were unpopular or short-lived in nature.

Figure 5: Currencies by Total Number of Appearances in the Dataset



Despite the prevalence of crypto-laundering, which generally necessitates the use of some form of exchange platform, no VCEs in the dataset were definitively geolocated outside of the US, although four unnamed exchanges were linked to US-based infrastructure. In some instances, no VCEs were identified at all, despite other information indicating that a VCE would likely have been employed at some point in the transfer process.

4.2 Case Studies

4.2.1 The 2019 Pyongyang Blockchain & Cryptocurrency Conference

This case study involves two related filings: USA v. Virgil Griffiths, and USA v. Alejandro Cao de Benos and Christopher Emms. Neither filing was coded in the dataset, as neither case included any financial transfer. Rather, the defendants facilitated and provided technical instruction, enabling North Korea actors to generate and conceal illicit revenue streams using VCs.

Emms, a British national, and Cao de Benos, a Spanish national, organized the 2019 Pyongyang Blockchain and Cryptocurrency Conference.[126] Cao de Benos was a well-known public supporter of the DPRK. Emms had a background in cryptocurrency payment processing. They recruited and arranged travel for Griffiths, a US citizen with expertise in the cryptocurrency sector.[127] At the Conference, Emms and Griffith demonstrated to North Korean officials how VCs could be used to circumvent sanctions, mapping out specific transaction patterns designed for this purpose.[128] The three defendants then sought additional opportunities to facilitate such activities, brokering introductions for conference attendees to cryptocurrency

---

[126] *United States v. Cao de Benos and Emms*, No. 1:22-cr-00091-PKC (S.D.N.Y. 2022).

[127] *United States v. Cao de Benos*; *United States v. Griffith*, No. 1:20-cr-00015-PKC (S.D.N.Y. 2020).

[128] *United States v. Griffith*; *United States v. Cao de Benos*.

service providers, recruiting cryptocurrency services for attendees, and seeking to develop blockchain infrastructure and procure associated equipment for the DPRK.[129]

4.2.2 Marine Chain Token

USA v. Jong Chang Hyok, Kim Il, and Park Jin Hyok is coded in the dataset, but has a distinguishing element that warrants closer inspection. The defendants, at the time of arrest, were in the process of producing and promoting Marine Chain Token. This purported blockchain platform would allow investors to purchase fractional ownership of maritime vessels. The token was a fraudulent investment scheme designed to extract funds from international investors to facilitate the DPRK nuclear program under the guise of a legitimate blockchain venture.[130] Enforcement efforts disrupted Marine Chain Token before the scheme could be implemented.

---

[129] *United States v. Griffith*; *United States v. Cao de Benos*.

[130] *United States v. Jon Chang Hyok, et al.*, No. 2:20-cr-00614-DMG (C.D. Cal. Jan. 28, 2021).

Chapter 5: Analysis

This chapter analyzes findings presented in the previous chapter. By synthesizing evidence of actor behaviours, geographic distribution, and financial mechanisms, the analysis moves beyond a descriptive account of the data towards a cumulative interpretation of how these networks function as an enterprise of the North Korean state, and what they reveal about VA-PF as a phenomenon. It is organized into 6 sections, five of which extend from the themes of the previous chapter: Actors & Attribution (5.1), Geography (5.2), Procurement & Predicate Offenses (5.3), Currencies (5.4), and Case Study Takeaways (5.5). The final section synthesizes what the data was missing, offering insights into the blind spots in current enforcement frameworks and the transformative potential of VA-PF.

5.1 Actors & Attribution

Analysis of attribution and identification rates across categories of actors reveals persistent middle opacity within PF networks. Transparency follows a u-shaped curve where it decreases as distance from the core proliferator increases. Visibility was highest at the core (regime affiliates) and terminal points (investors and recipients). This visibility likely stems from a targeted law enforcement focus on known entities previously flagged or identified as proximate to the regime. However, this transparency collapses as funds move into the center of the network. Intermediaries and financial facilitators, particularly VCEs, were profoundly opaque in terms of both attribution and identification. This suggests that CPF enforcement in these cases were endpoint centric.

This finding has at least two reasonable interpretations. Investigative efforts may not have expanded beyond geographic location. Alternatively, this information is withheld by law enforcement, likely to preserve operational security, shield investigative tactics, or preserve victim or intermediary reputations. Under either interpretation, this indicates that weak points in enforcement and regulation exist across the center of the networks. Continued opacity across the middle of the network means, inter alia, that: first, opportunities to disrupt the network before funds reach a recipient are limited or missing. These appear to fall outside of the enforcement jurisdiction in these cases, which makes seizing funds and holding the recipient accountable arduous. Second, identifying facilitators, including exchanges and their location, is difficult.

The observed disparity between rates of broad geographic attribution and specific actor identification is further driven by two limiting factors. First, are the technical limits of blockchain analytics; these allow addresses and wallets to be traced across a network. However, linking cryptotransactions to specific persons or entities requires regular, consistent, and accurate KYC data collection and sharing.[131] This process is currently fragmented. Second is the regulatory friction inherent to decentralized finance. Unlike the traditional financial sector, VAs operate in an environment that is designed to resist centralized oversight mechanisms, including state-driven AML and CPF frameworks.[132] Private sector actors are necessary to the development and operations of mixers, tumblers, and VCs. This creates a conflict of interest for

[131] Michael W. Calafos and George Dimitoglou, "Cyber Laundering: Money Laundering from Fiat Money to Cryptocurrency," in *Principles and Practice of Blockchains*, ed. K. Daimi, I. Dionysiou, and N. El Madhoun (Springer, 2023), 15-17.

[132] Burgess et al, "Terror on the Blockchain," 213; Calafos & Dimitoglou**,** "Cyber Laundering," 12.

states balancing economic competitiveness in the technology sector with national security, allowing digital finance to remain comparatively under-regulated and under-enforced. The rapid popularity growth and volatility of emerging technologies only accentuates the conflict-of-interests states face in attempting to regulate them.

The recurrence of specific facilitators across cases is further indicative of an institutionalized rather than opportunistic proliferation strategy. Failing to unveil the opaque middle in VA-PF networks allows the North Korean state to exploit jurisdictional ambiguity as a protective mechanism for network and asset longevity. The end-point actors identified remain legally and physically unreachable, often in jurisdictions such as the DPRK, where extradition is not feasible, while the identity and location of middle network actors are effectively shielded. However, the recurrence of specific IP addresses and wallets across cases indicates a potential vulnerability in this institutionalized strategy. If the DPRK reuses resources, then those resources represent high-value targets for enforcement. Identifying and dismantling recurring resources within the middle of the network would force the DPRK to expend limited expertise and funds to replace them, acting as a potential mechanism of deterrence. In addition, such interference would disrupt speed and coordination within the network. Thus, shifting enforcement focus away from primarily visible endpoints to recurring middle nodes may be an effective way of raising the cost of VA-PF in these cases.

5.2 Geography

The geographic distribution of the data reveals three key insights into the spatial logic of the DPRK's VA-PF strategy. First, these networks follow a triadic structure consisting of source,

transition, and destination regions that mirror the visibility curve established in the previous sub-section. Second, transition regions are strategically selected to serve as a source of jurisdictional shielding, contributing to the middle opacity observed across the VA-PF networks. Third, global enforcement remains highly asymmetric, as visibility is concentrated primarily where unilateral US investigation, enforcement, and prosecution can reach.

Source regions operate as sites for capital accumulation. They are developed and technologically advanced states which show an ideological antipathy towards the Kim Regime, such as the US and South Korea. Transition regions operate as sites for laundering and re-integration. Favoured jurisdictions have high degrees of financial secrecy and loose or permissive regulatory regimes, such as the UAE or Hong Kong. Inability to identify VCE locations calls into question whether these financial flows match the particular distribution of jurisdictions in the dataset. Perpetrating actors may still be linked to these regions regardless of the location of the platforms they exploit. Destinations are the ultimate beneficiary of funds and resources: the DPRK. Every case within the dataset shows direct ties to North Korea and its nuclear weapons program. The continuity of this structure across the dataset reinforces the argument that DPRK VA-PF is a strategic, coordinated effort, rather than a series of opportunistic or ad hoc operations.

The concentration of middle network actors within jurisdictions with histories of political shielding (i.e., China and the UAE) demonstrates how the DPRK weaponises financial secrecy.

Noteably, the absence of known enablers such as Russia[133] suggests either a total lack of VA-PF activity, or, more likely, a level of obfuscation so effective that it falls off the visibility curve.

The geographic distribution of the data likewise highlights a profound centralization of enforcement in the US, particularly in the District of Columbia. This supports a broader trend in financial crime: the structural asymmetries in global regulatory capacity. While the PF networks identified in the dataset operated transnationally, accountability was concentrated in a single jurisdiction. This can be explained, at least in part, by the robust legal authority the US is granted through its position as an Enforcer, exemplified by the powers it grants itself in laws that allow it to project regulatory power far beyond its physical borders, such as the IEEPA

However, this centralization also reveals a point of tension. The US acts both as a primary financial vector for actors at highly visible points within the observed networks, and an aggressive prosecutor of those actors. This duality may be attributable to US dominance in both the technological development space and global financial system. Across the cases, overall visibility of a network is highest where US enforcement is strongest and most accessible, but transparency drops as soon as funds enter the middle of the network. Because the US cannot unilaterally enforce transparency upon transition regions that contain key operational hubs – such as the UAE – they remain a barrier to resolving the issue of middle opacity. This suggests that without improved multilateral regulatory cohesion, the US will likely continue to excel at

[133] Berger, "A House Without Foundations," 17; Lampinen, "Russia-DPRK Relations," 4; Blank, "The North Korean Factor," 38; c.f. UN Security Council, *Report of the Panel of Experts (S/2024/211).*

identifying the start and end points of networks while remaining strategically blinded to middle-network actors.

5.3 Procurement & Predicate Offenses

The prevalence of crypto-laundering in the dataset is significant and could serve two non-exclusive functions: obfuscation of the origin of funds, and/or maximizing value prior to cash-out. Large transfers through the fiat banking system trigger KYC and AML requirements, bringing legal or regulatory scrutiny. By contrast, transactions routed through mixers, exchanges, and other decentralized platforms are harder to trace and subject to different, often less comprehensive or less readily enforced, regulations. Virtual funds can be split and routed through numerous wallets and addresses with minimal friction, and permissive platforms, such as Tornado Cash, used to lower the risk of detection.

In terms of the value generated by predicate offenses, the significant standard deviation relative to the mean (a coefficient variation of 1.3) demonstrates that VA-PF networks are not characterized by a steady-state accumulation of capital. The distribution is flat despite the wide interval as a result of a small number of events which generated disproportionate gains despite lower-value intrusions being most common. These outlier events provide the bulk of the total value the regime derived from the VA-PF networks in the dataset.

