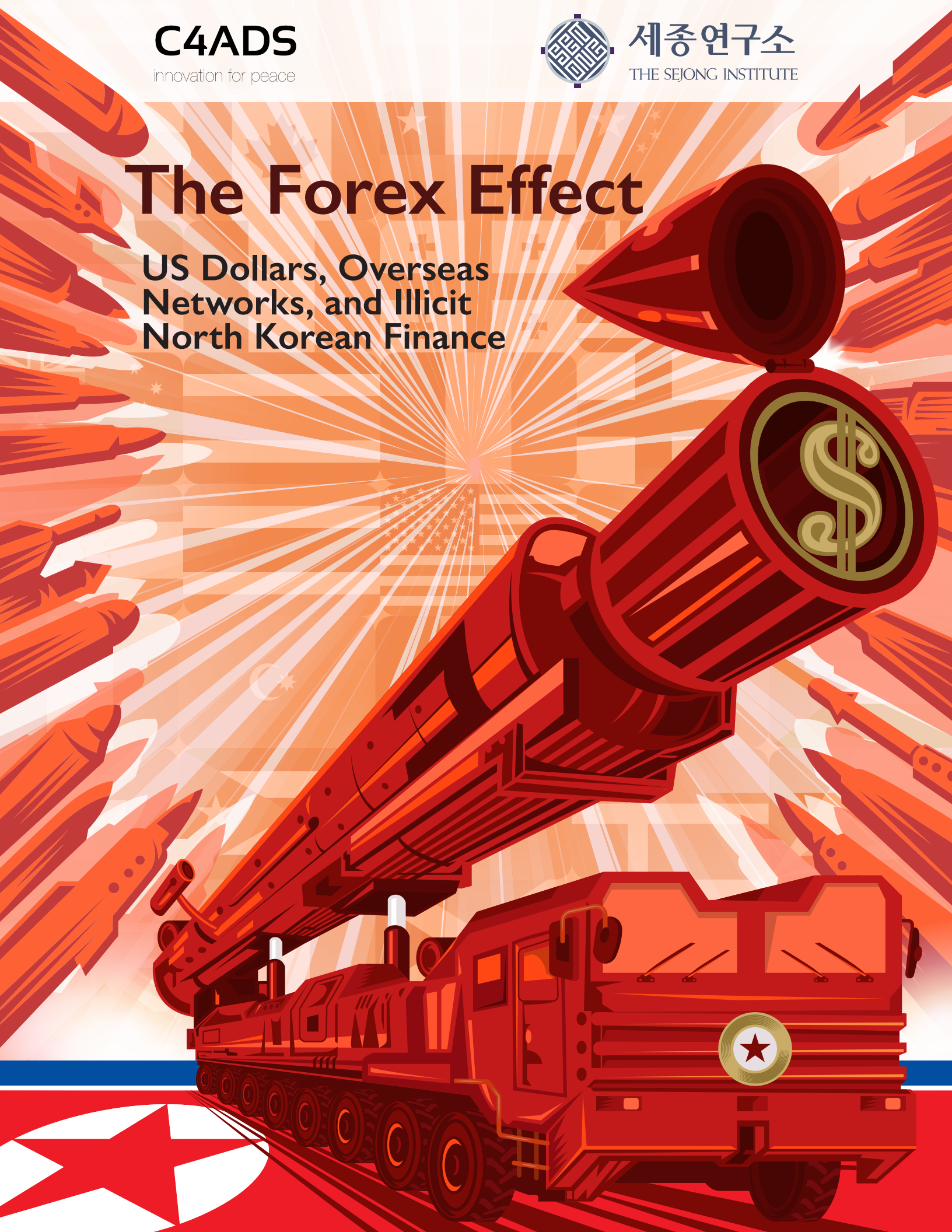


The Forex Effect

**US Dollars, Overseas
Networks, and Illicit
North Korean Finance**



ABOUT C4ADS

C4ADS (www.c4ads.org) is a 501(c)(3) nonprofit organization dedicated to data-driven analysis and evidence-based reporting of conflict and security issues worldwide. We seek to alleviate the analytical burden carried by public sector institutions by applying manpower, depth, and rigor to questions of conflict and security.

Our approach leverages nontraditional investigative techniques and emerging analytical technologies. We recognize the value of working on the ground in the field, capturing local knowledge, and collecting original data to inform our analysis. At the same time, we employ cutting edge technology to manage and analyze that data. The result is an innovative analytical approach to conflict prevention and mitigation.

© C4ADS 2017

ABOUT THE SEJONG INSTITUTE

THE SEJONG INSTITUTE is a private research institute that focuses on issues related to security, national unification, and foreign affairs. It is dedicated to enhancing national and social development through in-depth research and training programs necessary for national security, national unification, and improvement of international relations. Since its founding in 1984, it has been working to expand on its current status as South Korea's leading private think-tank to become a global think-tank for the 21st Century. The Sejong Institute will continue to carry out its mission and contribute to democracy in Asia and world peace.

ACKNOWLEDGEMENTS

C4ADS would like to thank Bill Newcomb, a C4ADS fellow and former member of the UN Panel of Experts Sanctions Committee 1718; John Park of the Harvard Kennedy School; Joshua Stanton, an attorney in Washington D.C.; Anthony Ruggiero of the Foundation for Defense of Democracies; and the many other individuals who generously provided advice and insight. Additionally, this report would not have been possible without C4ADS technology partners, whose software and systems were integral to the project's success.

LEGAL DISCLAIMER

The mention of any individual, company, organization, or other entity in this report does not imply the violation of any law or international agreement, and should not be construed as such. Throughout this report, we refer to and rely on criminal and civil complaints filed by the U.S. Department of Justice. Where such sources are used, C4ADS is not stating that the allegations made by DOJ in those pleadings are factually complete, it is merely reporting that such allegations have been made by the Department of Justice.

COVER IMAGE

The cover image was produced by Devin Thorne.

Table of Contents

EXECUTIVE SUMMARY	4
METHODOLOGY.....	5
INTRODUCTION.....	6
CASH DEPENDENT	8
DOLLARIZING THE REGIME.....	8
ENSURING REVENUE: THE BANGLADESH HEIST	9
INSTITUTIONALLY BOTTLENECKED.....	12
ECONOMICALLY VULNERABLE: THE FOREIGN EXCHANGE SYSTEM	12
PILLARS OF THE NORTH KOREAN FOREIGN EXCHANGE SYSTEM.....	13
ADAPTATION TO SANCTIONS: INTERCONNECTED NETWORKS	16
STRATEGIC CHOKEPOINTS: INJECTING LIQUIDITY.....	19
MEASURING IMPACT: FINANCING THE SYSTEM	19
EXPOSED TO DISRUPTION	21
GLOBAL INTEGRATION: WITHIN REACH.....	21
FINANCIAL LEVERAGE: SEIZING THE MONEY.....	23
FOLLOW THE MONEY: IDENTIFYING TARGETS	24
CONCLUSION	29

Executive Summary

Recent United Nations Security Council resolutions 2371 and 2375 and United States Executive Order 13810 have dramatically increased restrictions on North Korean overseas economic activity. Though North Korea has employed an array of overseas networks to counter international sanctions, the need to adapt has fundamentally changed the regime's international economic exposure. Today, the regime is dependent on the flow of hard currency to function. Maintaining this access and evading international sanctions have required the regime's foreign exchange banks to offshore critical financial infrastructure overseas. The resulting illicit overseas networks play a vital role as proxies for the North Korean banking and foreign exchange systems. However, being integrated into the international systems of banking, commerce, and logistics leaves these networks exposed to international law enforcement actions.

In this report, we build on the findings of our previous research to conduct an in-depth examination of the structure of North Korean illicit networks through their ties to the foreign exchange system. We focus in particular on the networks surrounding North Korea's major foreign exchange banks, which, tasked with the management of hard currency, have found themselves serving as a financial lifeline for the regime. Our report finds that this financial structure is reliant on a system that North Korea cannot control and is therefore vulnerable to systemic disruption.

- In **Cash Dependent**, we explore how maintaining a positive flow of hard currency has become an imperative for regime survival and how the regime has gone to great lengths, often by illicit means, to ensure ongoing access to it.
- In **Institutionally Bottlenecked**, we examine how the regime, hoping to maintain oversight and security, limited methods for storing and transacting in foreign currency internationally. We analyze how North Korea's policies led the regime to offshore critical portions of its financial system.
- In **Exposed to Disruption**, we look at how North Korean assets, nested within businesses overseas, are inherently vulnerable. We further explore the potential for international law enforcement action to dismantle critical nodes of the system.

Provocative actions taken by the Kim regime in the face of international pressure have made the situation on the Korean peninsula increasingly dangerous. Multiple tests of intercontinental ballistic missiles,¹ which now put Washington, DC within striking distance,² have increased the stakes of potential escalation. However, the international community also retains significant leverage if sanctions are properly enforced. The unanimous passage of back-to-back UN Security Council resolutions have put in place measures that can begin to pressure the regime effectively. Sectoral bans of North Korea's most lucrative exports, including coal, iron ore, textiles, and seafood products, will prevent the regime from collecting billions of dollars in hard currency annually. In fact, full enforcement of these measures restricts 90.5% of North Korea's 2016 export revenue, or \$2.3 billion annually.³ But these measures will take time to have an impact. In order to coerce the Kim regime back to the negotiating table non-violently, it is imperative that the international community enforce these resolutions, especially where the regime will feel this pressure most: in its foreign exchange earnings. We intend for this report to help make that possible.

1 Domonoske, C. (2017, November 28) North Korea Fires Apparent ICBM in First Missile Test in 2 ½ Months. NPR/ Retrieved from: <https://www.npr.org/sections/thetwo-way/2017/11/28/566994979/north-korea-apparently-fires-another-missile-after-2-1-2-month-break-between-tes>

2 Cohen, Z., Browne, R., Gaouette, N. (2017, November 30) New missile test shows North Korea capable of hitting all of US mainland. CNN. Retrieved from: <http://www.cnn.com/2017/11/28/politics/north-korea-missile-launch/index.html>

3 Document held by author, available upon request.

Methodology

This report reflects an eight-month follow-up investigation on entities and methods highlighted in C4ADS' reports, *Risky Business* and *In China's Shadow*. The report emphasizes the ongoing effectiveness of using open data to map and expose North Korean overseas networks. Throughout this research, we have prioritized using official documentation for which the source and credibility can be clearly established.

We began this investigation by building a baseline understanding of the roles and modus operandi of North Korean financial and overseas networks based on case studies of some of the most significant enforcement actions in the past year. These include the sanctions designations and civil asset forfeitures levied against a number of North Korean networks, most notably Dandong Hongxiang Industrial Development Co. Ltd., Mingzheng International Trading Co. Ltd., Dandong Zhicheng Metallic Material Co. Ltd., Jin-hou International Holdings, and Dandong Tianfu Trade Co. Ltd. Throughout this process, we relied on existing reporting, court documents, and public records to inform our understanding of the nature and structure of these networks.

In conducting this research, we focused on the structure of the North Korean overseas financial system and its ties to the Kim regime. We sought to build upon our understanding of North Korean networks with specific details and patterns of activities released in documents by the US Department of Justice. For key companies within this dataset, we used a wide range of global corporate, tax, property, maritime, and trade databases to map out their corporate holdings and activities. Where necessary, our findings were supplemented by native-language media, academic reporting, and expert interviews. Throughout this report, we refer to and rely on criminal and civil complaints filed by the US Department of Justice. Where such sources are used, C4ADS is not stating that the allegations made by DOJ in those pleadings are factually complete, it is merely reporting that such allegations have been made by the Department of Justice. Data from this expanded sample was structured within our Palantir Gotham network analysis platform.

Finally, we identified key entities for focused investigations based on patterns and trends found within the Palantir-structured data. To expand the emerging networks, we primarily used public records in several East Asian countries, including corporate registries, court filings, and trade data. Wherever possible, our priority was to identify unsanctioned companies associated with North Korean sanctioned entities, which could indicate ongoing proliferation activities and financing for North Korea.

There are some limitations in the methodology of this report. In many cases, there is no transaction-level financial data to confirm suspected illicit activity. As such, unless explicitly stated, the mention of any individual, company, organization, or other entity in this report does not necessarily imply the violation of any law, international agreement, or UN Security Council resolution, and should not be construed as such.

Introduction

Despite North Korea's declared "Juche" ideology of self-reliance, the country has become increasingly dependent on aspects of the international system to function. Having been forced to adapt its operations due to multiple rounds of international sanctions, the regime has traded a significant degree of control over its economy to maintain the development of its nuclear and missile programs.⁴ As one nuclear test and 23 missile tests in 2017 alone show, economic coercion has not yet deterred the regime from these programs. Nonetheless, sanctions have forced the regime to adapt in a way that has left it exposed and vulnerable.