This indicates a calculated risk-reward relationship between the technical set-up of an intrusion and the opportunistic window available to conduct the predicate offense within. Lower-value cases, often initiated through smaller scale intrusions with lower cost of entry (i.e., spearphishing), represent not only a means of fund generation, but also a way to gain and

maintain access to victim systems. While they may not always offer high-payoff opportunities, they provide a longer exploitation window and a means of accumulating "know-how." Conversely, high-impact tactics such as WannaCry ransomware have high potential gains but inevitably collapse the exploitation window upon execution due to their high degree of detectability. Strategically, this means that VA-PF networks do not require high-probability success across all operations to remain viable, and they are also not reliant on persistent low-level accumulation to generate funds.

The observed actor overlaps and high variability in predicate offenses demonstrated by the data, coupled with the form of state-based criminality that defines the DPRKs proliferation strategy, indicate that this behaviour may represent a form of centrally coordinated, distributed research and development. Rather than viewing the predicate offenses and networks as isolated, they can be interpreted as branches of a unified operational system. By maintaining persistent, low-cost presence in the digital environments of potential victims, the system accumulates intelligence and experience. These networks are not just conducting lower-scale predicate offenses or comparatively underperforming; they are also acting as a form of reconnaissance. This allows for the identification of specific structural vulnerabilities or security lapses that, once exploited, enable the extreme scaling seen in the higher-magnitude cases. In this light, the long-tail of the distribution serves a dual purpose: it provides a baseline of minor financial gains while simultaneously subsidizing the latent capacity required to execute a higher-magnitude offense when the window of opportunity arises.

5.4 Currencies

The prominence of VCs in the dataset underscores the extent to which VA-PF has veered away from the traditional financial system. VCs were often exclusively used for the duration of the PF networks activities, and in many cases fiat currencies were primarily employed as a cash-out rather than laundering mechanism. This is expected: VCs cannot be transformed into hard cash directly and must be used to purchase goods of equal value or transitioned into a fiat currency. Where fiat currencies were not employed to some extent, it is reasonable to conclude that the network either cashed out in an unknown or undisclosed way, or that the funds remained digital. Storing funds in the form of VCs may be a rational choice on the part of the network. They are more difficult to trace, attribute, and seize than fiat currencies. Trends in the use of currency across the data indicate that fiat currencies are thus primarily used in VA-PF networks to bridge transactions. They appear as temporary conversions during cash-out or initial stages of investment.

The frequency of currencies that appeared only once and had relatively short lifespans in the digital financial ecosystem is consistent with an empirical pattern of an opportunistic adoption of currency. There are four potential explanations for this behaviour. First is experimentation: use of tokens to test laundering paths or their compatibility with the design of a network. Second is volatility exploitation: volatile VCs mean a malicious actor can claim a loss in value, or sudden increase in funds to justify unusual, identified flows. Volatility also offers opportunities to maximize funds, in addition to making forensic interference harder. Constant value changes may make it more difficult to accurately trace funds. Third is resource

diversification: spreading funds across a wide variety of coins, particularly emerging tokens or those with low adoption rates, may complicate identifying and seizing them. Finally, is ease of adaptation and transfer: Tokens may be used only to confuse enforcement and regulatory efforts and then dumped or abandoned.

The dominance of VCs within the dataset signifies a move toward an ecosystem where fiat currency is relegated to a terminal bridge rather than a central laundering mechanism. By maintaining funds in a digital state for the majority of the network lifecycle, the DPRK maximizes the criminogenic potential of VAs. This represents a rational strategic pivot away from traditional modalities of PF, which rely on fiat currencies. Further, the rapid turnover and disposable nature of many VCs observed in the dataset highlight a form of tactical opportunism that, intentionally or not, complicates interdiction. Together, the currency trends position DPRK VA-PF networks as both constant and fluid; while the intent and triadic structure remain similar, the assets involved do not.

5.5 Case Study Takeaways

5.5.1 The 2019 Pyongyang Blockchain & Cryptocurrency Conference

What distinguishes this case from conventional PF typologies and others found in the dataset is the absence of a monetary transaction; instead, the primary commodity was technical expertise. Actors such as Emms and Griffiths function as brokers, of both knowledge and access

to parts of digital markets.[134] In this case, they provided reputational resources, technical expertise, and market access that would allow the DPRK to bypass regulatory and enforcement obstacles rather than funds. This case sheds light on an epistemic dimension of PF that is currently unaccounted for by CPF frameworks: the transfer of enabling capacity.

The transfer of knowledge leaves minimal or no trace. Once intellectual diffusion occurs, it becomes an invisible asset that is nearly impossible to interdict, freeze, or sanction. These brokers provide expertise and access required to reproduce and scale VA-PF. Case files also indicate that none of the three involved actors received financial compensation, which suggests that they were motivated by ideological or reputational incentives. For law enforcement, such actors may be difficult to deter through conventional mechanisms such as financial penalties or incarceration. Consequently, the case introduces the possibility that the opaque middle of the observed networks may not be attributable only to technology or geography; but professionalized evasion.

5.5.2 Marine Chain Token

Although enforcement efforts prevented Marine Chain Token from maturing, and it comprised a relatively small part of the overall proliferation network, it nevertheless represents a qualitative evolution in the DPRK's VA-PF strategy. Rather than exploiting existing platforms, the network was moving toward the creation of indigenous VAs for the regime. This is more

---

[134] For further research on professional intermediaries, see: Nicholas Donaldson and Christian Leuprecht, "Geopolitics of State Capture: Systemic Corruption as a Professional Service," in *The Financial War on Crime and Terrorism*, ed. Doron Goldbarsht, Louis de Koker, and Jamie Ferrill, European Yearbook of International Economic Law (Cham: Springer, 2025), 166; 172, https://doi.org/10.1007/978-3-032-06360-1_8.

than a tactical shift in fundraising behaviour; it represents a novel form of state-sponsored criminality.

From a structural standpoint, the creation of indigenous tokens would allow the regime to minimize attribution risk. By manufacturing their own financial instruments, the DPRK would be engaging in a form of weaponized interdependence previously only accessible to Enforcers. They could leverage global appetite for digital innovation and the decentralized nature of VCs to embed illicit-state-sponsored digital finance into the legitimate financial flow of target countries.

This indicates that the threat VA-PF poses to financial integrity may evolve. Transparency may cease to be a matter of tracing the theft of existing capital and instead become an issue of identifying the ontological legitimacy of the capital itself. If the DPRK can manufacture indigenous VAs, it can create a synthetic legitimacy for funds that move through its VA-PF networks by ensuring they have no traceable illicit history. In short, the DPRK may not merely be exploiting existing vulnerabilities in global financial flows, but actively seeking to manufacture new ones.

5.6 Synthesis: What Was & Was Not Observed, & Why It Matters

This analysis gives rise to three critical insights regarding the transformative potential of VA-PF.

5.6.1 The Collapse of the Generation and Laundering Stages

As discussed previously, money-laundering based crimes typically have three stages: generation, laundering, and integration. The DPRK VA-PF networks collapse the first of these two traditionally discreet stages into a single activity.

In conventional illicit finance, the acquisition of funds and subsequent process of disguising and operationalizing them are distinct phases.[135] Even in cases of crypto-money-laundering, these stages have been characterized as distinct.[136] The data presented in this thesis, however, indicates a functional merger. The actors involved in the predicate offenses, which provided the initial influx of funds for the network, were often the same individuals or groups responsible for routing, aggregating, and obfuscating those VAs during the laundering phase. Two profound implications for operational efficiency arise from such overlap, which together merge the first two stages of the laundering process.

First is cyber-enabled value creation, whereby the predicate offense itself is a mechanism of value creation and infusion into the network. It bypasses the need to divert funds from the licit financial system through either a legal or illegal channel. Second is built-in obfuscation. The acquisition of VAs via a predicate offense provides an initial layer of obfuscation not present in acquisitions of fiat currency. This allows laundering to begin concurrently with the process of generating funds.

---

[135] Kelpi & Nasir, "Money Laundering," 33-34; Tiechmann, "Recent Trends," 3; Gilmour et al., *Reexamining the PLI Model,* 113.

[136] Calafos & Dimitoglou, "Cyber Laundering," 2.

Merging these stages minimizes operational friction and reduces attribution risk. Further, it represents the transformative power of VAs to fundamentally alter the nature of PF as it is currently imagined by enhancing network speed, scale, and precision.

5.6.2 Off-Ramping as a Primary Interdiction Point

While the observed networks overwhelmingly favoured VAs as a mode of currency, the data indicates that off-ramping remains a necessity. Off-ramping describes the process of converting VAs into useable fiat currency. It is the primary point of interaction between VA-PF networks and the traditional financial system. This situates off-ramping as a unique and important site for law enforcement interdiction applicable across networks, regardless of currency or the antecedent laundering process.

While the data indicates that VAs are stored, seized, or transitioned into fiat currency, it does not show a widespread, internalized state off-ramp mechanism. This is supported by evidence of networks relying on external, low-tech conversion methods. Mechanisms included ATM cash-outs, over-the-counter brokers, and gift card purchases. In several cases of successful interdiction, VAs were seized before they could be off-ramped. When VAs were not seized, networks were identified as a result of the off-ramping process. When the ultimate fate of the funds was unclear, the mechanism and/or existence of an off-ramping process emerges as the likely point of ambiguity. Importantly, off-ramping need not occur immediately; funds can remain in the cycle of storage and laundering indefinitely. Continued storage and laundering of VAs can potentially function as a source of speculative profit or a hedge against inflation for the regime, providing an incentive to delay or avoid off-ramping. However, absent a widespread,

easily accessible VA-based financial architecture and trade system, turning VAs into real-world value still necessitates conversion. At some point, reliable systems for proliferation-related procurement require liquidity that VAs cannot provide. This trend suggests that while the DPRK is well-versed in generating and moving VAs, the complex, regulated, and geographically constrained act of transferring those values into hard currency represents a persistent vulnerability.

5.6.3 Institutionalization & External Reliance Dynamics

As noted earlier, the recurrence of actors, infrastructure, and network elements across cases demonstrates that DPRK VA-PF is an institutionalized, organized effort. Currently, such institutionalization manifests as a joint effort of self-sufficient infrastructure (cyber actors, predicate offense perpetrators, etc.) at the beginning of networks, and a strategic and repeated exploitation of external platforms and actors as networks expand. The networks exhibit a high degree of internal organization that is dedicated to leveraging decentralized pathways and regulatory gaps. This indicates that organizational capacity is not necessarily a limiting factor, but the amount of time, expertise, and new technology required to move away from external reliance in some areas may be.

However, the DPRK seems to be aiming to rectify this limitation. The two selected case studies demonstrate an attempt to internalize technological expertise and develop cyber-infrastructure that eliminates heavy reliance on external actors while also limiting exposure to the risk associated with high-profile cyberthefts. Such an effort indicates a longer-term aim to create a fully self-sufficient model of VA-PF: to identify weak points and mechanisms through

which they can be rectified may shed light on what the DPRK may do next. That gives some predictive traction to enforcement.

Chapter 6: Implications

Having established the observations and analytic value provided by the dataset in Chapters 4 and 5, this chapter contextualizes the significance of these findings. It articulates contributions to academic literature across data, methods, and theory, and derives practical, data-driven implications for global CPF policy and institutions. The findings ultimately frame the limits of the existing CPF regime as a symptom of a larger, systemic shift in financial power, driven by the adoption of VAs in PF. The findings are interpreted through the E/S/C framework introduced in Chapter 2.

6.1 Theoretical Contributions & Comparative Analysis

The findings of this thesis offer three distinct contributions to the literature on illicit finance, international relations, and proliferation.

6.1.1 Empirical & Methodological Innovation

This study developed the first structured dataset of VA-PF cases. It shifts the study of PF beyond qualitative typologies and descriptive evidence towards systematic empirical inquiry. The application of a replicable methodology adapted from a pre-existing model that was designed to study another kind of illicit network demonstrates that it is feasible and achievable to apply methods across illicit finance research. Further, the codification and analysis in this thesis and the associated dataset provide a foundation for future comparative work, both methodologically and theoretically. Coding variables that are relevant to cyber-infrastructure and the study of attribution rates represents a new mechanism to investigate other cyber-enabled

financial crimes in addition to VA-PF, and to quantify previously intangible but known aspects of these crimes. In grounding VA-PF empirically, this thesis contributes to central debates in the PF literature related to the adoption of VAs and provides insights into scale, mechanisms, and trends in the North Korean case.

Specifically, this thesis resolves the 'evidence paradox' identified in Section 2.2.2. The empirical observations presented in Chapters 4 and 5 do more than validate the scholarship suggesting that VAs are likely to be adopted by proliferators; they also weaken the counter-position, which posits that technological hurdles and high-risk criminality will prevent VA integration into PF networks. By demonstrating that these hurdles are not only being overcome by the DPRK but are also being weaponized to support evasion and obfuscation tactics, this thesis demonstrates that the risk-calculus of proliferators has been significantly underestimated in the literature.

6.1.2 Comparatives with Conventional PF

No structured dataset of traditional PF cases is available to conduct a genuine comparative analysis. However, the extant literature has identified core elements of conventional PF mechanisms and characteristics through qualitative case studies and typologies. This analysis draws from elements and insights identified by this thesis to enable a broad comparative overview of conventional and VA-PF. Both forms of financing rely on intermediary layering and jurisdictional dispersion. The results demonstrate a particular reliance on offshore facilitators (although both the literature and dataset indicate that, in the case of North Korea, such

facilitators may still be agents of the Kim regime).[137] Preliminary differences appear to lie primarily in mechanisms of transfer, the kinds of intermediary layering employed, and points of exploitation.

Conventional PF primarily exploits weaknesses within existing institutions. PF circumvents whole institutions or regulations through disguise (i.e., shell companies), complicity, and fraud (i.e., falsified trade records).[138] VA-PF, by contrast, exploits the absence of these institutions and regulations. Functionally, this substantiates that VA-PF networks are decoupling from significant portions of the global banking system.

Conventional PF transfers that once required complex, multi-layered structures of deception and carried high levels of detection risk as a result can now be executed in minutes, across multiple jurisdictions through VA-PF, using tokens and channels adopted for single transactions and then abandoned.[139] This inversion of speed and traceability complicates enforcement efforts and signifies a significant divergence in the laundering purpose, away from simply avoiding discovery and towards minimizing the window for interdiction itself.

VA-PF in the dataset relied almost exclusively on aggressive cyber operations for capital accumulation, whereas in conventional PF, passive fund accumulation seems more common (i.e.,

---

[137] Drame, Toler, & Pepper, *Forensic Analysis,* 5; Bechtol Jr., "North Korean Illicit Activities," 66; Kassenova & Early, *Countering the Challenges,* 23-26; Brewer, "Study of Typologies," 41-62.

[138] Bechtol Jr., "North Korean Illicit Activities," 63, 66; Kassenova & Early, *Countering the Challenges,* 23-26; Brewer, "Study of Typologies," 41-62; Drame, Toler, & Pepper, *Forensic Analysis,* 5.

[139] Drame, Toler, & Pepper, 5; Kassenova & Early, *Countering the Challenges,* 23-26; Brewer , "Study of Typologies," 41-62; see, as an example of complexity in traditional PF networks, FATF, *Typologies Report,* 5.

via front companies or worker scams).[140] This indicates a more offensive approach, which requires not only a greater initial investment (in developing expertise, technology, and intelligence gathering) but also demonstrate a higher risk tolerance in VA-PF networks than in conventional ones. Despite the high potential for attribution of large-scale cyber thefts/attacks, the DPRK continues to use them as a primary procurement method. This indicates confidence in both the network's ability to launder "hot" VAs, but also in the inability of enforcers to interdict at the level necessary to disrupt these activities. Further, continued, aggressive targeting of high-level targets indicates a speed and scale in procurement that is absent in most conventional PF networks. A single, successful cyber-heist can yield millions instantly, whereas means commonly associated with conventional methods rely on a slower, more incremental accumulation.[141] This functionally shifts the dynamic of risk: instead of primarily being concerned with flow-risk, where the risk is detecting patterns over time, VA-PF procurement introduces an event-risk, where the risk of detection largely rests on a single, high-impact event.

The acquisition of funds via a predicate offense such as cyber-theft that also acts as an initial layer to obfuscate, which allows laundering to begin concurrently with fund generation, represents a fundamental transformation in the PF process. Whereas cases of conventional PF seem to require stages of procurement and layering,[142] VA-PF collapses these stages, marking a

---

[140] Kassenova & Early, *Countering the Challenges,* 23-26; Brewer, "Study of Typologies," 41-62; Drame, Toler, & Pepper, *Forensic Analysis,* 5.

[141] Drame, Toler, & Pepper, 5; Kassenova & Early, *Countering the Challenges,* 23-26; Brewer, "Study of Typologies," 41-62.

[142] See, for case examples, Brewer, "Study of Typologies," 41-62.

shift away from the traditional money laundering process entirely and towards a new typology of illicit finance.

6.2 Theoretical Implications: The E/S/C Framework & The Digital Power Shift

The rise of VA-PF in the DPRK represents a larger, fundamental change in the strategic geometry of the E/S/C framework. That shows a theoretically novel insight: emerging technologies can trigger international power re-distributions.

6.2.1 Enforcers & the Degradation of Deterrence

Enforcers derive their power in large part from control over fiat currency systems and chokepoints. A pivot by PF networks to VAs bypasses these systems by design. The leverage of the Enforcer is reduced when the traditional financial system is bypassed in whole or large part: Enforcers now have nothing of which to deprive proliferators. This translates into a reduction of deterrent power and the coercive degradation of traditional financial statecraft on the part of the Enforcer.

This thesis contends that the role of the Enforcer remains viable, but it must shift its power-reliance from mere network centrality (physical control overflows) to incorporate data centrality (control over information about flows). While VAs need not pass through most elements of the traditional financial system, the data presented in Chapters 4 and 5 show that off-ramping remains critical to these networks, which makes it a primary interdiction point. Enforcement capacity must be re-centered to prioritize technological reach and information-gathering focused on conversion points rather than just transfer points. Such leverage is not as

all-encompassing as what the Enforcer possesses in the current CPF system, but it is crucial to ensuring that the Enforcer retains power to disrupt and deter.

6.2.2 Shields: VAs as Opportunity

At first glance, VAs render Shields almost unnecessary. They provide a more secure, expansive range of benefits than the benefits of selective compliance that Shields currently provide. However, they also offer a new opportunity for Shields to aggregate power and move beyond their current function in the E/S/C framework.

Strategically, Shields may be agnostic about VA enforcement and regulation where the core characteristics of VAs – such as decentralization – align with the national interests of the Shield. To do so would be an extension of the already demonstrated selective compliance and passive enforcement paradigm by which Shields currently operate. In doing so, digital safe harbours may be introduced to facilitate the movement and conversion of VAs, particularly in the off-ramping process. The middle network opacity highlighted in Chapter 5 demonstrates that the DPRK's VA-PF networks are likely already exploiting these harbours. Maintaining such leverage over proliferators and sidestepping the Enforcer-dominated financial system is in the interest of the shield. Wider VA adoption in illicit finance and society more broadly may also incentivize exploration and development of alternative, non-USD-centric financial mechanisms to further the goals of the Shield. Such developments are already emerging (i.e., the BRICS

framework)[143] and the creation of such a financial ecosystem is not only inherently shielding but also confers a level of enforcement power to Shields.

VAs confer immediate benefits: they allow the Shield to maintain plausible deniability to a much higher degree. They offer a means of demonstrating formal compliance with sanctions, which increases plausible deniability, while still permitting circumvention simply by failing to adopt stringent VA regulation. Additionally, the reduced power of Shields created by VA-PF means that their dampening effect in the Resistance-Amplification Cycle is also reduced. This has serious implications for Enforcer/Challenger dynamics.

6.2.3 Challengers & the Power-Accumulation Cycle

VA-PF gives Challengers a significant advantage. Decentralized, peer-to-peer VA networks impart autonomy for Challengers engaging in direct proliferation or facilitation. They reduce dependence on traditional financial conduits, thereby reducing both the power of Enforcers and reliance on Shields that limits bad behaviour by Challengers. This shift in dynamic is the fundamental power re-distribution that is observable in the E/S/C framework: *The Power-Accumulation Cycle*, which is an evolution of the Resistance-Amplification Cycle. The Power-Accumulation Cycle, informed by conceptions about the distribution of power put forward by theorists such as Max Weber, posits that Enforcers' loss of power accrues to Challengers.[144] This

---

[143] Svetlana Gusarova, Igor Gusarov, and Margarita Smeretchinskii, "Building a Digital Economy (The Case of BRICS)," *International Scientific and Practical Conference* 106 (2021): 6, https://doi.org/10.1051/shsconf/202110601019.