The North Korean economy is reliant on hard currency to function, especially on US dollars. Department of Justice documents state as much: "to obtain goods and services in the international market place...[North Korea] needs access to US dollars..."⁵ To acquire this foreign currency, the regime has relied on a variety of methods, from exploiting the wages of tens of thousands of North Korean laborers sent overseas, reportedly confiscating as much as 80% of earned income,⁶ to raising funds by illegally selling liquor in Pakistan.⁷ Even cell phones sales have become vectors for the regime to generate additional revenue. Phones that cost \$80 in China have reportedly been sold by the North Korean state for \$300.⁸ Ultimately, these are not a collection of random actions taken by a rogue regime; rather, they are symptoms of its dependence on foreign currency.

This dependence on foreign currency in an environment of increasing international sanctions and restrictions forced North Korea to adapt how it raises and transacts foreign currency, while still maintaining operational oversight and security. Even prior to international sanctions, North Korean banking regulations restricted how its financial institutions could reach international markets.⁹ Using a small number of foreign exchange banks, the regime created an inter-bank clearing system, effectively bottlenecking access to foreign currency reserves and international transactions. These institutions were themselves sanctioned for their role in financing the regime's nuclear and missile programs. Reliant on continued access to foreign currency, they adapted how they accessed the international market by outsourcing large pieces of their financial infrastructure to overseas commercial networks. According to the US Department of Justice, the ensuing illicit overseas financial networks, like Dandong Hongxiang Industrial Development Co. Ltd. and Dandong Zhicheng Metallic Material Co. Ltd., provided pathways for North Korea to illicitly transact billions of dollars on the regime's behalf.^{10 11}

While this economic outsourcing maintained the regime's foreign exchange system, it necessitated nesting vital financial infrastructure within the international systems of banking, commerce, and logistics. Our previous reports, *In China's Shadow* and *Risky Business*, revealed the structure of these networks and the environment in which they operate. Although these networks have adapted to international pressure, they still exist in a system that is centralized, limited, and vulnerable to disruption. This report builds upon our previous analysis to argue that an effective economic pressure strategy can target the North Korea regime where it is

4 (n.d.) NK Missile Tracker. NK News. Retrieved from: <https://www.nknews.org/pro/nk-missile-tracker/>.

5 U.S. v. All Funds in the Accounts of Blue Sea Business Co., Ltd., et al., Retrieved from: <https://www.justice.gov/opa/file/897051/download>.

6 Shin, C.H., Go, M.H. (2014, November 3) Beyond the UN COI Report on Human Rights in North Korea. The Asan Institute for Policy Studies. Retrieved from: <http://en.asaninst.org/contents/asan-report-beyond-the-coi-dprk-human-rights-report/>.

7 Sungwon, B. (2016, June 07). North Korean Diplomats Use Immunity for Money-making Scheme. VOA. Retrieved from: <https://www.voanews.com/a/north-korean-diplomats-use-immunity-for-money-making-scheme/3366859.html>

8 Hei-in, S. (2011, November 02). N.K. desperately collecting foreign currency. The Korea Herald. Retrieved from: <http://www.koreaherald.com/view.php?ud=20111102000761>

9 U.S. v. \$1,071,251.44 of Funds Associated with Mingzheng International Trading Limited, 17-CV-01166, (D.D.C.), ECF No. 1, Retrieved from: <https://www.courthousenews.com/wp-content/uploads/2017/06/Mingheng.pdf>.

10 Ibid.

11 U.S. v. All Wire Transactions Involving Dandong Zhicheng Metallic Material Company, Ltd., et al., 17-mj-217-DAR-BAH, (D.D.C.). Retrieved from: <http://www.dcd.uscourts.gov/sites/dcd/files/BAHMemoandOrder.pdf>.

most vulnerable: the limited foreign exchange system that manages its illicit financial activity.

In maintaining access to international financial, commercial, and logistics networks, North Korea has had to hide its activity, and more importantly its money, using an interconnected web of networks. These networks draw together revenue from disparate illicit activity into a centralized structure that finances the system of North Korean sanctions evasion. The system makes no distinction between sources of revenue. Sanctions have been put in place to stop North Korea from pursuing weapons of mass destruction (WMD), but the regime still maintains overseas networks to procure financial and material support for its WMD ambitions. Unraveling these financial structures can effectively cut off financing for North Korea's illicit activity. Recent actions taken by the United Nations, US Department of the Treasury, and the US Department of Justice have started to reveal the exposure created by the regime's foreign exchange system. In order to draw the regime back to the negotiating table, the international community must exercise its leverage over this dependency.

North Korea is reliant on a system it cannot control. Its vulnerability is economic; our leverage is financial.

Cash Dependent

Maintaining a positive flow of hard currency is imperative for regime survival. Access to these funds has played a major role in helping weather sanctions and the regime has gone to great lengths, often using illicit means, to ensure ongoing access to them.

Dollarizing the Regime

The use of foreign currency within the North Korean domestic economy has become a fact of life for average North Koreans. As journalists in North Korea routinely report paying for their expenses with dollars and euros, more reports have surfaced¹² that not only describe the use of foreign currency by average people, but also the methods the regime has taken to collect foreign currency from them.¹³ ¹⁴ Since the collapse of the Soviet Union, the North Korean economy has been in a nearly constant state of instability, and recent measures taken by the regime to maintain economic stability, especially in the past decade, have unwittingly tethered the North Korean economy to a dependence on foreign currency.

In November 2009, the regime revalued the North Korean Won in an attempt to suppress unofficial economic activity and inflation.¹⁵ It limited the amount of old money that North Korean citizens could exchange for new bills and put in place a timeframe during which these exchanges could occur.¹⁶ An apparent attempt to stabilize the economy for the impending leadership transition from Kim Jong-Il to Kim Jong-Un, the policy had several unintended consequences. The reform's immediate effect was to wipe out much of the savings of average North Koreans and trigger hyperinflation.¹⁷ The exchange rate of the North Korean Won depreciated precipitously, from 200 NKW for 1 US dollar to 1300 NKW for 1 US dollar in just three months. By March of 2010, less than four months after its implementation, the reform's architect was labeled "a son of a bourgeois conspiring to infiltrate the ranks of revolutionaries to destroy the national economy," and was executed by firing squad.¹⁸ The damage, though, had already been done; today, the black-market exchange rate is roughly 8,000 NKW for 1 USD.¹⁹

As average North Korean citizens searched for a stable way to securely store their assets and make daily purchases, they increasingly turned to foreign currency. While foreign currency had been a staple of the unofficial market economy since the early 1990's, the reforms of 2009 were decisive in bringing its use out of the shadows and more into the formal economy.²⁰ By April of 2013, a study by the Samsung Economic Research Institute estimated that in an economy worth \$21.5 billion, \$2 billion of foreign currency was in circulation.²¹ More recently, a 2017 study surveying 231 North Korean defectors found that in some areas,

12 Osnos, E. (2017, September 18) The Risk of Nuclear War with North Korea. The New Yorker. Retrieved from: <https://www.newyorker.com/magazine/2017/09/18/the-risk-of-nuclear-war-with-north-korea>.

13 Ah, S. S. (2017, November 16) Elites pay bribes with money extorted from lower cadres. Daily NK. Retrieved from: <http://www.dailynk.com/english/read.php?catald=nk01500&num=14832>.

14 Kim, C.H. (2017, October 14) Authorities demand Chinese yuan for mandatory new license plates. Daily NK. Retrieved from: <http://www.dailynk.com/english/read.php?catald=nk01500&num=14757>.

15 Sang-Hun, C. (2009, December 01). North Korea Revalues Its Currency. The New York Times. Retrieved from: <http://www.nytimes.com/2009/12/02/business/global/02korea.html?mcubz=3>.

16 Ibid.

17 Branigan, T. (2010, March 18). North Korean finance chief executed for botched currency reform. The Guardian. Retrieved from: <https://www.theguardian.com/world/2010/mar/18/north-korean-executed-currency-reform>.

18 Ibid.

19 (2017, December 7). Market Trends. DailyNK. Retrieved from: <http://www.dailynk.com/english/market.php>

20 Min Mun, S., Ho Jung, S. (2017, March). Dollarization in North Korea: Evidence from a Survey of North Korean Refugees. Korea Institute for International Economic Policy. East Asian Economic Review. Vol. 21, no. 1.

21 Yong Sueng, D. (2013, April). Use of Foreign Currencies in North Korea. SERI Quarterly. 106-109. Retrieved from: www.seriquarterly.com

the North Korean Won is no longer the primary currency citizens use to store their wealth. The survey, conducted by the Bank of Korea, showed that after the 2009 currency reforms, 70.7 percent of respondents held 90 percent or more of their assets in US dollars or Chinese Renminbi.²²

Ensuring Revenue: The Bangladesh Heist

To generate foreign exchange from around the world, the regime has relied on a wide array of transnational illicit schemes. These illicit networks have been highly diverse, highlighting the ingenuity and resilience of North Korean overseas networks to exploit the international market to ensure positive cash flows on the regime's behalf. There is perhaps no better example of this than the growing use of North Korean-backed cybercrime to help raise funds.

Over the past decade, North Korea has developed impressive cyber capabilities and used them to its advantage for a variety of purposes, from reportedly hacking Sony Pictures²³ to stealing US-South Korean war plans.²⁴ Cyberattacks are notoriously difficult to attribute, and their low cost makes them ideal for the Kim regime. According to Chris Inglis, a former deputy director of the National Security Agency (NSA), "Cyber is a tailor-made instrument of power for [North Korea]....It can hold large swaths of nation state infrastructure and private-sector infrastructure at risk. It's a source of income."²⁵

On February 4, 2016, the Bangladesh Central Bank sent out thirty-five transfer orders, requesting that nearly \$1 billion be sent out of the bank's settlement account at the Federal Reserve Bank of New York.²⁶ Manipulating the bank's access to SWIFT, an international financial network through which banks send financial messages, hackers stole \$81 million dollars before mistakes in payment documents halted the remaining transfers.²⁷ To gain access to the bank's computer system, hackers had used malware embedded on a benign website as early as seven months before the attack and subsequently introduced engineered code capable of circumventing traditional security backstops to issue the fraudulent transfer requests.²⁸

In April 2017, cyber security researchers at Kaspersky Lab used common attack signatures to link the attack to a specific North Korean cyber network: the "Lazarus Group."²⁹ Known for "attacking manufacturing companies, media and financial institutions in at least 18 countries around the world since 2009," the Lazarus Group is alleged to be a branch of North Korea's premier intelligence agency Reconnaissance General Bureau (RGB) and has also been credited with the 2014 hack into Sony Pictures.^{30 31} When asked about the

22 Min Mun, S., Ho Jung, S. (2017, March). Dollarization in North Korea: Evidence from a Survey of North Korean Refugees. Korea Institute for International Economic Policy. East Asian Economic Review. Vol. 21, no. 1.

23 (2015, January 03). Sony cyber-attack: North Korea faces new US sanctions. BBC. Retrieved from: <http://www.bbc.com/news/world-us-canada-30661973>.

24 Ibid.

25 Sanger, D. E., Kirkpatrick, D. D., Perleth, N. (2017, October 15). The World Once Laughed at North Korean Cyberpower. No More.. The New York Times. Retrieved from: <https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html>

26 Miglani, S., Quadir, S. (2016, May 04). Bangladesh Bank officials say to meet NY Fed, SWIFT; seek to recover stolen money. Reuters. Retrieved from: <https://www.reuters.com/article/us-usa-fed-bangladesh/bangladesh-bank-officials-say-to-meet-ny-fed-swift-seek-to-recover-stolen-money-idUSKCN0XW01A>

27 Quadir, S. (2016, March 10). How a hacker's typo helped stop a billion dollar bank heist. Reuters. Retrieved from: <https://www.reuters.com/article/us-usa-fed-bangladesh-typo-insight/how-a-hackers-typo-helped-stop-a-billion-dollar-bank-heist-idUSKCN0WC0TC>

28 (2017, April 03). Chasing Lazarus: A Hunt for the Infamous Hackers to Prevent Large Bank Robberies. Kaspersky Lab. Retrieved from: https://www.kaspersky.com/about/press-releases/2017_chasing-lazarus-a-hunt-for-the-infamous-hackers-to-prevent-large-bank-robberies

29 Finkle, J. (2017, April 03). Cyber security firm: more evidence North Korea linked to Bangladesh heist. Reuters. Retrieved from: <https://www.reuters.com/article/us-cyber-heist-bangladesh-northkorea/cyber-security-firm-more-evidence-north-korea-linked-to-bangladesh-heist-idUSKBN175214>

30 (2017, April 03). Chasing Lazarus: A Hunt for the Infamous Hackers to Prevent Large Bank Robberies. Kaspersky Lab. Retrieved from: https://www.kaspersky.com/about/press-releases/2017_chasing-lazarus-a-hunt-for-the-infamous-hackers-to-prevent-large-bank-robberies

31 Pearce, M. (2017, May 18). Their code was used to hack Sony and create 'WannaCry.' Meet the 'Lazarus Group,' the armed robbers of the

connections drawn by private security researchers claiming the group was responsible for both the Sony and Bangladesh attacks, Richard Ledgett, the Deputy Director of the National Security Agency, said he was “optimistic about the truth of that.”³² The Lazarus Group has since been credited with the Wannacry ransomware attack, which paralyzed the British National Health System in May 2017.^{33 34}

If the Lazarus Group did, in fact, steal \$81 million from the Bangladesh Central Bank, the subsequent laundering of the stolen money required the work of a much larger global illicit network. The proceeds were sent to accounts at Rizal Commercial Banking Corporation in the Philippines.³⁵ Account holders, who were later found to have opened the accounts with false documents,³⁶ withdrew the funds, converted them to Philippine pesos and consolidated the money into the account of a Chinese-Filipino businessman.³⁷ The attack was planned meticulously. The transfer requests came over the Chinese New Year, ensuring that bank employees would not be at work to catch the suspicious activity.³⁸ By the time regulators were able to send out alerts to freeze and repatriate the funds back to the Bangladesh Central Bank, the \$81 million had been withdrawn, redeposited, and transferred through different accounts several times over.³⁹ Planners had identified loopholes in Philippine anti-money laundering regulations, specifically that casinos had been exempt from reporting regulations introduced in 2013.⁴⁰ The money was used to buy a large number of chips in VIP junket rooms at several casinos, before then disappearing.⁴¹ To date, only a fifth of the \$81 million has been recovered and returned to the Bangladesh Central Bank.⁴²

The use of cyber assets to steal funds at this scale for a nation state is unprecedented. According to Ledgett, “If that linkage from the Sony actors to the Bangladeshi bank actors is accurate – that means that a nation state is robbing banks....That’s a big deal.”⁴³ However, the Bangladesh bank heist is also a critical indicator of the regime’s larger vulnerability: it is reliant on access to hard currency to survive and it is willing to go to unprecedented lengths to obtain it.

Internet. Los Angeles Times. Retrieved from: <http://www.latimes.com/nation/la-fg-lazarus-group-20170518-story.html>

32 Viswanatha, A., Hong, N. (2017, March 22). U.S. Preparing Cases Linking North Korea to Theft at N.Y. Fed. The Wall Street Journal. Retrieved from: <https://www.wsj.com/articles/u-s-preparing-cases-linking-north-korea-to-theft-at-n-y-fed-1490215094>

33 Pearce, M. (2017, May 18). Their code was used to hack Sony and create ‘WannaCry.’ Meet the ‘Lazarus Group,’ the armed robbers of the Internet. Los Angeles Times. Retrieved from: <http://www.latimes.com/nation/la-fg-lazarus-group-20170518-story.html>

34 Harley, N. (2017, October 14). North Korea behind WannaCry attack which crippled the NHS after stealing US cyber weapons, Microsoft chief claims. The Telegraph. Retrieved from: <http://www.telegraph.co.uk/news/2017/10/14/north-korea-behind-wannacry-attack-crippled-nhs-stealing-us/>

35 Lema, K., Marshall, A.R.C. (2016, March 29). Casino agent in Philippines says high-rollers brought in heist money. Reuters. Retrieved from: <https://www.reuters.com/article/us-usa-fed-bangladesh-philippines/casino-agent-in-philippines-says-high-rollers-brought-in-heist-money-idUSKCN0WV1N7>

36 Ibid.

37 (2016, March 20). Bangladesh bank heist exposes Philippine dirty money secrets. The Straits Times. Retrieved from: <http://www.straitstimes.com/asia/se-asia/bangladesh-bank-heist-exposes-philippine-dirty-money-secrets>

38 Paz, C.D. (2016, April 18). TIMELINE: Tracing the \$81-million stolen fund from Bangladesh Bank. Rappler. Retrieved from: <https://www.rappler.com/business/industries/209-banking-and-financial-services/125999-timeline-money-laundering-bangladesh-bank>

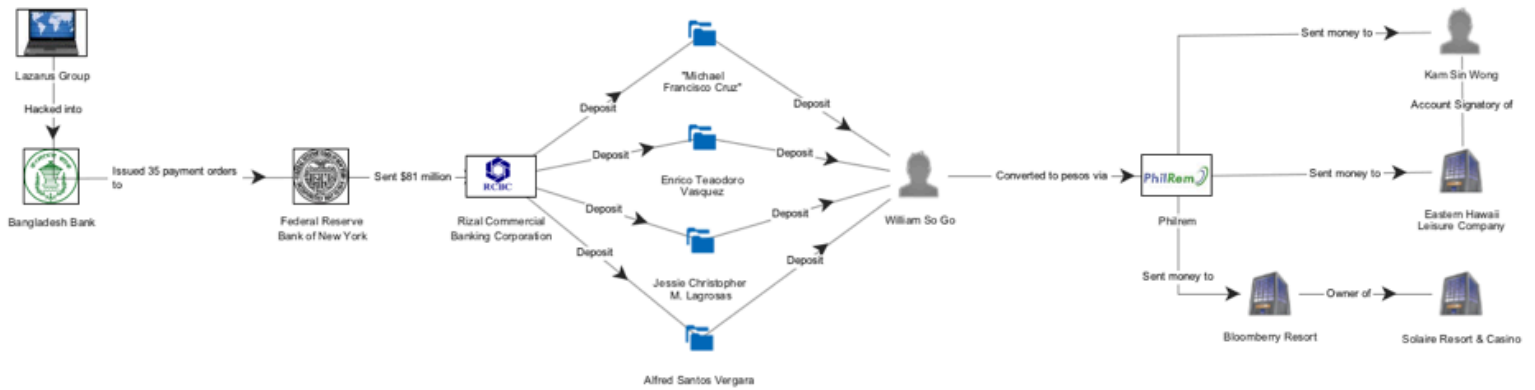
39 Katz, A., Fan, W. (2017, August 11). A Baccarat Binge Helped Launder the World’s Biggest Cyberheist. Bloomberg. Retrieved from: <https://www.bloomberg.com/news/features/2017-08-03/a-baccarat-binge-helped-launder-the-world-s-biggest-cyberheist>

40 Agence France-Presse. (2013, February 06). Casinos exempt from tougher anti money-laundering law. Rappler. Retrieved from: <https://www.rappler.com/nation/21209-ph-casinos-exempt-from-tougher-anti-money-laundering-law>

41 Paz, C.D. (2016, March 16). \$81-M bank heist money trail hits dead end in casinos. Rappler. Retrieved from: <https://www.rappler.com/business/industries/209-banking-and-financial-services/125959-bangladesh-bank-fund-heist-senate-hearing>

42 Katz, A., Fan, W. (2017, August 11). A Baccarat Binge Helped Launder the World’s Biggest Cyberheist. Bloomberg. Retrieved from: <https://www.bloomberg.com/news/features/2017-08-03/a-baccarat-binge-helped-launder-the-world-s-biggest-cyberheist>

43 Groll, J.E. (2017, March 21). NSA Official Suggests North Korea Was Culprit in Bangladesh Bank Heist. Foreign Policy. Retrieved from: <https://foreignpolicy.com/2017/03/21/nsa-official-suggests-north-korea-was-culprit-in-bangladesh-bank-heist/>



To date, only a fifth of the \$81 million has made its way back to the Bangladesh Central Bank

Institutionally Bottlenecked

In order to maintain regime oversight and operational security in the face of international sanctions, the regime has limited how it holds and transacts in foreign currency internationally. Adapting to maintain this access, the regime has been forced to offshore large portions of its financial system.

Economically Vulnerable: The Foreign Exchange System

To be of use, any potential funds raised from the Bangladesh heist would have to find their way back to the North Korean financial system. This newly raised capital would then join funds raised from other revenue-generating organizations, both licit and illicit, in North Korea's foreign reserve accounts. While the importance of hard currency to the regime has increased, the financial institutions tasked with the day-to-day management of these funds have faced unprecedented challenges, causing fundamental shifts in the North Korean banking sector. Prior to international sanctions North Korea had already restricted the number of banks allowed to make international transactions.⁴⁴ These banks, holding accounts for North Korean institutions, including those involved in the regime's nuclear and missile programs, have themselves become the targets of international sanctions.

Foreign Trade Bank: Established in 1959, North Korea's Foreign Trade Bank (FTB) acts as the umbrella bank for foreign currency transactions in North Korea.^{45 46} This includes handling all foreign currency transactions for North Korea's government ministries and their subordinate trading companies.⁴⁷ ⁴⁸ According to Stephen Haggard of the Peterson Institute for International Economics, "the bank undertakes foreign exchange transactions, including those related to trade of various state-owned enterprises involved in the country's WMD programs."⁴⁹ Furthermore, the bank sets the official exchange rate for North Korean Won.⁵⁰ US Department of the Treasury designated the FTB on March 11, 2013, freezing any of its assets that were in or might transit through the United States, on the grounds that "North Korea uses FTB to facilitate transactions on behalf of actors linked to its proliferation network."⁵¹ In light of the US action, banks in other countries, including Japan and China, reportedly cut formal ties with FTB in 2013.^{52 53}

44 U.S. v. \$1,071,251.44 of Funds Associated with Mingzheng International Trading Limited, 17-CV-01166, (D.D.C.), ECF No. 1, Retrieved from: <https://www.courthousenews.com/wp-content/uploads/2017/06/Mingheng.pdf>.

45 (2013, March 11). Treasury Sanctions Bank and Official Linked to North Korean Weapons of Mass Destruction Programs. U.S. Department of the Treasury. Retrieved from: <https://www.treasury.gov/press-center/press-releases/Pages/jl1876.aspx>.

46 U.S. v. \$6,999,925.00 of Funds Associated with Velmur Management PTE Ltd., et al., 17-CV-01705 (D.D.C.), ECF No. 1. Retrieved from: <https://www.justice.gov/usao-dc/press-release/file/992171/download>.

47 (2013, March 11). Treasury Sanctions Bank and Official Linked to North Korean Weapons of Mass Destruction Programs. U.S. Department of the Treasury. Retrieved from: <https://www.treasury.gov/press-center/press-releases/Pages/jl1876.aspx>.

48 U.S. v. \$1,071,251.44 of Funds Associated with Mingzheng International Trading Limited, 17-CV-01166, (D.D.C.), ECF No. 1, Retrieved from: <https://www.courthousenews.com/wp-content/uploads/2017/06/Mingheng.pdf>.

49 Haggard, S. (2013, March 22). The Foreign Trade Bank Sanctions. Peterson Institute for International Economics. Retrieved from: <https://piee.com/blogs/north-korea-witness-transformation/foreign-trade-banks-sanctions>

50 U.S. v. \$6,999,925.00 of Funds Associated with Velmur Management PTE Ltd., et al., 17-CV-01705 (D.D.C.), ECF No. 1. Retrieved from: <https://www.justice.gov/usao-dc/press-release/file/992171/download>.

51 (2013, March 11). Treasury Sanctions Bank and Official Linked to North Korean Weapons of Mass Destruction Programs. U.S. Department of the Treasury. Retrieved from: <https://www.treasury.gov/press-center/press-releases/Pages/jl1876.aspx>.

52 Rabinovitch, S., Mundy, S. (2013, May 07). China reduces banking lifeline to N Korea. Financial Times. Retrieved from: <https://www.ft.com/content/a7154272-b702-11e2-a249-00144feabdc0>.

53 (2013, March 21). North Korean trade bank set to be blacklisted. The Japan Times. Retrieved from: <https://www.japantimes.co.jp/>

Korea Kwangson Banking Corporation: According to the US Department of Justice, Korea Kwangson Banking Corporation (KKBC) serves as a subsidiary to FTB, assisting in foreign transactions of North Korea's state-owned enterprises involved in the country's WMD program.⁵⁴ Sanctioned in August of 2009, KKBC was designated by the US Department of the Treasury for providing financial support to some of North Korea's most notorious weapons proliferators. These proliferation organizations, such as Korea Mining Development Trading Corporation (KOMID), were "utilizing KKBC to facilitate funds transfers likely amounting to millions of dollars."⁵⁵

Pillars of the North Korean Foreign Exchange System

Today, rather than traditional financial institutions that handle funds on behalf of their clients, North Korea's foreign exchange banks work as large-scale accounting firms, moving money held in accounts in the name of front companies to maintain the balances of their domestic North Korean customers, including the regime itself. The US Department of the Treasury has stated that "the DPRK uses and maintains a network of financial representatives, primarily in China, who operate as agents for North Korean financial institutions." It further stated that by operating outside of North Korea, these agents are free to "orchestrate schemes, set up front or shell companies, and manage surreptitious bank accounts to move and disguise illicit funds, evade sanctions, and finance [WMD] proliferation."⁵⁶ In outsourcing these financial functions, North Korean foreign exchange banks such as FTB and KKBC were able to turn to those individuals or companies that stood to profit the most from North Korea's continued presence in international trade—the Chinese companies that were most central to their overseas business.