[144]See, for relevant grounding discussion on power struggle and power distribution in international relations, Hans J. Morgenthau, *Politics among Nations: The Struggle for Power and Peace* (Alfred A. Knopf, 1948);

accumulation loop is directly enabled by the characteristics of VA-PF. The decentralized, pseudonymous nature of VAs largely replaces the power of Shields, acting as a perpetual, one-sided, dampening effect. Shields still remain part of the cycle, but are liberated from their passive, defensive role and can act as strategic pivots that can modulate their compliance to bargain for political leverage or even oscillate between the roles of Challenger and Enforcer without losing the inherent protective advantage of being a regulatory sanctuary

VA-PF exponentially increases the probability that Challengers will successfully engage in evasion despite Enforcer resistance. These enforcement failures then actively inform subsequent Challenger behaviour, the success of which further damages the structural authority and leverage of the Enforcer. If repeated over time, this translates to a cumulative reallocation of hard power: as the probability of stopping Challengers declines, the balance of power gradually and increasingly favours them. This will enable Challengers to pursue revisionist agendas more freely and with higher potential for success. That cements a vicious cycle where power feeds power as the international order changes.

In essence, the E/S/C framework demonstrates the VA-PF is transformative; viewed looking inward from outside of the system-internal logic that grounds policy and scholarship, it forces a redistribution of power that would otherwise appear to be a mere diffusion. This then allows us to draw conclusions about the impact of such redistribution: the transformative

Max Weber, *Politics as Vocation*, trans. H. H. Gerth and C. Wright Mills (Oxford University Press, 1946); Max Weber, *Economy and Society: A New Translation*, ed. and trans. Keith Tribe (Harvard University Press, 2019).

potential of VAs in the digital arena translates to tangible hard power outcomes in international dynamics of coercion and deterrence.

6.2.4 Implications of the E/S/C Framework for Academia

These findings challenge the pervasive tendency of the literature to model PF as a series of tactical adaptations within a fixed financial architecture. This thesis has argued that such a lens creates an epistemological blindness in academia, where the full scope of the transformative potential of VAs is obscured by the implicit assumption that the ontological backdrop of financial control will remain constant. Through the E/S/C Framework, this thesis illustrates that VA-PF is not a form of system-internal evasion, but a move toward a new paradigm of illicit finance that fundamentally minimizes reliance on legacy infrastructure. While conventional scholarship has modeled adaptation as a series of actions within given relationships, the E/S/C framework reveals the potential of VAs to fundamentally reconfigure those relationships and their dynamics. The qualitative case studies presented in Sections 4.2 and 5.5 further substantiate this, showing that proliferators like the DPRK are actively working to resolve any remaining dependencies on the legacy system. In doing so, Challengers like the DPRK are not just hiding from the Enforcer through new Shields; they are seeking to exit the Enforcer's sphere of structural influence entirely.

Further, the Power-Accumulation Cycle provides a theoretical expansion to the resolution of the debate around VA adoption discussed in Section 2.2.2. While the data presented in this thesis empirically reinforces the position that VAs possess criminogenic attributes that will incentivize their adoption by proliferators, the PAC offers a further contribution to the literature.

It demonstrates that VAs facilitate more than an enhancement of existing PF processes. They also offer opportunities to reconfigure the structural distribution of power within the CPF regime by rebalancing the ratio between evasion capacity and enforcement authority within the international system. This finding necessitates a pivot in academic conversation away from narrow study of compliance and evasion and toward a more profound investigation of financial de-territorialization and the implications of erosion of state monopoly on value-transfer oversight.

6.3 Policy Implications & Directives

The empirical findings and theoretical implications give rise to short and long-term possibilities for the global CPF regime and key actors at the multilateral and domestic level.

6.3.1 Multilateral Implications

The dataset illustrates both an opacity gradient in actor attribution levels as proliferation networks extend their reach, and highlights the typological merge of two fundamental elements of the money laundering process: generation and layering. Designed for application to the movement of goods and fiat currencies, current regulatory instruments cannot easily capture the instantaneous and ephemeral nature of VA transfers and decentralized finance systems. This necessitates two policy shifts in relation to the CPF framework, and the multilateral institutions involved in its design:

First, the FATF and UN will need to transcend a model of financial regulation and CPF enforcement that is primarily based in nation-states, or explore entirely new alternatives. Doing

so lowers the burden on Enforcers to maintain a system that VA-PF typology is designed to bypass. It enables them to prioritize data-centrality and new regulatory approaches aimed at maximizing opportunities to interdict VAs. Furthermore, Enforcers cannot remain responsible for rectifying the issue of regulatory asymmetry. Expectations of Enforcers being able to leverage all other states into compliance are unrealistic and exacerbate tensions between Enforcers and Challengers unnecessarily by incentivizing aggressive tactics and jurisdictional overreach. Reduced reliance is especially important given the possible implications of the Power-Accumulation Cycle. By diversifying away from Enforcer-centric CPF, power can be proactively redistributed to actors that are engaged in supporting the mission of the Enforcer, thereby reducing the power Challengers can accumulate directly from Enforcers.

Second, and following this initial shift, the dissonance of enforcement created by fragmentation among the FATF's soft-law framework, the UN's binding but slow-moving sanctions apparatus, and national-level CPF regimes must be rectified. This fragmentation diminishes coherence across jurisdictions and contributes to both regulatory arbitrage and the uneven distribution of regulatory responsibility to Enforcers. Replacing the multilateral architecture or reforming the UN and the FATF to offset the structural issues that pose the largest barriers to effective countering of VA-PF is not practical. Instead, this thesis suggests the formation of an adaptive layer that is capable of bridging normative and operational divides between the multi and unilateral layers of CPF. One such manifestation would be a semi-autonomous, intergovernmental consortium modeled on entities such as the Proliferation

Security Initiative,[145] but directed specifically at VA-PF. This would enable FATF standards and UN resolutions to be operationalized and interpreted in a harmonized manner through cooperative intelligence-sharing and joint enforcement efforts. That would reduce lag without undermining institutional legitimacy. Additionally, a layer of insulation may prevent certain structural weaknesses in multilateral institutions (i.e., veto power on the UNSC) from having a negative trickle-down effect.

At the same time, the UN and the FATF must pivot away from relying solely on financial penalties and economic consequences for PF activities. The research indicates that this does not incentivize compliance in cases such as the DPRK's and may actually do the opposite.[146] Instead, these institutions must find ways to build a deterrent architecture. The under-regulation of VAs thus becomes a benefit. Deterrence capacity can be built into the regulatory framework, rather than added retroactively. That the potential of VAs is still emerging and not fully realized is also a benefit. If designed to be future-facing and flexible rather than unnecessarily prohibitive, such efforts are unlikely to be shut down immediately by Challengers or counter current imperatives of Shields. They thus present a more viable option that continued build-up of the multilateral sanction regime for managing VA-PF at this moment in time.

---

[145] For more, see Habib, "The Enforcement Problem," 57; Haggard & Nolan, "Sanctioning North Korea," 20; United States Department of State, Bureau of International Security and Nonproliferation, "Proliferation Security Initiative," accessed January 2, 2026, https://www.state.gov/bureau-of-international-security-and-nonproliferation/proliferation-security-initiative.

[146] Frank, "Political Economy of Sanctions," 12, 17, 31; Habib, "The Enforcement Problem," 51-52; Haggard & Nolan, "Sanctioning North Korea," 21, 23; Jessen, "Sanctions Compliance," 571; Brooks, "Sanctions and Regime Type," 17.

6.3.2 Redefining the Public-Private Boundary of Enforcement

Decentralized financial systems and VAs rely on privately operated infrastructure; private developers, engineers, and operators are crucial gatekeepers that are currently unaccounted for in the CPF regime. Future CPF efforts must recognize these private actors as more than subjects of compliance. They are active participants in financial governance, with the power to shape both norms and accessibility of digital domains and tools. Intelligence in illicit finance is already increasingly derived from or made feasible by private actors, such as blockchain analytics firms.[147] The boundary between public and private enforcement is thus already blurred in relation to VAs. This necessitates new cooperative efforts aimed at countering VA-based illicit finance broadly.

6.3.3 Enforcement Directives

The data and observations of this thesis present two significant opportunities for refining future interdiction efforts: a revision of the sequential risk model, and a shift from flow to event-based risk assessments and response.

Traditional CPF models assume a sequential, three stage process: procurement/placement, layering, and integration. This structure presumes multiple, discrete opportunities for disruption. VA-PF has effectively collapsed the traditional sequence. This

[147] See, for example, Chainalysis, "How Chainalysis Helped the FBI Track Down and Freeze Millions in the Caesars Casino Ransomware Attack," *Chainalysis Blog*, June 6, 2025, accessed December 15, 2025, https://www.chainalysis.com/blog/chainalysis-fbi-caesars-ransomware-recovery/.

structural transformation and the resulting erosion of established detection windows necessitates immediate, feasible shifts in enforcement directives: regulation and enforcement must de-emphasize placement controls. The observed data demonstrates that entry points into the traditional financial system are largely obsolete in VA-PF; interdiction of network funds at these entry points is thus ineffective. Instead, efforts should concentrate on interdiction at off-ramping points, which remain the most visible point of interaction between VA-PF networks and the regulated economy. Updating extant financial regulation and policy to reflect red-flag behaviours associated with known off-ramp activities, such as ATM cash-outs, should be the priority.

Preliminary comparison indicates that conventional PF has relied on slow, incremental methods of accumulation. That creates a substantial temporal window for financial intelligence, enforcement agencies, and financial institutions to detect and freeze assets as they flow through the network. VA-PF networks have drastically shrunk the window to interdict at the procurement stage through cyber-enabled predicate offenses. That complicates efforts further by acting as both a mechanism of procurement and initial layering step in the network. The shift of risk from a flow to event-based metric necessitates areas of priority for enforcement: speed and forensic capacity, cross-jurisdictional response, and targeting of core infrastructure.

First, with a limited window for interdiction in the initial phases of VA-PF, enforcement must prioritize the development of high-speed, forensic models for detection and response. This necessitates substantial investments in blockchain analytics, cooperation with blockchain developers and VA platforms (that also constitute potential targets), and synergy with policymakers responsible for setting the limits of available response mechanisms.

Second, the borderless, instantaneous nature of the movement of VAs means that successful responses must be measured in hours, not days or weeks. Prioritization of high-speed cross-border data sharing among financial intelligence units, law enforcement, and the private sector is needed to identify lost assets, involved actors, and potential points of off-ramping, which seems to be geographically opportunistic and, therefore. may prove difficult to predict without such cooperative systems in place.

Finally, the DPRK's preference for high-level cyber operations as predicate offenses indicates a highly specialized infrastructure. Repeated use of actors and digital resources across the dataset suggests that this infrastructure remains limited. Enforcement should focus on dismantling the digital resource pool from which these networks draw, along with identifying and disabling core actors to limit the capability of both current and subsequent proliferators.

Such shifts are relatively feasible. Making small, precise changes based on evidence will be integral to success in developing regulatory, policy, and enforcement systems capable of meeting the VA-PF challenge.