Although China makes up over 90 percent of North Korean trade today, it has not always been this way. According to John Park, director of the Korea Working Group at the Harvard Kennedy School, the main catalyst for this shift didn't occur until Chinese Premier Wen Jiabao's 2009 visit to Pyongyang.⁵⁷ Wen signed three agreements – under the headings of economic development, tourism, and education – that signaled to Chinese companies that it was legal to conduct commercial activities with North Korean entities and provided a loophole with respect to UN sanctions.⁵⁸ Park states that "the loophole took the form of a clause in UN Security Council resolutions stipulating that member states are not prohibited from engaging in economic development or humanitarian activities with the DPRK. When subsequently pressed to implement sanctions more robustly, Chinese authorities claimed that the commercial interactions in question were legitimate economic development activities."⁵⁹

By further sanctioning the regime, Park points out, the United States had succeeded in elevating the risk for some of those doing business with North Korea, dissuading them from continuing to do so. But "other Chinese middlemen saw the elevated risk as a special business opportunity. Rather than being deterred

news/2013/03/21/national/n-korean-trade-bank-set-to-be-black-listed/#.WcAMk9OGPuQ.

54 U.S. v. \$1,071,251.44 of Funds Associated with Mingzheng International Trading Limited, 17-CV-01166, (D.D.C.), ECF No. 1, Retrieved from: <https://www.courthousenews.com/wp-content/uploads/2017/06/Mingheng.pdf>.

55 (2009, August 11). Treasury Designates Financial Institution Tied to North Korea's WMD Proliferation. U.S. Department of the Treasury. Retrieved from: <https://www.treasury.gov/press-center/press-releases/Pages/tg260.aspx>.

56 (2017, November 2) Advisory on North Korea's Use of the International Financial System. Financial Crimes Enforcement Network. Retrieved from: https://www.fincen.gov/sites/default/files/advisory/2017-11-02/DPRK%20Financing%20Advisory%20FINAL%2011022017_0.pdf.

57 Albert, E. (2017, September 27) The China-North Korea Relationship. Council on Foreign Relations. Retrieved from: <https://www.cfr.org/background/china-north-korea-relationship>.

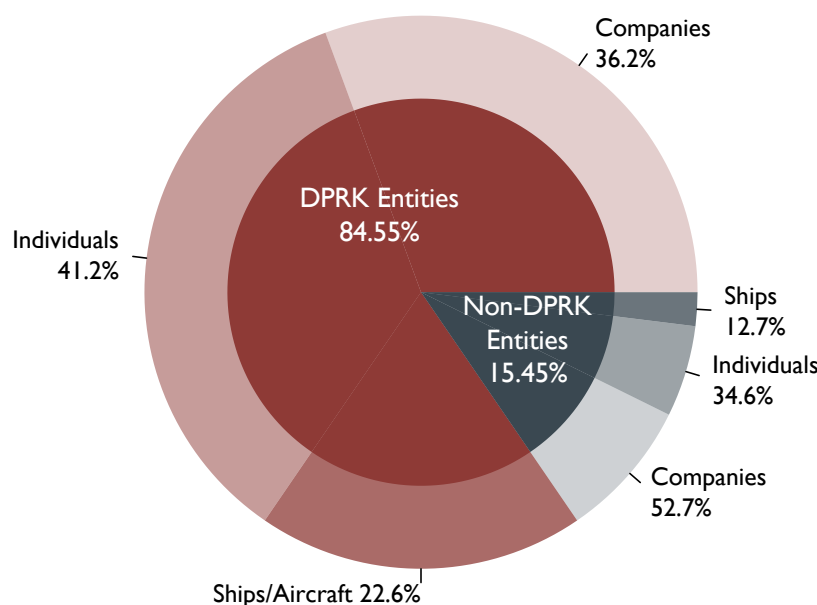
58 Park, John. Interviewed by Author. Washington DC. (2017, November 20).

59 Ibid.

by the elevated risk, it incentivized them.”⁶⁰ By paying higher commission fees due to the increased risk, North Korean entities were able to motivate their Chinese counterparties to provide additional services, such as banking, effectively circumventing international sanctions. Incentivized by higher commission fees and increased price tags for illicit items, North Korean entities were able to rent more sophisticated procurement and logistics capabilities from more capable Chinese middlemen.⁶¹ These middlemen developed multi-purpose business partnerships with select North Korean clients that covered selling goods from the North as well as procuring illicit components in the Chinese marketplace. These sophisticated activities soon began to bring in larger contracts for the middlemen, consolidating the number of major firms that did business with the North Korean regime. By 2016, the top ten importers of North Korean goods in China controlled nearly 30 percent of trade revenue.⁶²

The reasons for the success of this outsourcing are clear: 84 percent of entities designated by the US Department of the Treasury are located within North Korea or are North Korean citizens.⁶³ To date, only 55 non-North Korean entities have been designated for sanctions, many of which were only designated in the past year.⁶⁴ These more recent actions by the US Department of the Treasury have begun to reveal that even after FTB and KKBC were able to successfully offshore key components of their financial infrastructure, the system remained remarkably centralized. Disparate illicit activity and networks were shown to have been connected by a narrow structure of illicit financial proxies.

Distribution of US Department of the Treasury North Korea Sanctions Designations



⁶⁰ Ibid.

⁶¹ Ibid.

⁶² Document held by author, available upon request.

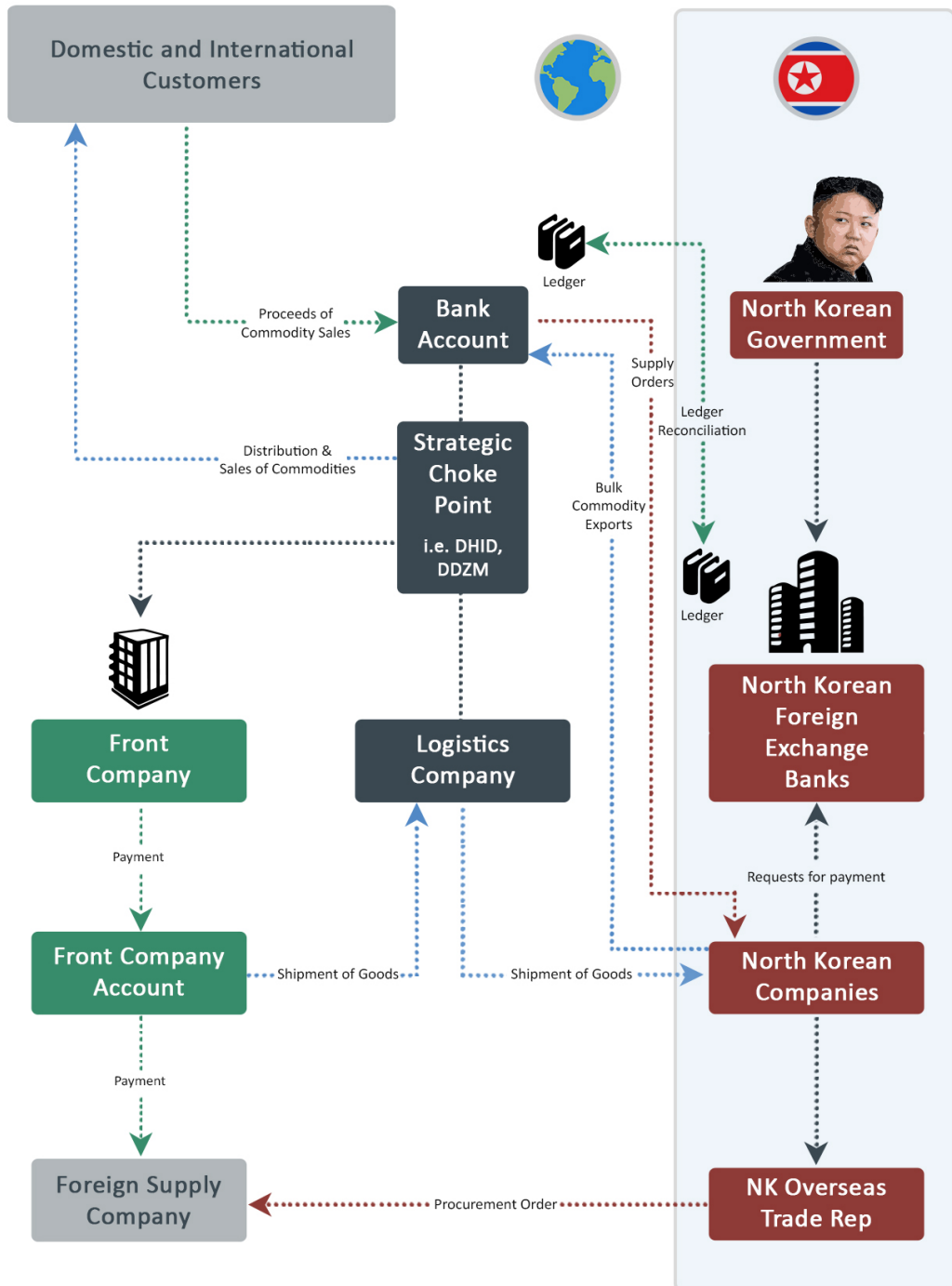
⁶³ (n.d.) Sanctions List Search. Office of Foreign Asset Control. Retrieved from: <https://sanctionssearch.ofac.treas.gov/>.

⁶⁴ Ibid.

North Korea's Illicit Overseas Economy

In order to make international transactions, North Korea's foreign exchange banks have outsourced financial management to key overseas trading companies. Fueled by revenue from bulk commodity exports, the illicit networks developed around these "strategic chokepoints" were vital in making payments on behalf of the regime. Over a seven-year period, beginning after sanctions on KKBC, two companies in China - DHID and DDZM - moved over \$2 billion in illicit assets on behalf of the Kim regime.

Ledger systems record financial transfers for North Korean organizations without having to hold money within North Korea or transfer money through the financial system. Identical records reconcile account activity between North Korea and China without the actual movement of cash.



Adaptation to Sanctions: Interconnected Networks

Although North Korea was able to successfully offshore aspects of its financial infrastructure to companies overseas, the connected structure of its foreign exchange began to link its overseas networks. Actions taken by the US Department of Justice have revealed the relationships, including specific transactions (citing information otherwise unobtainable in the open source) that highlight the degree to which these firms interacted with each other.

Chinese financial institutions like the Bank of Dandong were perfect conduits at the start of this development in outsourcing. According to the US Department of the Treasury, between May 2012 and May 2015, the Bank of Dandong conducted roughly \$133.6 million in transactions through US correspondent accounts that were with or on behalf of US and UN sanctioned entities.⁶⁵ Representatives from KKBC were present at the bank, providing a direct link between North Korean foreign exchange institutions and the Bank of Dandong, an institution that the US Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) called "a gateway for North Korea to access the US and international financial systems despite US and UN sanctions."⁶⁶ In its June 29, 2016 Notice of Proposed Rulemaking, announcing the designation of the bank as a financial institution of primary money laundering concern, FinCEN highlighted that millions of dollars of transactions had been made on behalf of companies involved in the procurement of ballistic missile technology.⁶⁷ However, when KKBC was sanctioned in 2009, North Korea began to adapt the way in which it interacted with financial institutions. One of KKBC's best international gateways was one of Bank of Dandong's minority stakeholders: Dandong Hongxiang Industrial Development Co. Ltd. (DHID) 丹东鸿祥实业发展有限公司.⁶⁸

According to a US Department of Justice indictment, DHID represented 20 percent of China-North Korea trade in 2010.⁶⁹ C4ADS' previous reports, *In China's Shadow* and *Risky Business*, discussed DHID's financial links with North Korea extensively. The company was a leader in the development of trade with North Korea and was headed by a Chinese national and Communist Party member, Ma Xiaohong 马晓红.⁷⁰ Ma's operation eventually expanded to include holdings as varied as international freight and travel services, restaurants, hotels, and Chinese-North Korean joint ventures.⁷¹ On its website, the company described itself as a "bridge between DPRK and the world."⁷² Documents released by the US Department of Justice indicate that when KKBC was sanctioned in 2009, bank representatives needed to find a reliable and secure way to maintain its ability to conduct transactions in US dollars. It found its solution by using DHID and its front companies. Nearly 60 percent of the 28 front companies owned by DHID were registered or purchased within two years of August 11, 2009, the day KKBC was sanctioned. Of these, only two had been incorporated or purchased prior to August 2009.^{73 74 75} By the end of 2016, the DHID global network had expanded to include

65 (2017, July 7) Proposal of Special Measure Against Bank of Dangdong as a Financial Institution of Primary Money Laundering Concern. Financial Crimes Enforcement Network (FinCEN), Treasury. Retrieved from <https://www.federalregister.gov/documents/2017/07/07/2017-14026/proposal-of-special-measure-against-bank-of-dandong-as-a-financial-institution-of-primary-money>.

66 Ibid.

67 Ibid.

68 Chinese Business Registry Filing, document held by author available upon request. Retrieved from <http://gsxt.saic.gov.cn/>.

69 U.S. v. Dandong Hongxiang Industrial Development Co., Ltd., et al, Mag. No. 16-6602 (JAD), (D.N.J.), Complaint Attach. Retrieved from: <https://www.justice.gov/opa/file/897041/download>.

70 Chinese Business Registry Filing, document held by author available upon request. Retrieved from <http://gsxt.saic.gov.cn/>.

71 Ibid.

72 (n.d.). Liaoning Hongxiang Industrial Group. Retrieved from <http://lnhongxiang.com/cn>.

73 C4ADS research available upon request.

74 Hong Kong Business Registry Filing, document held by author available upon request. Retrieved from <http://www.icris.cr.gov.hk>.

75 (2009, August 11) Treasury Designates Financial Institution Tied to North Korea's WMD Proliferation. United States Department of Treasury. Retrieved from <https://www.treasury.gov/press-center/press-releases/Pages/tg260.aspx>.

43 companies on four continents.⁷⁶

According to the US Department of Justice, DHID helped North Korea conduct foreign trade through this elaborate network of shell and front companies, using the US financial system without detection for seven years.⁷⁷ In September 2016,⁷⁸ the Public Security Department of Liaoning Province announced that it was investigating DHID for “serious economic crimes”⁷⁹ and the US Department of Justice unsealed an indictment charging DHID, Ma Xiaohong, and several other top employees with aiding KKBC and acting as a financial proxy to evade sanctions.⁸⁰ DHID was not only a major conduit for North Korean finance, but also a regional hub for North Korean activity. One of the company’s holdings, the Chilbosan Hotel, was reported to be a command outpost for North Korean cyber activity.⁸¹ According to US technology firm Hewlett Packard, within China “[North Korea] maintains technical reconnaissance teams responsible for infiltration of computer networks, hacking to obtain intelligence, and planting viruses on enemy networks.”⁸²

Transactions made between different overseas networks even connect global nodes of North Korea’s system of illicit international finance. Documents released by the United Nations Panel of Experts on North Korea (UN POE) in 2017 show one of DHID’s front companies, Nice Field International 明正国际贸易有限公司, received \$610,000 in payments from MKP Capital.⁸³ Malaysia Korea Partners (MKP), the owner of MKP Capital, is a Malaysia-based firm controlled by Han Hun Il, a reported associate of Kim Jong-un’s uncle Jang Song Thaek, who was purged in 2013.⁸⁴ According to Lee Chol Ho, a North Korean defector who worked for Han for nine years, “When people from the [North Korean] Central Committee visited Malaysia, they only met with Han....They didn’t even bother to see the ambassador.”⁸⁵ These same branches of the system also connected foreign exchange banks. Nice Field International also did significant business with Mingzheng International Trading Co. Ltd, which the US Department of Justice alleges was making illicit payments on behalf of the North Korean government, acting as a “front company for a covert branch of FTB,” and laundering US dollar payments.⁸⁶ The connections between North Korea’s overseas networks, which conduct multiple types of illicit activity on behalf of different North Korean organizations, begin to reveal how deeply interconnected its overseas system is. Losing the ability to rely on a single piece of that system, such as DHID, can dramatically raise the transaction costs for multiple networks around the globe.

76 C4ADS research available upon request.

77 U.S. v. \$1,071,251.44 of Funds Associated with Mingzheng International Trading Limited, 17-CV-01166, (D.D.C.), ECF No. 1, Retrieved from: <https://www.courthousenews.com/wp-content/uploads/2017/06/Mingheng.pdf>.

78 Nakashima, E. (2016, September 26) U.S. charges four Chinese, firm with aiding Pyongyang’s nuclear program. Washington Post. Retrieved from https://www.washingtonpost.com/world/national-security/us-charges-four-chinese-nationals-and-a-chinese-company-with-aiding-pyongyangs-nuclear-program/2016/09/26/1a7a4b16-8407-11e6-92c2-14b64f3d453f_story.html?utm_term=.018ea2749931.

79 Perlez, J., Buckley, C. (2016, September 20) China Announces Inquiry into Company Trading with North Korea. New York Times. Retrieved from <https://www.nytimes.com/2016/09/21/world/asia/north-korea-china-inquiry-hongxiang.html?mcubz=3>.

80 U.S. v. All Funds in the Accounts of Blue Sea Business Co., Ltd., et al., Retrieved from: <https://www.justice.gov/opa/file/897051/download>.

81 Lee, D. (2015, May 29) Bureau 121: How good are Kim Jong-un’s elite hackers? BBC. Retrieved from <http://www.bbc.com/news/technology-32925503>.

82 (2014, August) Profiling an enigma: The mystery of North Korea’s cyber threat landscape. Hewlett Packard Security Research. Retrieved from http://community.hpe.com/hpeb/attachments/hpeb/off-by-on-software-security-blog/388/2/HPSR%20SecurityBriefing_Episode16_NorthKorea.pdf.

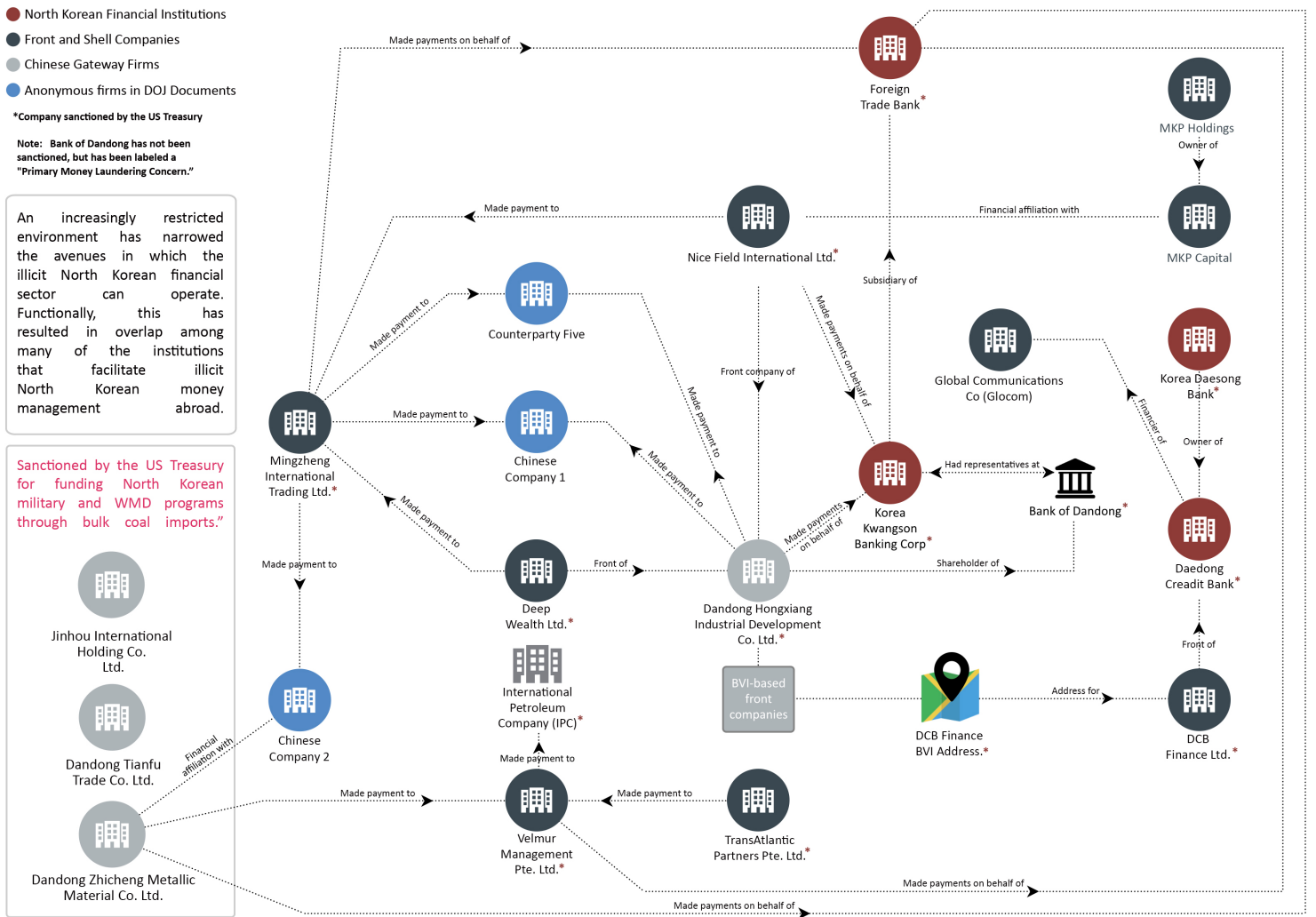
83 (2017, September 5). United Nations Security Council Report of Resolution 2345 (2017). United Nations Security Council.

84 Pearson, J., Allard, T., Latiff, R. (2017, April 9) Exclusive – ‘Dollars and euros’: How a Malaysian helped fund North Korea’s leadership. Reuters. Retrieved from <https://www.reuters.com/article/us-northkorea-malaysia-business/exclusive-dollars-and-euros-how-a-malaysian-firm-helped-fund-north-koreas-leadership-idUSKBN17C0AN>.

85 Ibid.

86 U.S. v. \$1,071,251.44 of Funds Associated with Mingzheng International Trading Limited, 17-CV-01166, (D.D.C.), ECF No. 1, Retrieved from: <https://www.courthousenews.com/wp-content/uploads/2017/06/Mingheng.pdf>.

Strategic Bottlenecks: Interconnected Illicit Overseas Financial Networks



Strategic Chokepoints: Injecting Liquidity

North Korean front companies are designed to obfuscate their ultimate beneficial ownership to allow them to more freely operate for the regime. However, they are simply the action arms of the broader system of North Korea's foreign exchange system. These companies may make payments on behalf of FTB or KKBC or purchases on behalf of other North Korean government entities, but, as many of them exist only on paper, they have no ability to generate the money that they hold in their bank accounts. These accounts are filled with the revenue created by "strategic chokepoints," companies like DHID—large scale, North Korea-centric trading firms. Through sales of North Korean commodities, they create liquidity for the entire system. Until recently, these transactions centered mostly around North Korean exports of coal.

From 2014 to 2016, Dandong Zhicheng Metallic Material Co. Ltd. (DZMM) 丹东至诚金属材料有限公司 appears to be the top importer of North Korean coal to China.⁸⁷ Trade data indicates that the company was the largest importer of North Korean goods in China, representing nearly 10 percent of total 2016 imports by revenue.⁸⁸ Yet, like DHID, the most important role that DZMM played was not only as a broker for North Korean exports, but also as an intermediary for North Korea's foreign exchange system, in this case FTB.⁸⁹ Trade from this single company provided the regime with annual earnings of over \$250 million, injecting liquidity into disparate illicit North Korean networks.⁹⁰ ⁹¹ On August 22, 2017, the US Department of Justice announced that DZMM was found to have "used the foreign exchange received from the end users of North Korean coal to purchase other items for North Korea, including nuclear and missile components."⁹²

Measuring Impact: Financing the System

Using these networks, North Korean's foreign exchange banks were able to maintain access to US dollar accounts and transact globally without detection until earlier this year. Most notably, DHID reportedly allowed KKBC to conduct over \$1.3 billion in transactions,⁹³ DZMM reportedly conducted over \$700 million in prohibited transactions,⁹⁴ and Bank of Dandong reportedly conducted \$133 million.⁹⁵ This money, over \$2 billion dollars within a seven-year period, is not a trivial figure in an economy as small as North Korea's. Moreover, these funds were spent to circumvent international sanctions meant to prevent North Korea from obtaining WMD's. The same day that DZMM was sanctioned by the US Department of the Treasury for its role in managing the finances of FTB, two other Chinese companies were designated: Dandong Tianfu Trade Co. Ltd. 丹东天富贸易有限公司 and Jin-hou International Holding Co. 金猴国际控股有限公司.⁹⁶ Defector testimony included in the Department of Justice documents stated that DZMM was one of three "primary

⁸⁷ Document held by author, available upon request.

⁸⁸ Ibid.

⁸⁹ U.S. v. \$6,999,925.00 of Funds Associated with Velmur Management PTE Ltd., et al., 17-CV-01705 (D.D.C.), ECF No. 1. Retrieved from: <https://www.justice.gov/usao-dc/press-release/file/992171/download>.

⁹⁰ (n.d.) www.zhichengsteel.cn. Archive.org. Retrieved from <http://web-beta.archive.org/web/20160406222337/www.zhichengsteel.cn>.

⁹¹ U.S. v. \$6,999,925.00 of Funds Associated with Velmur Management PTE Ltd., et al., 17-CV-01705 (D.D.C.), ECF No. 1. Retrieved from: <https://www.justice.gov/usao-dc/press-release/file/992171/download>.

⁹² U.S. v. \$4,083,935.00 of Funds Associated with Dandong Chengtai Trading Limited, 17-CV-01706 (D.D.C.), ECF No. 1, Retrieved from: <https://www.justice.gov/usao-dc/press-release/file/992451/download>.

⁹³ U.S. v. \$1,071,251.44 of Funds Associated with Mingzheng International Trading Limited, 17-CV-01166, (D.D.C.), ECF No. 1, Retrieved from: <https://www.courthousenews.com/wp-content/uploads/2017/06/Mingheng.pdf>.