6.4 Summary

The implications of VA-PF speak to a structural contradiction at the core of the global CPF regime: a system designed to counter known typologies and work within a familiar financial ecosystem is increasingly being confronted by emerging and decentralized networks. Within such an environment, traditional power dynamics are no longer upheld by CPF frameworks. The redistribution of power alters the balance of coercion and compliance that sustains the existing order and makes current CPF efforts increasingly outdated. Addressing this transformation does

not require dismantling the CPF regime; it necessitates reconfiguration of it. The capacity to realize such reconfiguration before technological evolution renders these insights obsolete will define how the international financial order of tomorrow looks.

Chapter 7: Conclusion

7.1 Summary of Contributions & Findings

The North Korean nuclear project has long been understood as a product of isolation and survival. This research demonstrates that the persistence of the Kim regime's nuclear program cannot be explained solely by military logic or ideological rigidity. It also reflects an economic strategy of adaptation. VAs in the North Korean context do not merely supplement existing proliferation mechanisms; they transform them. Historically, the DPRK's ecosystem of illicit finance has relied on front companies, overseas trading, and smuggling.[148] The introduction of VAs is an evolutionary leap; the same structural conditions that drove the DPRK toward criminal enterprise to generate revenue – sanctions and surveillance – also incentivized the development of cyber capabilities.[149] VAs are the perfect tool for a state that is already compelled toward autonomy and skilled in obfuscation.

North Korea demonstrates how VAs can shift PF from material and transactional systems to decentralized, digital ecosystems. That redefines our understandings of proliferation and sanction evasion, and associated ways to prevent, detect, and enforce against it. Beyond documenting North Korean ingenuity and offering prescriptions for the future of CPF, this thesis also provides a fresh analytical lens to IIPE and PF scholarship. It counters the prevailing

---

[148] Drame, Toler, & Pepper, *Forensic Analysis,* 5; Brewer, "Study of Typologies," 41-62; Kassenova & Early, *Countering the Challenges,* 23-26; FATF, *Typologies Report,* 9-11.

[149] Frank, "Political Economy of Sanctions," 20, 30; Wronka, "Digital Currencies," 1274; von Soest, "Authoritarian Regimes," 11-12.

assumption of a static financial control system, demonstrating that PF has evolved beyond tactical adaptation within fixed bounds; VAs are a system-transformative shift.

Is the current CPF system effective in constraining the DPRK's nuclear ambitions when VAs are employed as a financing mechanism? The logic of coercion presupposes that isolation produces compliance. The DPRK has transformed isolation into innovation. In such a case, deterrence loses its punitive power, and the targeted state adapts by way of substitution.

The dataset constructed from this research reveals a pattern of adaptation that redefines how proliferation is funded, concealed, and sustained when VAs are integrated. The findings discussed in Chapters 4 and 5 demonstrate that the DPRK's use of VAs is not merely an extension of existing proliferation activities, but also structural innovation. VA-PF draws strength from the decentralization that regulators struggle to control. This underscores the urgency of rethinking CPF not just as a regulatory challenge, but as a contest in which proliferators and regulators continuously reshape the boundaries of financial control, visibility, and accessibility in response to each other's behaviour.

This thesis shows how the DPRK exemplifies the convergence of cyber and financial innovation in PF; how VAs enable and drive proliferation evolution; and how VA use exposes structural and conceptual limits in existing regulatory systems.

7.2 Directions for Future Research

This study indicates several directions for future research. These efforts would complement the work of this thesis, expand PF research in new directions, and open opportunities for continued inquiry on the topic of VA-PF.

7.2.1 Comparative Studies & Dataset Development

This thesis shows how the DPRK exemplifies the convergence of cyber and financial innovation in PF; how VAs enable and drive DPRK proliferation evolution; and how VA use by the DPRK exposes the limits of current scholarship, which remains focused on a banking-centric model of control that is increasingly structurally indeterminate. While the dataset contained in this thesis focused exclusively on the DPRK and VA-PF, structured comparison with other known proliferators is necessary to evaluate whether observed VA-PF dynamics are unique to North Korea or represent broader systemic trends. Comparing conventional and VA-PF across a variety of states offers opportunities to examine divergences in trends between the two forms of PF. Such cross-case comparatives would clarify the extent to which VA-PF differs from known behaviours of proliferation, assist in establishing empirical foundations for future PF research, and offer more nuanced, specific insights for policy makers, law enforcement, and academia.

7.2.2 Expanded Models of Network Analysis

Mapping networks through additional mechanisms such as SNA, Python, or R could further illuminate patterns of relationships in PF networks. This is particularly true if applied to additional or expanded datasets such as that produced for this thesis: analytic potential increases

as available data points increase. The development of open-access, transparent data analysis on PF offers opportunities to align policy development with academic inquiry, offering opportunities for cross-disciplinary collaboration and the translation of academic findings into actionable recommendations.

7.2.3 Token Lifecycle & Asset Flows

The dataset revealed a wide range of VCs employed by PF networks. Currency liquidation patterns may present an opportunity to develop diagnostic indicators of VA-PF. Tracing correlations between token generation, liquidity provision, adoption, and drainage may be useful in identifying both ongoing VA-enabled proliferation activities and in recognizing elements that make particular VCs more appealing to proliferators. In short, research into the VCS themselves could potentially shed light on their integration into PF networks.

7.2.4 Re-Evaluation of Regulatory Architecture

The primarily nation-based model of financial regulation, already criticized for both under and overreach in different contexts, is inherently limited in its ability to govern non-territorial financial systems such as cryptocurrency and decentralized finance.[150] Future scholarship might explore potential alternatives or paths for adapting this model to reconcile the need for sovereignty in regulatory frameworks and financial systems with the de-territorialized nature of VCs and cyberspace.

---

[150] Macfarlane, "Strengthening Sanctions," 206-207.

7.2.5 Security Theory & Practical CPF

VAs are strategic equalizers. They democratize access to global finance. This undermines the monopoly of regulated financial systems and incentivizes the development of asymmetric cyber capabilities in sanctioned or otherwise excluded states. Future CPF research would benefit from conceptualizing crypto-crime and VA-PF through the lens of security theory, and expand into IR theory, political economy, and criminology to understand how cyber-enabled illicit finance can be co-opted as a form of statecraft by building out the E/S/C framework presented by this thesis. Bridging theoretical, conceptual, and empirical research from across relevant disciplines helps us to understand the impacts and implications cyberspace and VAs have on international relations. Specifically, research must move away from the 'compliance-evasion' binary that dominates current CPF literature; further inquiry into the limits of state power in an era where value transfer is no longer tethered to geographic chokepoints would be beneficial.

7.3 Concluding Thoughts

While focused on North Korea, the findings derived from this research are not limited to the unique dynamics of North Korea: they serve as an early warning system for the erosion of global financial governance for the international community. The DPRK is best interpreted as a blueprint, not an anomaly.

The typological merger of theft and laundering, combined with cooperation from a Shield or Challenger archetype, indicate a replicable playbook for other sanctioned states or transnational criminal organizations looking to integrate VAs into their illicit finance streams. The ability of VAs to redistribute power, as demonstrated through the E/S/C Framework, offers

incentives to these actors, and highlights the risk of failing to identify, disrupt, and respond to VA-PF. The DPRK's success today can be copied and scaled tomorrow. States subject to less stringent oversight may find it even easier to replicate and succeed in avoiding detection. The North Korean case demonstrates that the boundaries of proliferation are shifting from physical to digital. Through analysis of such an extreme case, the research provides generalizable insights into the nature of modern proliferation and offers actionable recommendations to adapt counter-proliferation strategies.

Conventional tools of coercion and deterrence are designed for a banking-centric world and reaching diminishing returns. The same technologies that empower VA-enabled proliferation can also offer new avenues for regulation, collaboration, and coordination. If the international community cannot evolve extant systems to maximize these opportunities, blockchain will continue to finance the bomb.

References

Anderson, Nicholas D. "Explaining North Korea's Nuclear Ambitions: Power and Position on the Korean Peninsula." *Australian Journal of International Affairs* 71, no. 6 (2017): 621–41. https://doi.org/10.1080/10357718.2017.1317328.

Arms Control Association. "UN Security Council Resolutions on North Korea." Accessed January 14, 2025. https://www.armscontrol.org/factsheets/un-security-council-resolutions-north-korea.

Bank of Korea. *Gross Domestic Product of North Korea in 2008*. Seoul: Economic Statistics Department, 2009. https://www.nkeconwatch.com/nk-uploads/gdp_of_north_korea_in_2008.pdf.

Bechtol, Bruce E., Jr. "North Korean Illicit Activities and Sanctions: A National Security Dilemma." *Cornell International Law Journal* 51, no. 1 (2018): 57–99. https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=1913&context=cilj.

Berger, Andrea. "A House Without Foundations: The North Korea Sanctions Regime and Its Implementation." *Royal United Services Institute Whitehall Report* 3, no. 17 (June 2017). https://static.rusi.org/201706_whr_a_house_without_foundations_web.pdf.

Biersteker, Thomas J., Sue E. Eckert, Marcos Tourinho, and Zuzana Hudáková. "UN Targeted Sanctions Datasets (1991–2013)." *Journal of Peace Research* 55, no. 3 (2018): 404–12. https://www.jstor.org/stable/48595892.

Blank, Stephen. "The North Korean Factor in the Sino-Russian Alliance." *Korea Economic Institute of America,* July 29, 2019. https://keia.org/wp-content/uploads/2020/05/kei_jointus-korea_2019_1.2.pdf.

Blank, Stephen. "Russia's Proliferation Pathways." *Strategic Insights*, December 2008. https://apps.dtic.mil/sti/pdfs/ADA517404.pdf.

Brewer, Johnathan. "The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation." *Center for a New American Security*, January 2018. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/CNAS%20ProliferationFinance.pdf.

Brewer, Johnathan. "Study of Typologies of Financing of WMD Proliferation." *King's College London, Center for Science and Security Studies, Project Alpha*, October 13, 2017. study-of-typologies-of-financing-of-wmd-proliferation-2017.pdf

Brooks, Risa A. "Sanctions and Regime Type: What Works, and When?" *Security Studies* 11, no. 4 (2002): 1–50. https://doi.org/10.1080/714005349.

Burgess, Ariel, Rhianna Hamilton, and Christian Leuprecht. “Terror on the Blockchain: The Emergent Crypto-Crime-Terror Nexus.” In *Financial Crime, Law, and Governance*, Ius Gentium: Comparative Perspectives on Law and Justice, vol. 116, 203–27. Springer, 2024. https://doi.org/10.1007/978-3-031-59547-9_9.

Buzan, Barry. *People, States and Fear: The National Security Problem in International Relations*. Wheatsheaf Books, 1983.