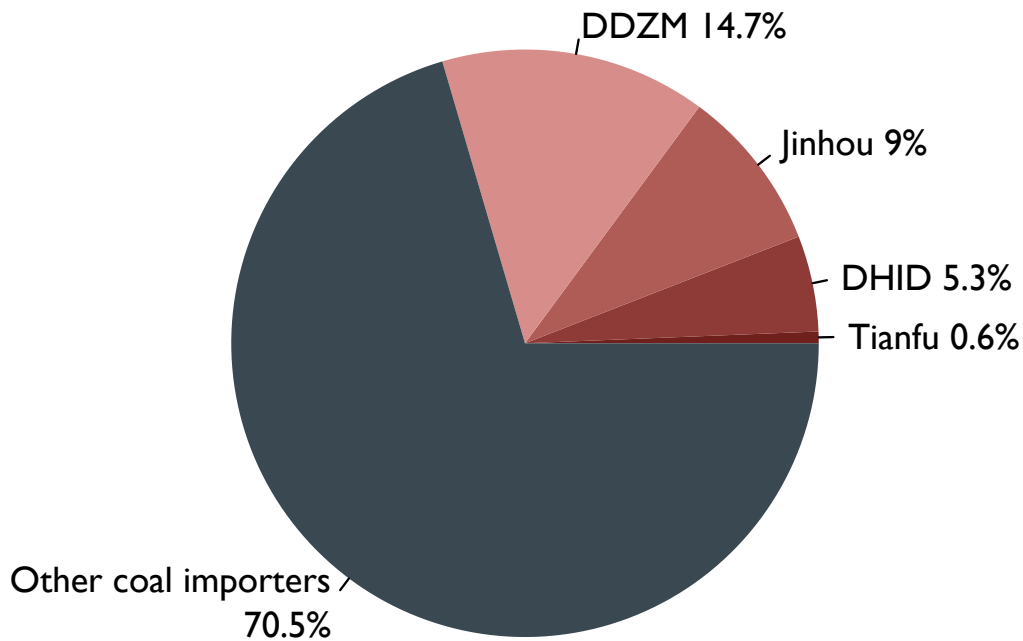
⁹⁴ U.S. v. All Wire Transactions Involving Dandong Zhicheng Metallic Material Company, Ltd., et al., 17-mj-217-DAR-BAH, (D.D.C.). Retrieved from: <http://www.dcd.uscourts.gov/sites/dcd/files/BAHMemoandOrder.pdf>.

⁹⁵ (2017, July 7) Proposal of Special Measure Against Bank of Dandong as a Financial Institution of Primary Money Laundering Concern. Financial Crimes Enforcement Network (FinCEN), Treasury. Retrieved from <https://www.federalregister.gov/documents/2017/07/07/2017-14026/proposal-of-special-measure-against-bank-of-dandong-as-a-financial-institution-of-primary-money>.

⁹⁶ (2017, August 22) Treasury Targets Chinese and Russian Entities and Individuals Supporting the North Korean Regime. United States Department of the Treasury. Retrieved from <https://www.treasury.gov/press-center/press-releases/Pages/sm0148.aspx>.

China-based importers of North Korean coal, all three of which followed the same general business patterns... moving coal out of North Korea and moving illegal goods—including military munitions and items—into North Korea.”⁹⁷ These statements further detailed that the regime uses 95 percent of its foreign exchange revenue from coal for its military and WMD programs.⁹⁸ According to trade records from 2013 to 2016, the four major Chinese companies sanctioned for North Korean ties—DHID, DZMM, Dandong Tianfu Trade Co., and Jin-Hou International Holding Co. Ltd.—were responsible for importing over 30 percent of North Korean coal over that time period.⁹⁹ During this four-year period, these imports would have provided an estimated \$1,331,024,223 to the North Korean military and WMD program.¹⁰⁰

Breakdown of North Korean Coal Imports to China from 2013 through 2016



⁹⁷ U.S. v. \$4,083,935.00 of Funds Associated with Dandong Chengtai Trading Limited, 17-CV-01706 (D.D.C.), ECF No. 1, Retrieved from: <https://www.justice.gov/usao-dc/press-release/file/992451/download>.

⁹⁸ Ibid.

⁹⁹ Document held by author, available upon request.

¹⁰⁰ Ibid.

Exposed to Disruption

By nesting its illicit activity in its overseas networks, North Korea has maintained its access to the international financial system, but its assets are inherently vulnerable. Actions taken by international law enforcement to date have revealed the potential to unravel the entire system.

Global Integration: Within Reach

North Korea's overseas networks have been vital proxies for the regime and its foreign exchange system. The fact that they exist outside North Korea has provided them greater opportunities to freely transact internationally. The benefits of being entrenched within international systems of banking and trade, though, is accompanied by an inherent vulnerability to international sanctions and restrictions. In fact, since September 2016, eight large-scale Chinese trading firms have been sanctioned by the US Department of the Treasury for their roles in supporting North Korea's nuclear and ballistic missile programs.¹⁰¹ These companies have supplied everything from illicit pathways for foreign exchange banks to "motor vehicles, electrical machinery, radio navigational items, aluminum, iron, pipes, and items associated with nuclear reactors."¹⁰²

Trade data from 2013 to 2016 show that although over 90 percent of the \$1.3 billion in export shipments these companies sent went to North Korea, these companies also remained globally integrated,¹⁰³ with shipments being sent to an additional 64 countries over that same period.¹⁰⁴ Over \$50 million worth of these exports were sent to South Korea alone, leaving open the possibility that the regime circumvented trade restrictions through the re-exportation of goods through China.¹⁰⁵ Imports received by these companies from North Korea showed a similar level of concentration, representing over 94 percent of the \$1.6 billion total.¹⁰⁶ Moreover, over \$70 million of the remaining imports came from the United States.¹⁰⁷ As was previously discussed, some of these firms were alleged by the US Department of Justice to serve as re-export hubs for dual-use and military material necessary for the regime's nuclear and missile programs.¹⁰⁸ The complexity of these companies' involvement with North Korea does not allow for easy distinction between transactions made on behalf of North Korea and those that were not – indeed, the co-mingling of transactions can be a means to conceal their nature, and the existence of trade at these volumes indicates this distinction is largely artificial. Using these companies, it is likely that North Korea had access to business jurisdictions around the world, including the United States.

Sun Sidong 孙桐东, the owner of one of these sanctioned firms and designated on November 21, 2017 for his association "with front companies for weapons of mass destruction-related North Korean organizations," is a perfect example of this integration.^{109 110} The owner of China-based Dandong Dongyuan Industrial Co. Ltd.

101 The eight firms are: Dandong Hongxiang Industrial Development Co. Ltd., Dandong Zhicheng Metallic Material Co. Ltd., Dandong Tianfu Trade Co. Ltd., Dandong Kehua Economic and Trade Co. Ltd., Jin-hou International Holding Co. Ltd., Dandong Xianghe Trading Co. Ltd., Dandong Hongda Trade Co. Ltd., and Dandong Dongyuan Industrial Co. Ltd.

102 (2017, November 21) Treasury Sanctions Trading, Labor, and Shipping Companies and Vessels to Further Isolate North Korea. United States Department of the Treasury. Retrieved from <https://www.treasury.gov/press-center/press-releases/Pages/sm0220.aspx>.

103 Document held by author, available upon request.

104 Ibid.

105 Ibid.

106 Ibid.

107 Ibid.

108 U.S. v. All Wire Transactions Involving Dandong Zhicheng Metallic Material Company, Ltd., et al., 17-mj-217-DAR-BAH, (D.D.C.). Retrieved from: <http://www.dcd.uscourts.gov/sites/dcd/files/BAHMemoandOrder.pdf>.

109 More information on Sun Sidong and his network can be found in C4ADS' report, *Risky Business*.

110 (2017, November 21) Treasury Sanctions Trading, Labor, and Shipping Companies and Vessels to Further Isolate North Korea. United States Department of the Treasury. Retrieved from <https://www.treasury.gov/press-center/press-releases/Pages/sm0220.aspx>.

丹东源实业有限公司, Mr. Sun is also listed as the president of Dongyuan Enterprise USA Inc., a company based out of Flushing, New York.¹¹¹ ¹¹² Located in a two-story brick house on Robinson Street, the company was registered on May 29, 2015 by Mou Chunna 牟春哪,¹¹³ a manager and minority shareholder in one of Mr. Sun's China-based businesses.¹¹⁴ Customs records state that this US company received a shipment of over six tons of used furniture on March 2, 2017,¹¹⁵ and records show that an application for a H1-B visa was submitted by Dongyuan Enterprise USA Inc. for a Financial Analyst in September of 2016.¹¹⁶ In addition, Mr. Sun, who was identified in our previous report as having exported over \$28 million in dual use goods to North Korea and was later designated by the US Department of the Treasury for these activities, was able to purchase a property in Great Neck, New York valued at over \$1 million in December 2016.¹¹⁷

Fortunately, the ability of companies to do business openly with North Korea and still engage in global commerce may soon come to an end. The September 2016 passage of UN Security Council Resolution 2375 could have a dramatic effect on restrictions surrounding the North Korea regime's main exports. Bans on coal, iron ore, seafood products, and textiles have largely closed pathways for North Korea to sell its most valuable exports openly.¹¹⁸ Internal analysis has shown that, if fully enforced, these measures would restrict 90.5% of 2016 export revenue, or \$2.3 billion annually.¹¹⁹ Executive Order 13810, enacted September 21,



111 (2017) Dongyuan Enterprise USA Inc. Manta. Retrieved from <http://www.manta.com/c/mhbbvy5/dongyuan-enterprise-usa-inc>.

112 New York State Business Registry Filing, document held by author available upon request.

113 Chinese Business Registry Filing, document held by author available upon request. Retrieved from <http://gsxt.saic.gov.cn/>.

114 New York State Business Registry Filing, document held by author available.

115 Document held by author, available upon request.

116 (2017) Dong Yuan Enterprise USA Inc Salaries. Visadoor. Retrieved from <http://visadoor.com/h1b-2016-dong-yuan-enterprise-usa-inc>.

117 Document held by author, available upon request.

118 (2017, September 11). Security Council Imposes Fresh Sanctions on Democratic People's Republic of Korea, Including Bans on Natural Gas Sales, Work Authorization for its Nationals. United Nations. Retrieved from: <https://www.un.org/press/en/2017/sc12983.doc.htm>.

119 Document held by author, available upon request.

2017, further simplifies the negative costs of doing business with North Korea, dramatically lowering the bar for actions that merit sanctions. Among other measures, any company found “to have engaged in at least one significant importation from or exportation to North Korea of any goods, services, or technology,” can be sanctioned by the US Department of the Treasury.¹²⁰ Measures like these are intended to make the potential cost of doing business with North Korea prohibitive. The recent case of ZTE is a striking example of this. In March of 2017, ZTE, a Chinese multinational telecommunications equipment company with annual revenue in the tens of billions of dollars reached an agreement with the US Departments of the Treasury, Justice, and Commerce to pay a combined civil penalty of \$1.19 billion for sanctions and export control violations.¹²¹ While much of its activity focused on export violations related to Iran, documents detailed its violations of export regulations applicable to North Korea using a web of shell companies to obscure its involvement with the regime.¹²²

Financial Leverage: Seizing the Money

New sanctions and actions to enforce them can change the incentive structure companies face in doing business with North Korea and cause large-scale repercussions for the regime’s foreign exchange earnings, but it will take time for these measures to impact the regime’s bottom line. The US Department of Justice has clearly accelerated its targeting of North Korea’s foreign currency income and exchange reserves. Since September 2016, it has filed civil forfeiture complaints against funds held by North Korea-linked companies, including DHID, DZMM, and Mingzheng International Trading Corporation. It has identified North Korea-linked funds in US dollar accounts at some of the world’s largest banks. In the DHID forfeiture action alone, it sued to forfeit 25 bank accounts in 12 banks, including Agricultural Bank of China, China Construction Bank, and Industrial and Commercial Bank of China.¹²³ Funds placed under civil asset forfeiture from these networks, totaling \$84,364,544, represent a portion of the hard currency accounts of North Korea’s foreign exchange banks. They are vital regime assets.¹²⁴

The Department of Justice’s seizures since September 2016 amount to three times what was frozen in 2005 from Banco Delta Asia (BDA) after the US Department of the Treasury named the Macau-based institution as a primary money laundering concern.¹²⁵ According to retired World Bank expert Brad Babson, the \$25 million frozen by Macau from BDA and the closure of its foreign reserve accounts was enough to have “an unusually effective impact.”¹²⁶ Continued targeting of North Korea’s foreign currency accounts will allow the international community to generate additional leverage to coerce the regime into disarmament negotiations. Furthermore, as the entire system is interlinked, actions taken against nodes can lead to the identification of other parts of the network, achieving an unravelling effect and exposing the entire system.