Calafos, Michael W., and George Dimitoglou. “Cyber Laundering: Money Laundering from Fiat Money to Cryptocurrency.” In *Principles and Practice of Blockchains*, edited by K. Daimi, I. Dionysiou, and N. El Madhoun, 271–300. Springer, 2023.

Carlin, Maya. “The Air Force Built 195 F-22s Instead of 750 and Destroyed the Tooling to Make More – Now China Has Exactly the Air Force the Raptor was Designed to Defeat.” *19FortyFive*. March 2026. https://www.19fortyfive.com/2026/03/the-air-force-built-195-f-22s-instead-of-750-and-destroyed-the-tooling-to-make-more-now-china-has-exactly-the-air-force-the-raptor-was-designed-to-defeat/.

Carlisle, David, and Kayla Izenman. “Closing the Crypto Gap: Guidance for Countering North Korean Cryptocurrency Activity in Southeast Asia.” *Royal United Services Institute Occasional Paper*, April 2019. https://static.rusi.org/20190412_closing_the_crypto_gap_web.pdf.

Cha, Victor, and Lisa Collins. “Treasury Department Designates North Korea Under Section 311.” *Center for Strategic and International Studies*, June 1, 2016. https://www.csis.org/analysis/treasury-department-designates-north-korea-under-section-311.

Chainalysis. “How Chainalysis Helped the FBI Track Down and Freeze Millions in the Caesars Casino Ransomware Attack.” *Chainalysis Blog*, June 6, 2025. Accessed December 15, 2025. https://www.chainalysis.com/blog/chainalysis-fbi-caesars-ransomware-recovery/.

Corobana, Adrian. “Financial International Sanctions and Cryptocurrencies: Challenges and Solutions.” *European Business Law Journal* 1, no. 1 (2023): 71–80. https://doi.org/10.24818/EBLJ/2022/1/1.06.

Council on Foreign Relations. “Six-Party Talks and North Korea’s Nuclear Program.” *CFR Backgrounder*. Accessed January 21, 2026. https://www.cfr.org/backgrounders/six-party-talks-north-koreas-nuclear-program.

Cozzi, Fabio. “Will Blockchain Technologies Strengthen or Undermine the Effectiveness of Global Trade Control Regulations and Financial Sanctions?” *Global Jurist* 20, no. 2 (2020). https://doi.org/10.1515/gj-2019-0047.

D’Alessandra, Federica. “Conceptualizing Great Power Perpetrators.” *Genocide Studies and Prevention: An International Journal* 18, no. 1 (2024): 151–89.

https://ora.ox.ac.uk/objects/uuid:800e5170-39cc-485d-9985-1b1baf5b6024/files/rmp48sf11g.

de Koker, Louis. "The FATF'S Combating of Financing of Proliferation Standards: Private Sector Implementation Challenges." In *Financial Crime and the Law*, Ius Gentium: Comparative Perspectives on Law and Justice, vol. 115, edited by D. Goldbarscht and L. de Koker, 123–66. Springer, 2024.

de Koker, Louis. "Supporting the Combatting of Financing of Weapons of Mass Destruction with AI Technologies." In *Proceedings of Artificial Intelligence Governance Ethics and Law (AIGEL)*, 9–21. Barcelona, Spain, 2022. https://ceur-ws.org/Vol-3531/LPaper_02.pdf.

Donaldson, Nicholas, and Christian Leuprecht. "Geopolitics of State Capture: Systemic Corruption as a Professional Service." In *The Financial War on Crime and Terrorism*, edited by Doron Goldbarsht, Louis de Koker, and Jamie Ferrill, 163–182. European Yearbook of International Economic Law. Springer, 2025. https://doi.org/10.1007/978-3-032-06360-1_8.

Drame, Bafode, Lisa Toler, and Katherine Bachner. *Forensic Analysis of Terrorist Counter-Financing to Combat Nuclear Proliferation*. No. BNL-111867-2016. Brookhaven National Lab (BNL), Upton, NY, 2016.

Financial Action Task Force. *Complex Proliferation Financing and Sanctions Evasion Schemes*. Paris: FATF, June 2025. https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/Complex-PF-Sanctions-Evasions-Schemes.pdf.

Financial Action Task Force. *Horizontal Review of FATF Standards on Virtual Assets and Virtual Asset Service Providers*. Paris: FATF/OECD, 2024. https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/FATF-Targeted-Update-VA-VASP-2024.pdf.

Financial Action Task Force. *Guidance: Countering Proliferation Financing*. February 2018. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Countering-Proliferation-Financing.pdf.coredownload.pdf.

Financial Action Task Force. *The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*. Paris: FATF/OECD, 2012 (updated 2023). https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.

Financial Action Task Force. *Combating Proliferation Financing*. Paris: FATF/OECD, 2010. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Combating%20Proliferation%20Financing.pdf.

Financial Action Task Force. *Guidance on the Effective Implementation of Targeted Financial Sanctions Related to Proliferation of Weapons of Mass Destruction*. Paris: FATF/OECD,

2008. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-UNSCRS-Prolif-WMD.pdf.

Financial Action Task Force. *Typologies Report on Proliferation Financing*. June 18, 2008. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf.

Fisher, Tricia, and Daniel White. "Implementing UN Sanctions on Democratic People's Republic of Korea." *Old Dominion University Model United Nations Council Issue Brief*, 2025. https://www.odu.edu/sites/default/files/2025/documents/SC%20North%20Korea%20Sanctions.pdf.

Farrell, Henry, and Abraham L. Newman. "Weaponized Interdependence: How Global Economic Networks Shape State Coercion." *International Security* 44, no. 1 (2019): 42–79. https://doi.org/10.1162/isec_a_00351.

Fox, William T.R. *The Super-Powers: The United States, Britain, and the Soviet Union—Their Responsibility for Peace*. New York: Harcourt, Brace and Company, 1944.

Frank, Ruediger. "The Political Economy of Sanctions Against North Korea." *Asian Perspective* 30, no. 3 (2006): 5–36. http://www.jstor.org/stable/42704552.

Gilmour, Paul, Brian Omondi, H. Feyza Alkac, Bing Han, Abigail Carre, Dina Kapardis, and Cerri Halfpenny. "Reexamining the PLI Model of Money Laundering." *The Institute of Money Laundering Prevention Officers,* 2025. https://brianforensics.com/wp-content/uploads/2024/11/Institute-Report-Reexamining-the-PLI-Model-of-Money-Laundering.pdf.

Gray, Kevin, and Jong-Woon Lee. "Following in China's Footsteps? The Political Economy of North Korean Reform." *The Pacific Review* 30, no. 1 (2017): 51–73. https://doi.org/10.1080/09512748.2015.1100666.

Gusarova, Svetlana, Igor Gusarov, and Margarita Smeretchinskii. "Building a Digital Economy (The Case of BRICS)." *International Scientific and Practical Conference* 106 (2021): 1–9. https://doi.org/10.1051/shsconf/202110601019.

Habib, Benjamin. "The Enforcement Problem in Resolution 2094 and the United Nations Security Council Sanctions Regime: Sanctioning North Korea." *Australian Journal of International Affairs* 70, no. 1 (2016): 50–68. https://doi.org/10.1080/10357718.2015.1095278.

Haggard, Stephan, and Marcus Noland. "Sanctioning North Korea: The Political Economy of Denuclearization and Proliferation." *Asian Survey* 50, no. 3 (2010): 539–68. https://doi.org/10.1525/as.2010.50.3.539.

Harrell, Peter, Elizabeth Rosenberg, and Edoardo Saravalle. *China's Use of Coercive Economic Measures*. Washington, DC: Center for a New American Security, June 2018. https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/China_Use.pdf.

He, Kai, Huiyun Feng, Steve Chan, and Weixing Hu. "Rethinking Revisionism in World Politics." *The Chinese Journal of International Politics* 14, no. 2 (2021). https://doi.org/10.1093/cjip/poab004.

Hymans, Jacques E. C. "Assessing North Korean Nuclear Intentions and Capacities: A New Approach." *Journal of East Asian Studies* 8 (2009): 259–92. https://dornsife.usc.edu/jacques-hymans/wp-content/uploads/sites/323/2023/09/Hymans_JEAS_North_Korea_article.pdf.

Hysa, Xhimi. "Critical Case." In *The SAGE Encyclopedia of Research Design*, 2nd ed., edited by Bruce B. Frey, 356. SAGE Publications, 2022. https://doi.org/10.4135/9781071812082.n130.

Ivanov, E. G., and A. V. Solovyov. "The Erosion of the UN Security Council Sanctions Regime Against the DPRK." *Journal of International Analytics* 14, no. 1 (2023): 67–81. https://doi.org/10.46272/2587-814X-2023-14-1-67-81.

Jessen, Henning. "Multilateral and Unilateral Sanctions Compliance and Challenges." In *Peace, Justice, and Strong Institutions*, edited by W. Leal Filho et al., 570–80. Springer, 2021.

Jun, Jenny, Scott LaFoy, and Ethan Sohn. "North Korea's Cyber Operations: Strategy and Responses." *Center for Strategic and International Studies*, December 2015. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf.

Jung, Giwoong, Kihyun Lee, Won Geun Choi, and Sung Hoon Jeh. "Why Russia and China Advocate Korean Peace-Unification Public Diplomacy?" *Journal of International Relations* 26, no. 2 (2023): 1–28. DOI: 10.22414/rusins.2023.33.1.237

Kassenova, Togzhan, and Bryan R. Early. *Countering the Challenges of Proliferation Financing*. Washington, DC: Center for a New American Security, July 2023. https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/China_Use.pdf.

Kelpi, Mohd Yazid bin Zul, and Maruf Adeniyi Nasir. "Money Laundering: Analysis on the Placement Methods." *International Journal of Business, Economics and Law* 11, no. 5 (2016): 32–40. http://irep.iium.edu.my/65817/1/Analysis%20on%20placement%20methods.pdf.

Kim, Byung-Yeon. *Unveiling the North Korean Economy: Collapse and Transition*. Cambridge University Press, 2017.

Kirkpatrick, Katherine, Christine Savage, Russell Johnston, and Matthew Hanson. "Virtual Currency in Sanctioned Jurisdictions: Stepping Outside of SWIFT." *Journal of Investment Compliance* 20, no. 2 (2019): 39–44. https://doi.org/10.1108/JOIC-04-2019-0019.

Kliene-Ahlbrandt, Stephanie. "North Korea's Illicit Cyber Operations: What Can Be Done?" *38 North*, February 2020. 2020-0228_SKA_NK-Cyber-Operations.pdf

Koen, Vincent, and Jinwoan Beom. "North Korea: The Last Transition Economy?" *Organization for Economic Co-operation and Development Working Paper No. 1607*, 2020. https://one.oecd.org/document/ECO/WKP(2020)15/en/pdf.

Kuik, Cheng-Chwee. "Getting Hedging Right: A Small-State Perspective." *China International Strategy Review* 3, no. 2 (2021): 300–315. https://doi.org/10.1007/s42533-021-00089-5.

Lampinen, Frida. "Russia-DPRK Relations: Implications for the UNSC's Mandate." *Institute for Security and Development Policy Issue Brief*, February 9, 2024. https://www.isdp.eu/wp-content/uploads/2024/02/Brief-Frida-Feb-9-2024-final-.pdf.

Lee, Grace. "The Political Philosophy of Juche." *Stanford Journal of East Asian Affairs* 3, no. 1 (2003): 205–112. https://time.com/wp-content/uploads/2014/12/korea1.pdf.

Leuprecht, Christian, Arthur Cockfield, Pamela Simpson, and Masseh Haseeb. "Tracking Transnational Terrorist Resourcing Nodes and Networks." *Florida State University Law Review* 46 (2019): 289–344. https://www.fsulawreview.com/wp-content/uploads/2022/08/TRANSNATIONAL-TERRORIST-RESOURCING-.pdf.

Macfarlane, Emma K. "Strengthening Sanctions: Solutions to Curtail the Evasion of Sanctions Through the Use of Cryptocurrency." *Michigan Journal of International Law* 42, no. 1 (2021): 199–229. https://doi.org/10.36642/mjil.42.1.strengthening.

Maletova, Olha, Lyudmila Telizhenko, Mykola Starynskyi, M. Dumchykov, and Ruslana Dehtair. "Predicate Offense in Money Laundering Cycle." *Cuestiones Políticas* 47, no. 71 (2023): 23–35. https://doi.org/10.46398/cuestpol.4179.01.

Morgenthau, Hans J. *Politics among Nations: The Struggle for Power and Peace*. Alfred A. Knopf, 1948.

Nuclear Threat Initiative. "Six-Party Talks." *Inventory of International Nonproliferation Organizations and Regimes, Center for Nonproliferation Studies*, May 24, 2012. https://media.nti.org/pdfs/6ptalks_1.pdf.

Office of Foreign Assets Control. "North Korea Sanctions Program." United States Department of the Treasury, November 2, 2016. https://ofac.treasury.gov/media/9221/download?inline.

Office of Management and Budget. *Fiscal Year 2009 Information Technology Budget Overview and Update*. Washington, DC: The White House, 2008. https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/omb/assets/egov_docs/FY09_IT_Budget_Rollout.pdf.

Organski, A. F. K. *World Politics*. Alfred A. Knopf, 1964.

Ougrham-Gormley, Sonia Ben. "Banking on Nonproliferation." *The Nonproliferation Review* 19, no. 2 (2012): 241–65. https://doi.org/10.1080/10736700.2012.690963.

Passas, Nikos. "Financial Controls and Counter-Proliferation of Weapons of Mass Destruction." *Case Western Reserve Journal of International Law* 44, no. 3 (2012): 747–63. https://files01.core.ac.uk/download/pdf/214077663.pdf.

Perlo-Freeman, Sam, Olawale Ismail, Julian Cooper, and Carina Solmirano. "Military Expenditure." In *SIPRI Yearbook 2010: Armaments, Disarmament and International Security*, 181–224. Oxford: Oxford University Press, 2010. https://www.sipri.org/sites/default/files/SIPRIYB201005A.pdf.

Perry, William J. "Proliferation on the Peninsula: Five North Korean Nuclear Crises." *The Annals of the American Academy of Political and Social Science* 607 (2006): 78–86. http://www.jstor.org/stable/25097840.

Salisbury, Daniel. "Spies, Diplomats and Deceit: Exploring the Persistent Role of Diplomatic Missions in North Korea's WMD Proliferation and Arms Trafficking Networks." *Asian Security* 17, no. 3 (2021): 313–30. https://doi.org/10.1080/14799855.2021.1942848.

Sagan, Scott D. "Why Do States Build Nuclear Weapons?: Three Models in Search of a Bomb." *International Security* 21, no. 3 (1996): 54–86. https://doi.org/10.2307/2539273.

Schweller, Randall L. "Bandwagoning for Profit: Bringing the Revisionist State Back In." *International Security* 19, no. 1 (1994): 72–107. https://doi.org/10.2307/2539149.

Struckman, Kara, and Madison Binder. "The Bybit Heist: What Happened & What Now?" Wilson Center, March 31, 2025. https://www.wilsoncenter.org/article/bybit-heist-what-happened-what-now.

Teichmann, Fabian Maximilian. "Recent Trends in Money Laundering and Terrorism Financing." *Journal of Financial Regulation and Compliance* 27, no. 1 (2019): 2–12. https://doi.org/10.1108/JFRC-03-2018-0042.

Twomey, Christopher. "Explaining Chinese Foreign Policy toward North Korea: Navigating between the Scylla and Charybdis of Proliferation and Instability." *Journal of Contemporary China* 17, no. 56 (2008): 401–23. https://doi.org/10.1080/10670560802000167.

Ungboriboonpisal, Ticha. “Efficacy of Economic Sanctions in the Face of Cryptocurrency.” *New York University Journal of International Law and Politics* 55 (2022): 221–35. https://www.nyujilp.org/wp-content/uploads/2023/03/Comment4.pdf.

United Nations. *Charter of the United Nations*. 26 June 1945, 1 UNTS XVI.

United Nations. “Security Council Fails to Extend Mandate for Expert Panel Assisting Sanctions Committee on Democratic People’s Republic of Korea.” Press release, March 28, 2024. https://press.un.org/en/2024/sc15648.doc.htm.

United Nations Security Council. *Provisional Rules of Procedure of the Security Council*. UN Doc. S/96/Rev.7, 1982.

United Nations Security Council. *Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)*. S/2024/221. New York: United Nations, March 7, 2024. https://undocs.org/S/2024/221.

United States Department of State. “Background Note: North Korea.” January 20, 2012. https://2009-2017.state.gov/outofdate/bgn/northkorea/148537.htm.

United States Department of State, Bureau of International Security and Nonproliferation. “Proliferation Security Initiative.” Accessed January 2, 2026. https://www.state.gov/bureau-of-international-security-and-nonproliferation/proliferation-security-initiative.

United States Government Accountability Office. *Defense Acquisitions: Assessments of Selected Weapon Programs*. GAO-09-326SP. Washington, DC, 2009. https://www.gao.gov/assets/gao-09-326sp.pdf.

United States Department of Treasury. *2024 National Proliferation Financing Risk Assessment*. Washington, DC. 2024. https://home.treasury.gov/system/files/136/2024-National-Proliferation-Financing-Risk-Assessment.pdf.

United States Government Publishing Office. “North Korea Sanctions and Policy Enhancement Act of 2016.” https://www.govinfo.gov/content/pkg/COMPS-11985/pdf/COMPS-11985.pdf.

United States v. Jon Chang Hyok, et al. No. 2:20-cr-00614-DMG. Central District of California, 2021.

United States v. Griffith. No. 1:20-cr-00015-PKC. Southern District of New York, 2020.

United States v. Cao de Benos and Emms. No. 1:22-cr-00091-PKC. Southern District of New York, 2022.

Vacusta, Bogdan. "Sanctions Evasion and Virtual Assets: Implications for National Security." *Strategic Impact* 87, no. 2 (2023): 49–65. https://doi.org/10.53477/1842-9904-23-11.

Vincente, Adérito. "United Nations Security Council Reform: The Question of the Veto Power." *United Nations Institute for Training and Research Multilateral Diplomacy Summer School–Student Papers*, 2013, 19–38. https://doi.org/10.13140/RG.2.2.26138.93121.

von Soest, Christian. "How Authoritarian Regimes Counter International Sanctions Pressure." *German Institute for Global and Area Studies*, no. 336 (September 2023). https://pure.giga-hamburg.de/ws/files/49014203/GIGA_WP_336.pdf.

Walt, Stephen M. *The Origins of Alliances*. Cornell University Press, 1987.

Waltz, Kenneth N. *Theory of International Politics*. Addison-Wesley, 1979.

Warf, Barney. "The Hermit Kingdom in Cyberspace: Unveiling the North Korean Internet." *Information, Communication & Society* 18, no. 1 (2015): 109–20. https://doi.org/10.1080/1369118X.2014.940363.

Weber, Max. *Economy and Society: A New Translation*. Edited and translated by Keith Tribe. Harvard University Press, 2019.

Weber, Max. *Politics as Vocation*. Translated by H. H. Gerth and C. Wright Mills. Oxford University Press, 1946.

Wolf, Charles, Jr., and Kamiljon T. Akramov. *North Korean Paradoxes: Circumstances, Costs, and Consequences of Korean Unification*. Santa Monica, CA: RAND Corporation, 2005. https://www.rand.org/pubs/monographs/MG333.html.

World Bank. "GNI (current US$) - United States." World Bank Open Data. Accessed March 13, 2026. https://data.worldbank.org/indicator/NY.GNP.MKTP.CD?locations=US.

Wright, Summer. "The Evolution of Sanctions Evasion: How Cryptocurrency is the New Game in Evading Sanction and How to Stop It." *International Journal of Law, Ethics, and Technology* 1 (2023): 1–25. https://doi.org/10.55574/vohs5203.

Wronka, Christoph. "Digital Currencies and Economic Sanctions: The Increasing Risk of Sanction Evasion." *Journal of Financial Crime* 29, no. 4 (2022): 1269–82. https://doi.org/10.1108/JFC-07-2021-0158.

Zellers, Kole. "Hacked! North Korea's Billion-Dollar Crypto Heisting Scheme." *Penn State Journal of Law & International Affairs* 12, no. 1 (2024). https://insight.dickinsonlaw.psu.edu/cgi/viewcontent.cgi?article=1369&context=jlia.

Appendix A: Variable List and Coding Protocol: VA-PRM[151]

Variable [152]	Type	Definition/Value	Operationalization	Considerations/Coding Choice Notes
Case Name	Categorical	The legal case name (e.g., USA V. John Doe).	Extracted verbatim.	Ensure court record or docket number is included for replicability.
Jurisdiction	Categorical	The official judicial venue.	Extracted verbatim.	If moved through court system/multiple jurisdictions, record court listed in the primary document referenced.
Charges	Categorical	Legal charges being brought by the Crown/defendant against the accused.	Extracted verbatim.	If multiple, list in order of appearance in the legal document in separate adjacent columns (e.g., Charge 1, Charge 2).
Investor (Invest)	Categorical	The specific member or entity that initiated the influx of funds into the network. A witting participant or "front" node	Identified by position within the network; usually first point of interaction between the funds of interest and the network of interest	If funds are unknowingly injected via an attack, code the source as "Victim" and code the actor who triggered the injection as "Investor". If unnamed, record as

[151] Some variables & definitions have been borrowed from the original TRM; see Leuprecht et al., "Tracking Terrorist Resourcing Nodes," 341.