120 (2017, September 21). Presidential Executive Order on Imposing Additional Sanctions with Respect to North Korea. The White House Office of the Press Secretary. Retrieved from: <https://www.whitehouse.gov/the-press-office/2017/09/21/presidential-executive-order-imposing-additional-sanctions-respect-north>.

121 Mozur, P., Kang, C. (2017, March 7). U.S. Fines ZTE of China \$1.19 Billion for Breaching Sanctions. The New York Times. Retrieved from: <https://www.nytimes.com/2017/03/07/technology/zte-china-fine.html>.

122 (2017, March 7). Secretary of Commerce Wilbur L. Ross, Jr. Announces \$1.19 Billion Penalty for Chinese Company’s Export Violations to Iran and North Korea. U.S. Department of Commerce. Retrieved from: <https://www.commerce.gov/news/press-releases/2017/03/secretary-commerce-wilbur-l-ross-jr-announces-119-billion-penalty>.

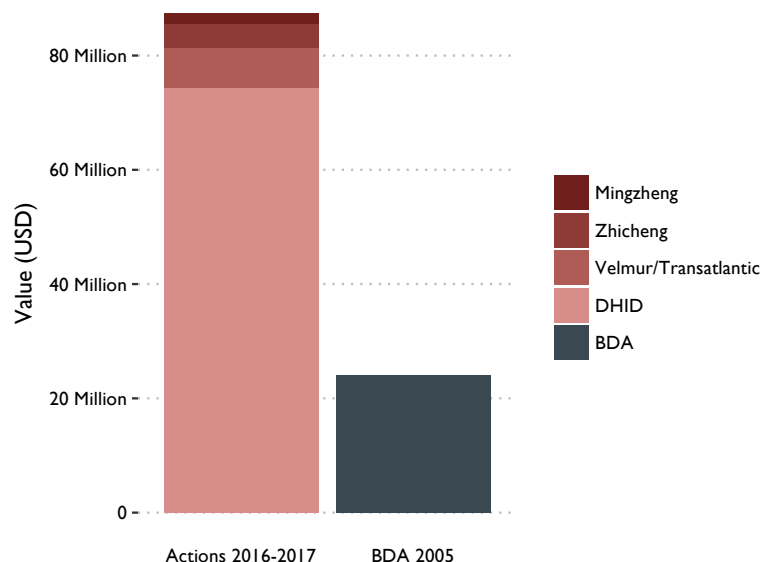
123 U.S. v. All Funds in the Accounts of Blue Sea Business Co., Ltd., et al., Retrieved from: <https://www.justice.gov/opa/file/897051/download>.

124 C4ADS research available upon request.

125 (2005, September 15). Treasury Designates Banco Delta Asia as Primary Money Laundering Concern under USA PATRIOT Act. U.S. Department of the Treasury. Retrieved from: <https://www.treasury.gov/press-center/press-releases/Pages/js2720.aspx>.

126 Lague, D., Greenlees, D. (2007, January 18). Squeeze on Banco Delta Asia hit North Korea where it hurt – Asia – Pacific – International Herald Tribune. The New York Times. Retrieved from: <http://www.nytimes.com/2007/01/18/world/asia/18iht-north.4255039.html?mcubz=3>.

Combined Actions Taken Against North Korean Overseas Assets



Follow the Money: Identifying Targets

As previous reports have shown, tracing transactions between North Korea's overseas networks can begin to link disparate illicit activities through ties to North Korea's system of foreign exchange. Yet the question remains: how can members of international law enforcement bodies identify these networks to enforce the coercive economic measures of successive UN resolutions? The answer lies in following the money. Even the actions of North Korea's premier intelligence agency, the Reconnaissance General Bureau (RGB), are limited by their need to maintain accounts in North Korea's foreign exchange banks.

The RGB, which the US Department of the Treasury designated in August 2010, "trades in conventional arms and controls ... Green Pine Associated Corporation (Green Pine), which was also identified for sanctions by the President ... for exporting arms or related materiel from North Korea."¹²⁷ To raise hard currency for the regime, RGB and Green Pine have reportedly sold conventional weapons to countries around the world, including Syria,¹²⁸ Egypt,¹²⁹ and the UAE.¹³⁰ In this respect, these weapons proliferators serve a role analogous to those of the "strategic chokepoint" trading companies, such as DHID and DZMM. Just as in the cases of DHID and DZMM, the illicit networks employed by RGB are both connected to North Korean illicit activity and to the illicit system of North Korean overseas finance.

Reporting done by Reuters and the UN POE highlights the extent of the network surrounding the RGB's use of the Malaysia-based firm Global Communications (Glocom). Although North Korean companies have been banned since 2009 from exporting arms and related material, Glocom, operating under the slogan "Anywhere,

127 (2010, August 30) Fact Sheet: New Executive Order Targeting Proliferation and Other Illicit Activities Related to North Korea. US Department of the Treasury. Retrieved from: <https://www.treasury.gov/press-center/press-releases/Pages/tg839.aspx>.

128 Pearson, J. (2014, March 11) Front companies, embassies mask North Korean weapons trade-U.N. Reuters. Retrieved from: <https://www.reuters.com/article/us-korea-korea-un/front-companies-embassies-mask-north-korean-weapons-trade-u-n-idUSBREA2A08020140311>.

129 Warrick, J. (2017, October 1) A North Korean ship was seized off Egypt with a huge cache of weapons destined for a surprising buyer. The Washington Post. Retrieved from: https://www.washingtonpost.com/world/national-security/a-north-korean-ship-was-seized-off-egypt-with-a-huge-cache-of-weapons-destined-for-a-surprising-buyer/2017/10/01/d9a4e06e-a46d-11e7-b14f-f41773cd5a14_story.html?utm_term=.cd0b3606a667.

130 Ramani, R. (2017, August 8) Why Did UAE Purchase Weapons from North Korea. The Diplomat. Retrieved from: <https://thediplomat.com/2017/08/why-did-the-uae-purchase-weapons-from-north-korea/>.

Anytime in Battlefield,” has sold radio systems meant for military and paramilitary organizations.¹³¹ In July 2016, customs agents interdicted an air shipment headed to Eritrea that had originated in China. The cargo of 45 boxes, bound for Eritech Computer Assembly & Communications Technology PLC, was made up of high-frequency software-defined radios, crypto-speaker microphones, GPS antennas, high-frequency whip antennas, clone cables, camouflaged rucksacks, and carry pouches.¹³² Some of the boxes were labeled Glocom, and some included material marked “made in DPR Korea.”¹³³

Although Glocom maintains an office in the “Little India” neighborhood of Kuala Lumpur, no company exists under the name Global Communications in the Malaysian business registry.¹³⁴ However, two Malaysian front companies operated by North Koreans, International Golden Services Sdn Bhd and International Global Systems Sdn Bhd, operate Glocom out of its second-floor “Little India” office.¹³⁵ Furthermore, the UN POE shows Glocom is a front company for the North Korean firm Pan Systems Pyongyang.¹³⁶ Both International Golden Services and Pan Systems Pyongyang are controlled by RGB agent Ryang Su Nyo,¹³⁷ ¹³⁸ who has been involved in multiple instances of illicit activity involving the raising of hard currency for the regime. In February 2014, for example, Ryang and two other North Korean agents were detained in Kuala Lumpur International Airport for attempting to smuggle \$450,000 in cash through customs.¹³⁹ When questioned, the trio told Malaysian authorities that the funds belonged to the North Korean embassy.¹⁴⁰ Through Pan Systems Pyongyang and under the alias Wonbang Trading Co., Ryang may also be involved in revenue generation through RGB coal exports.¹⁴¹ The UN POE has stated that an investigation is ongoing to determine whether this company is in fact Wonbong Trading Co., a leading North Korean coal exporter run by the RGB.¹⁴²

Ryang is reportedly an employee of the RGB’s Liaison Office 519,¹⁴³ an organization that specializes in overseas operations to conduct arms sales and weapons procurement.¹⁴⁴ In the past, Ryang’s Pan Systems Pyongyang had transacted with multiple organizations related to North Korean weapons procurement.¹⁴⁵ According to media reports, the organization has even sold arms to Somali pirates.¹⁴⁶ Between 2011 and 2015, Pan Systems Pyongyang had regular transactions with the sanctioned North Korean weapons proliferator

131 Pearson, J., Latiff, R. (2017, February 26) North Korea spy agency runs arms operation out of Malaysia, U.N. says. Reuters. Retrieved from: <https://www.reuters.com/article/us-northkorea-malaysia-arms-insight/north-korea-spy-agency-runs-arms-operation-out-of-malaysia-u-n-says-idUSKBN1650YE>.

132 (2017, February 27). United Nations Security Council Report of Resolution 2276 (2016). United Nations Security Council.

133 Ibid.

134 Pearson, J., Latiff, R. (2017, February 26) North Korea spy agency runs arms operation out of Malaysia, U.N. says. Reuters. Retrieved from: <https://www.reuters.com/article/us-northkorea-malaysia-arms-insight/north-korea-spy-agency-runs-arms-operation-out-of-malaysia-u-n-says-idUSKBN1650YE>.

135 Ibid.

136 Ibid.

137 Malaysian Business Registry Filing. Document held by author, available upon request.

138 (2017, February 27). United Nations Security Council Report of Resolution 2276 (2016). United Nations Security Council.

139 Pearson, J., Latiff, R. (2017, February 26) North Korea spy agency runs arms operation out of Malaysia, U.N. says. Reuters. Retrieved from: <https://www.reuters.com/article/us-northkorea-malaysia-arms-insight/north-korea-spy-agency-runs-arms-operation-out-of-malaysia-u-n-says-idUSKBN1650YE>.

140 (2017, February 27). United Nations Security Council Report of Resolution 2276 (2016). United Nations Security Council.

141 Ibid.

142 Ibid.

143 Ibid.

144 Kim, S. (2016, March 7) The web structure of “Room 39” and other North Korean Foreign Currency Operations. Mediapen. Retrieved from: <http://www.mediapen.com/news/view/128167>.

145 (2017, February 27). United Nations Security Council Report of Resolution 2276 (2016). United Nations Security Council.

146 Kim, S. (2016, March 7) The web structure of “Room 39” and other North Korean Foreign Currency Operations. Mediapen. Retrieved from: <http://www.mediapen.com/news/view/128167>.

KOMID.¹⁴⁷ In 2010 and 2013 the company also made transactions to the Hong Kong-based company Greenpine International, whose sole shareholder, Kim Song Il, was arrested in Hawaii attempting to purchase night vision goggles from a federal agent.¹⁴⁸ Information provided to C4ADS by someone with knowledge of the Glocom network indicates that one of the RGB representatives, Kim Chang Hyok, met with an Egyptian general in 2011.¹⁴⁹ Reporting by the Washington Post confirmed that a seized shipment of \$23 million worth of rocket propelled grenades was found aboard the North Korean ship the Jie Shun,¹⁵⁰ which was purchased by the Egyptian government.¹⁵¹ Estimates claim North Korea raises between \$100 and \$300 million annually through the sale of arms and related material.^{152 153}

To be of use to the regime, funds generated by Ryang and Glocom's illicit military equipment sales, like those stolen from the Bangladesh Central Bank, would need to be placed within the North Korean foreign exchange system. To access the international financial system and procure arms and related material, Pan Systems Pyongyang and its front companies used an extensive network of offshore bank accounts. These accounts, in both dollars and euros, were operated by Daedong Credit Bank (DCB), a sanctioned subsidiary of Korea Daesong Bank (KDB) and third arm of North Korea's foreign exchange system.^{154 155} Since 1998, DCB had helped Ryang to move money in and out of North Korea—between Pan Systems and more than 20 companies on the Chinese mainland, in Hong Kong, and in Singapore.¹⁵⁶

Korea Daesong Bank: The financial arm of North Korea's Office 39, Korea Daesong Bank (KDB) was sanctioned by the US Department of the Treasury in November 2010. This institution engaged in illicit economic activities and managed slush funds for North Korean leadership.¹⁵⁷ KDB and Korea Daesong General Trading Company, designated by the US Department of the Treasury on the same day, were "key components of Office 39's financial network supporting North Korea's illicit and dangerous activities."¹⁵⁸ A subsidiary of KDB, Daesong Credit Bank (DCB), was sanctioned in June 2013. This front had been used to carry out international financial transactions to avoid scrutiny by financial institutions screening transactions related to North Korea."¹⁵⁹

Just as with FTB and KKBC, KDB and its subsidiary DCB have had to take countermeasures to maintain their

147 (2017, February 27). United Nations Security Council Report of Resolution 2276 (2016). United Nations Security Council.

148 Whitehurst, L. (2016, February 25) North Korea man to be sentenced in night-vision goggle case. AP. Retrieved from: <http://www.businessinsider.com/ap-north-korea-man-to-be-sentenced-in-night-vision-goggle-case-2016-2>.