[152] In order of appearance in dataset. For any variables where there are multiple instances (ex., multiple investors), list in order of chronological appearance (this may differ from appearance in the legal document) unless otherwise noted in coding choice notes, and identify with number (ie., Investor 1). Each instance should have its own column, added after all variables related to the first instance are listed (ie., order for 2 investors would be Investor 1, Investor 1 C, Investor 1 P, Investor 1 S, followed by Investor 2, Investor 2 C.....and so on). For any variables where it is clear information is incomplete – ie., first investor is named and this is followed by " and unknown accomplices", list first investor by name, second investor as "unknown investor 2", and leave a third variable column blank highlighted in red to show potential continuation of the network. Also use blanks highlighted in red to show variables that must be present for described network function to be possible but are not identifiable to legal document (e.g., a bank must have been used but no banks are noted). For any variables where all information is available, and the legal document indicates a clear end to the network structure related to that variable, fill any additional columns in the dataset for that variable with N/A across the remainder of the case row rather than leaving blank. Also use N/A in instances where the variable was not present or could not reasonably be inferred to have been present in the network structure.

		responsible for entering capital into the system.	in the chronological retelling of the case. Recorded as full name if available, extracted verbatim.	association with entity (e.x., "RGB member") or, if that information is also unavailable, as "unknown investor". In either instance, ensure they are named with a # that corresponds to their chronological appearance in the legal document.
Investor Location (listed in separate columns as INVEST C, P, and S)	Categorical	Where the investor resided or was located at the time of network activities. C is the name of the city (i.e., Kingston) P is the name of the sub-national region (e.x., Ontario), S is the country or larger state (e.x., Canada).	Extracted verbatim.	If information is unavailable, leave blank. If city name is repeated elsewhere in relation to a different geographic location (e.x., for Kingston, Canada vs Kingston, Jamaica, use an additional identifier on one to differentiate – Kingston (J) would be appropriate in this example).
Recipient (Rec)	Categorical	The end-node individual, department, or entity that ultimately received the funds or goods.	Identified by network topography; the terminal point where asset movement ceases. Record as full name if available, extracted verbatim.	If an actor retains a commission or fee before sending the remaining balance forward, code them as both "FIA" and "Recipient". If unnamed, follow the same conventions as Investor variable.
Recipient Location (listed in separate columns as Rec C, P, and S)	Categorical	The location where the recipient took possession of the funds or goods, or where the final account/repository is based. Follow the same conventions as Investor Location variable.	Extracted Verbatim	Follow the same conventions as Investor Location variable.

Bank	Categorical	Name of the traditional financial institution that transferred network funds.	Extracted Verbatim	If the bank was stolen from/funds were transferred out in an attack, class as "Victim". If explicitly noted that the bank is aware of fund origins/destination/network activities and facilitates the transfer anyway, class as both "Bank" and "FIA". If unnamed, follow the same conventions as Investor variable.
Bank Location (listed in separate columns as Bank C, P, and S)	Categorical	The location of the bank where the transfer of funds took place. Follow the same conventions as Investor Location variable.	Extracted verbatim	Follow the same conventions as Investor Location variable.
Virtual Currency Exchange (VCE)	Categorical	The digital platform or service used to swap fiat currency for cryptocurrency, or to move funds between different types of digital assets.	Extracted verbatim or inferred based on documented transaction patterns (e.g., use of mixers/tumblers)	Follow the same conventions as Bank variable.
Virtual Currency Exchange Location	Categorical	The registered location of the VCE where the transfer of funds took place.	Extracted Verbatim	Follow the same conventions as Investor Location variable.

(listed in separate columns as VCE C, P, and S)		Follow the same conventions as Investor Location variable.		
Financial Intermediary (FIA)	Categorical	The agent (individual or organization) facilitated the channeling of funds between the investors (source of funds) and the recipients/regime.	Identified by network topography; assets pass through these nodes but never permanently stop or originate there. Recorded as full name if available, extracted verbatim.	FIAs may hold overlapping roles: ensure they are appropriately classed in all applicable variable categories. If unnamed, follow the same conventions as Investor variable.
Financial Intermediary Location (listed in separate columns as FIA C, P, and S)	Categorical	The location where the intermediary resided/was located when funds or goods passed through them between origin and destination.	Extracted verbatim.	Follow the same conventions as Investor Location variable.
Financial Intermediary Mechanism Type (FIA Mech)	Categorical	How the funds or goods were transferred within the network.	Extracted verbatim	May aggregate into a few typologies as coding continues; ensure use of consistent language/terminology across cases when describing the same activities.
Victim	Categorical	The individual, corporation, or entity targeted by the attack.	Identified by network topography; will often be explicitly noted as victims. Recorded as full name is available, extracted verbatim.	If unnamed, code using explicit sector identifiers provided in the docket (e.g., Defence Contractor or Software Development Company)

Victim Location (listed in separate columns as Victim C, P, and S)	Categorical	The location of the individual, corporation, or entity targeted by the attack.	Extracted verbatim	Follow the same conventions as Investor Location.
Attack Dates (listed in separate columns as Attack Start and Attack End)	Categorical	The specific instance of a coordinated strike, typically via cyber-means, intended to generate revenue or disrupt systems for the benefit of the proliferation network.	Extracted verbatim	Start dates in smaller, long campaigns may not be noted, more likely to be found where single-strike or large-scale attacks took place. End date is date of attack/exfiltration, not necessarily the date when the victim identifies or resolves the intrusion.
Attack Mechanism (Attack Mech)	Categorical	The technical method used to execute the attack.	Extracted verbatim	Prioritize technical specificity over generalizations, if available record by both name and type (e.g., “Maui Ransomware” is preferable to just “Ransomware”)
Agent	Categorical	The primary perpetrator responsible for the activity of the network as a whole.	Extracted verbatim.	In these cases, always identified as the Democratic People's Republic of Korea (DPRK). Can generally be found on first page or early in preamble/background section.
Agent Affiliate	Categorical	The specific individual or sub-group (e.g., Lazarus Group, APT38) acting as the link between the immediate criminal ring and the DPRK state apparatus.	Extracted verbatim.	This individual will normally also play an identified, central role(s) within the network.
Agent Affiliate Role	Categorical	The specialized function performed by the affiliate within the operation, such as hacker,	Inferred by coder based on the actions taken by identified	May aggregate into a few typologies as coding continues; ensure use of consistent

		money launderer, or recruiter.	actor within the network.	language/terminology across cases.
Agent Affiliate Location (only S)	Categorical	The country where the agent affiliate primarily operated from/resided during the network activities	Extracted verbatim	Follow the same conventions as Investor Location variable.
Investigating Agency	Categorical	The name of the committee or government body that investigated the case.	Extracted verbatim	Include specific sub-units where available (e.g., IRS – Criminal Investigations Cyber Crimes Unit)
Investigating Agency Location (only S)	Categorical	The location of the committee or government body that investigated the case.	Extracted verbatim	Will often, but not always, be the same country that ultimately brings charges.
Cash Raised/Stolen	Continuous	The total amount of currency obtained by the network.	Totaled by coder based on information provided in legal document.	Will exclusively be funds associated with victim information and/or investor information.
Non-Cash Goods raised/stolen	Categorical	The description of physical assets or intellectual property (e.g., software code, dual-use technology) obtained by the network.	Extracted verbatim or inferred by coder based on fund usage/seizure information.	Designed to capture resource items such as dual-use industrial components, sensitive data, or other material assets of value.
Value of non-cash goods raised/stolen	Continuous	The estimated market value in USD of the non-cash goods at the time of theft or acquisition.	Totaled by coder based on information provided in legal documents and information on USD value at a given time.	May or may not be estimable; if not, mark as blank highlighted in red. For seized items such as houses/other material assets, check for additional legal documents or official appraisal appendices with estimable values included.
Seizure/	Categorical	The dates from when cash was first	Reconstructed by the coder based on	Start dates may or may not coincide with attack end

Fundraising Dates (listed in separate columns as Seizure/ Fundraising Start and Seizure/ Fundraising End)		raised/stolen to when it stopped being raised/stolen.	chronological retelling of criminal activity, and/or information on victim/investor activities.	dates; end dates may coincide with transfer start dates. Window will usually be between these dates even if they do not directly coincide with them.
Cash Transferred	Continuous	The total amount of funds in approximate USD successfully moved to the final destination.	Totaled by coder based on transaction information provided in legal document.	Will exclusively be funds associated with investor transfers to financial intermediaries and financial intermediary transfers to recipients. This value may diverge from Cash Raised/Stolen.
Transfer Dates (listed in separate columns as Transfer start and Transfer end)	Categorical	The dates from when cash was first transferred from an investor to another member of the network until the last transfer to a recipient.	Reconstructed by coder based on chronological retelling of criminal activity, and/or information on intermediary/recipient activities.	
Currency	Categorical	The specific type of denominations used in network transactions (e.g., USD, EUR, BTC, ETH).	Extracted verbatim.	Only list each currency type used by network once, even if converted back and forth multiple times. Option to code in order by appearance in chronology (as done for this dataset) or by volume of use, depending on research objectives.

Appendix B: Case List

- United States v. 113 Virtual Currency Accounts. No. 1:20-cv-00618. District of Columbia, 2020.
- United States v. 280 Virtual Currency Accounts. No. 1:20-cv-02396. District of Columbia, 2020.
- United States v. Ghaleb Alaumary. No. 2:20-cr-00043. Southern District of Georgia, 2020.
- United States v. Jon Chang Hyok, et al. No. 2:20-cr-00614-DMG. Central District of California, 2021.
- United States v. Kim Kwang Jin, et al. No. 1:23-cr-00128. Northern District of Georgia, 2023.
- United States v. Paxful User ID Account 4690943 (Affidavit in Support of Seizure). District of Columbia, 2020.
- United States v. Rim Jong Hyok. No. 1:24-cr-00216. District of Kansas, 2024.
- United States v. Sim Hyon Sop, et al. No. 1:23-cr-00130. District of Columbia, 2023.
- United States v. Sim Hyon Sop, Wu Huihui, et al. No. 1:23-cr-00129. District of Columbia, 2023.
- United States v. Storm and Semenov. No. 1:23-cr-00430. Southern District of New York, 2023.
- United States v. Virtual Currency Associated with North Korean IT Worker Laundering and Sanctions Evasion Conspiracies. No. 1:23-cv-03022. District of Columbia, 2023.