149 Confidential Source.

150 For more information on the network surrounding the Jie Shun see the June 2017 C4ADS report, *Risky Business*.

151 Warrick, J. (2017, October 1) A North Korean ship was seized off Egypt with a huge cache of weapons destined for a surprising buyer. The Washington Post. Retrieved from: https://www.washingtonpost.com/world/national-security/a-north-korean-ship-was-seized-off-egypt-with-a-huge-cache-of-weapons-destined-for-a-surprising-buyer/2017/10/01/d9a4e06e-a46d-11e7-b14f-f41773cd5a14_story.html?utm_term=.cd0b3606a667.

152 (2010, November 5). United Nations Security Council Report of Resolution 1874 (2009). United Nations Security Council.

153 (2016, April 29) N. Korean Arms Dealers Run Out of Safe Havens. The Chosun ilbo. Retrieved from: http://english.chosun.com/site/data/html_dir/2016/04/29/2016042901075.html.

154 (2017, February 27). United Nations Security Council Report of Resolution 2276 (2016). United Nations Security Council.

155 (2010, November 18). Treasury Designates Key Nodes of the Illicit Financing Network of North Korea's Office 39. U.S. Department of the Treasury. Retrieved from: <https://www.treasury.gov/press-center/press-releases/Pages/tg962.aspx>.

156 (2017, February 27). United Nations Security Council Report of Resolution 2276 (2016). United Nations Security Council.

157 (2010, November 18). Treasury Designates Key Nodes of the Illicit Financing Network of North Korea's Office 39. U.S. Department of the Treasury. Retrieved from: <https://www.treasury.gov/press-center/press-releases/Pages/tg962.aspx>.

158 Ibid.

159 (2013, June 27). Treasury Sanctions Bank, Front Company, and Official Linked to North Korean Weapons of Mass Destruction Programs. U.S. Department of the Treasury. Retrieved from: <https://www.treasury.gov/press-center/press-releases/Pages/jl1994.aspx>.

ability to serve their North Korean customers—in this case, agents of North Korea’s main foreign intelligence agency. As in other cases, to ensure the capacity to transact with international suppliers in foreign currency, these institutions used bank accounts held by front companies. In this regard, specific transaction records recovered by C4ADS highlight the global integration DCB was able to leverage on Glocom’s behalf.

In January 2013, an East Asian electronics reseller received a payment of a little over \$15,000 from the Hong Kong-based company Shengang Trade & Investment 深光贸易投资有限公司.¹⁶⁰ The reseller was unaware that it was doing business with North Korea; Glocom representative Pyon Won Gu had informed the company that payment would come from Glocom’s representative in China.¹⁶¹ The components purchased were destined for Glocom, and prominently displayed within communications equipment in the company’s online catalog.¹⁶² While there was no overt linkage to North Korea, the Hong Kong-based company is a prime example of a remitting front company for DCB, effectively obscuring the regime’s presence in the international financial system. The remittance payment even passed through a correspondent account held at Bank of America.¹⁶³

Shengang Trade & Investment was incorporated on June 17, 2011. Its sole shareholder, Sun Chon Lam 孫春琳, listed a director residential address in Dandong, China.¹⁶⁴ As is common among North Korean foreign exchange bank front companies, the firm was active in multiple jurisdictions around the world. In addition to remittances on behalf of Glocom, Shengang Trade & Investment has made purchases from Russia, which appear to be on the regime’s behalf. Russian customs records show Shengang Trade & Investment as the consignor of a March 1, 2017 shipment of 289 tons of seafood products, sent from Russia to North Korea.¹⁶⁵ Imports came from PKF Severo-Kurilsky Rybokombinat, a Russian fishery operating in Sakhalin Oblast.¹⁶⁶ According to trade records, exports to North Korea by the Russian company were sent to only one additional company. On June 7, 2017, Korea Chongsong Trading Co. received a shipment of seafood products from the Russian company.¹⁶⁷ ¹⁶⁸ “Chongsong” means “green pine” in Korean, and is one of several UN-recognized aliases of the North Korean weapons proliferator Green Pine Associated Corporation. While there is no direct evidence that the companies are linked, the connection seems highly probable given that North Korean organizations often maintain naming standardization.

Like the North Korean regime, the RGB is reliant on access to foreign currency to function. Although it is the country’s main foreign intelligence agency, large pieces of RGB’s internal infrastructure are built to ensure positive cash flow through a diversified set of illicit activities: Glocom using sales of military equipment,¹⁶⁹ the Lazarus group through hacking,¹⁷⁰ and Wonbang Trading Co. Ltd. through sales of coal.¹⁷¹ Glocom’s ties to the foreign exchange system through accounts at DCB illustrate the same institutional bottleneck seen in various other North Korean networks. The system is fundamentally interconnected and vulnerable. The success of North Korea’s illicit activities is contingent on a range of foreign entities providing key services,

¹⁶⁰ Confidential source.

¹⁶¹ Confidential source.

¹⁶² Document held by author available upon request.

¹⁶³ Confidential source.

¹⁶⁴ Hong Kong Business Registry Filing, document held by author available upon request. Retrieved from <http://www.icris.cr.gov.hk>.

¹⁶⁵ Document held by author available upon request.

¹⁶⁶ Ibid.

¹⁶⁷ (n.d.) Dalryba.ru Retrieved from: <http://www.dalryba.ru/content/trebuetsya-mtr>

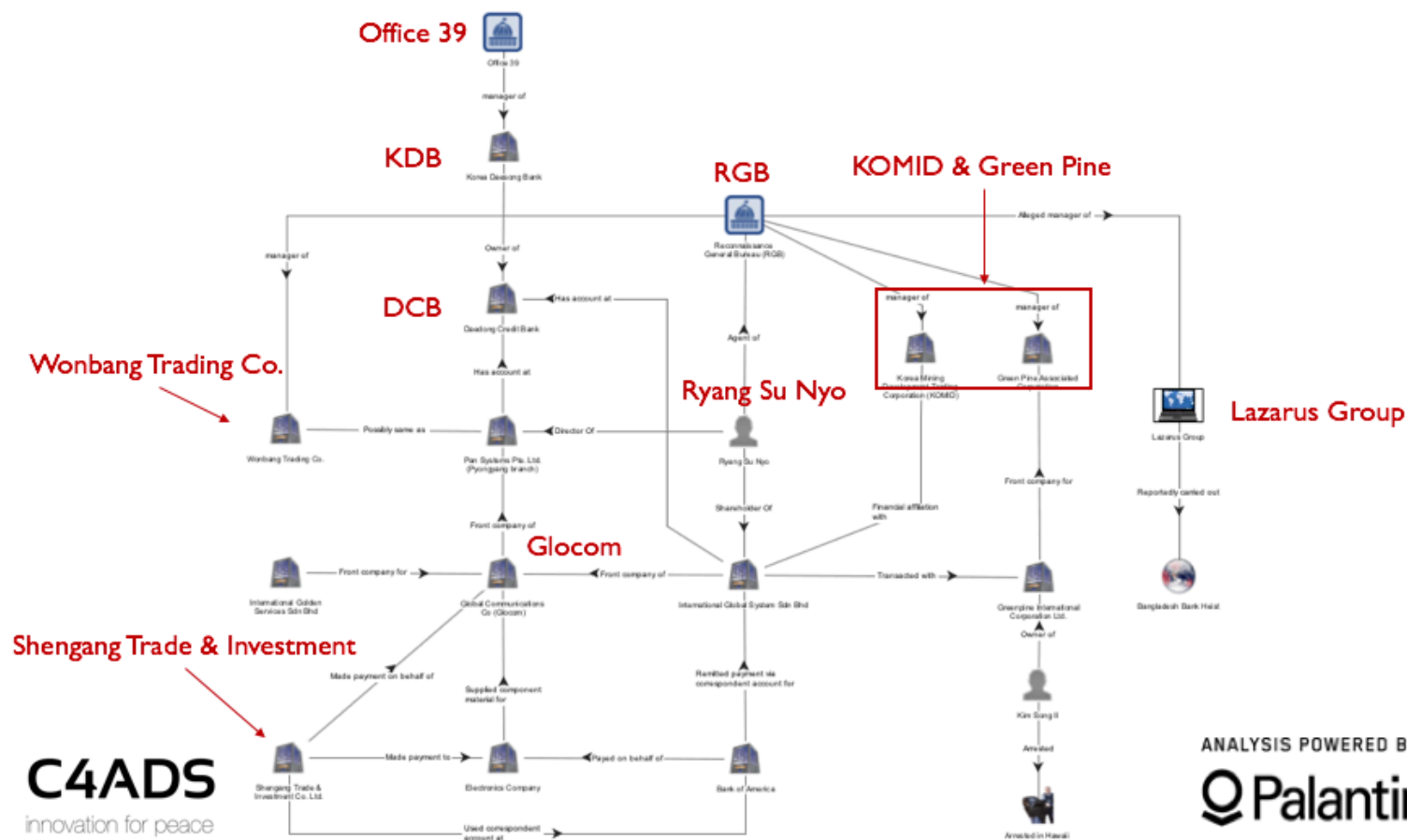
¹⁶⁸ Document held by author available upon request.

¹⁶⁹ (2017, February 27). United Nations Security Council Report of Resolution 2276 (2016). United Nations Security Council.

¹⁷⁰ (2017, April 03). Chasing Lazarus: A Hunt for the Infamous Hackers to Prevent Large Bank Robberies. Kaspersky Lab. Retrieved from: https://www.kaspersky.com/about/press-releases/2017_chasing-lazarus-a-hunt-for-the-infamous-hackers-to-prevent-large-bank-robberies.

¹⁷¹ (2017, February 27). United Nations Security Council Report of Resolution 2276 (2016). United Nations Security Council.

from passing through payments to providing logistics, none of which North Korea can control. However, it is an environment that the international community does control. By levying fines, denying access to the US financial system, seizing assets, and filing indictments, it is possible to expose and disrupt this system. It is imperative to follow the money.



Conclusion

The past year has seen a tremendous change in North Korea's economic environment. The quick and unanimous passage of UNSCR 2371 and 2375 has restricted 90.5 percent of North Korean export revenue from 2016.¹⁷² In addition, nearly 80 percent of North Korean export shipments from 2016 are now banned under UN restrictions,¹⁷³ and new visas for North Korean overseas laborers have been prohibited.¹⁷⁴ These actions, if enforced uniformly and completely, will have a significant, negative impact on the North Korean economy, denying the regime billions in annual revenue. In the past, North Korea has survived sanctions by outsourcing financial services and procurement networks to maintain access to hard currency and materiel. As future restrictions seek to further shrink the operating environment for North Korea's overseas networks, the regime will have a harder and harder time accessing the services and earning revenue the regime so vitally needs. If the international community continues to exert financial pressure, we will possibly reach a point where North Korea will not be able to adapt to this kind of challenge.

Access to hard currency is vital for the regime to maintain its grip on power. As demonstrated by the networks in this report, the foreign exchange banks that the regime has tasked with holding and transacting foreign currency have shown tremendous levels of ingenuity to circumvent international sanctions and raise revenue. These networks and companies have functioned by finding commercial counterparts that would benefit from doing business with North Korea, often because of lucrative North Korean exports like coal, and they have subsequently outsourced their financial responsibilities to their commercial counterparts. These incentives may no longer be worth the risk, as civil asset forfeitures against companies working on North Korea's behalf might indicate and as UN Security Council resolutions continue to shrink North Korea's viable operating environment. Looking ahead, the international community must exercise and enforce these new restrictions to more effectively exert financial leverage. As seen in the case of Glocom's use of Shengang Trade & Investment, these companies do rely on the international system to function overseas, including using major dollar clearing banks. Addressing this dependence is the surest way to begin to cut off North Korea's foreign exchange banks from their assets and the regime from its foreign reserve accounts.

Even as the international community has taken increasingly restrictive steps to deter the regime from continuing its pursuit of WMD, the regime has maintained its provocative stance, testing a ballistic missile as recently as November 28, 2017.¹⁷⁵ International sanctions have fundamentally changed the way that the North Korean economy functions, making it inherently vulnerable and providing the means to pursue additional non-violent coercion. Links between disparate networks have begun to show that actions taken against one network can have disrupting effects against the whole system. The hard currency the Kim regime has used to procure proliferation material for its nuclear and missile program and fund its international sanctions evasion network may end up being its greatest vulnerability. It is the most compelling means to force the regime to return to the negotiating table.

North Korea is reliant on a system it does not control. Its vulnerabilities are economic; our leverage is financial.

172 Document held by author, available upon request.

173 Ibid.

174 (2017, September 11). Security Council Imposes Fresh Sanctions on Democratic People's Republic of Korea, Including Bans on Natural Gas Sales, Work Authorization for its Nationals. United Nations. Retrieved from: <https://www.un.org/press/en/2017/sc12983.doc.htm>.

175 Fifield, A. (2017, November 29). North Korea's latest missile launch appears to put U.S. capital in range. The Washington Post. Retrieved from: https://www.washingtonpost.com/world/north-korea-fires-missile-for-the-first-time-in-more-than-two-months/2017/11/28/0c136952-d46c-11e7-9461-ba77d604373d_story.html?utm_term=.3e62896c70a6

C4ADS

innovation for peace



세종연구소

THE SEJONG INSTITUTE

