Royal United Services Institute
for Defence and Security Studies

Occasional Paper

Closing the Crypto Gap

Guidance for Countering North Korean Cryptocurrency Activity in Southeast Asia

David Carlisle and Kayla Izenman

Closing the Crypto Gap

Guidance for Countering North Korean Cryptocurrency Activity in Southeast Asia

David Carlisle and Kayla Izenman

RUSI Occasional Paper, April 2019

Royal United Services Institute
for Defence and Security Studies

188 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 188 years.

Published in 2019 by the Royal United Services Institute for Defence and Security Studies.

RUSI Occasional Paper, April 2019. ISSN 2397-0286.

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org

RUSI is a registered charity (No. 210639)

Contents

Executive Summary

DESPITE RECENT DIPLOMATIC progress with the US, North Korea remains the world's most significant weapons of mass destruction (WMD) proliferation threat. North Korea has gone to extremes to raise funds and evade international sanctions, recently expanding these efforts to include the exploitation of cryptocurrencies such as Bitcoin. Cryptocurrencies likely play only a peripheral role in North Korea's overall fundraising and sanctions-evasion activity. However, the sophistication of North Korea's broader cybercrime operations and its general demand for ongoing financial resources present the risk that its cryptocurrency activity could become a sustained security challenge, particularly as international sanctions lead North Korea to seek financial lifelines outside the mainstream sector. The UN Security Council's Panel of Experts on North Korea has suggested that cryptocurrencies offer North Korea 'more ways to evade sanctions given that they are harder to trace, can be laundered many times and are independent from government regulation'.[1]

In general, North Korea could seek to use cryptocurrencies as part of its proliferation financing efforts through:

- Fundraising: To sustain its ongoing needs for cash, North Korea may obtain cryptocurrencies with the aim of converting them to fiat currencies in the short term.
- Stockpiling: North Korea could accumulate reserves of cryptocurrencies with the objective of eventually spending them or converting them into fiat currency at some point in the future.
- Circumvention: North Korea could use cryptocurrencies to pay directly for goods, services and resources that are explicitly prohibited by international sanctions.

Southeast Asia has long been vulnerable to North Korea's WMD proliferation financing and sanctions-evasion activities, given its proximity to North Korean proliferation networks and the availability of sophisticated trade and finance infrastructure. The region is vulnerable to North Korea's cryptocurrency-enabled activity as well, and important gaps remain.

For example, gaps in local regulatory frameworks could allow North Korea, or other actors, to exploit cryptocurrency exchanges and other related platforms. Since Southeast Asia also features a nascent but burgeoning cryptocurrency industry, local law enforcement agencies will likely require further knowledge and resources to ensure that they can successfully respond to cryptocurrency-related criminal activity over time should the local cryptocurrency industry continue to grow in scale.

---

1. United Nations Security Council, 'Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)', 21 February 2019, S/2019/171, p. 51.

By taking steps such as developing effective regulatory frameworks and leveraging public–private partnership initiatives, countries in the region can mitigate North Korea's cryptocurrency activity successfully.

Introduction

CRYPTOCURRENCIES ARE DECENTRALISED, peer-to-peer (P2P) payment technologies that enable counterparties to exchange value without a regulated financial institution or other intermediary.[1] Consequently, cryptocurrencies have become a favoured tool for illicit actors, such as cybercriminals, seeking to operate outside the regulated financial sector.

As international sanctions against North Korea have expanded and pressure has increased on financial institutions to disrupt North Korea's financial networks, the regime has been forced to find creative ways to evade sanctions. Consequently, since at least early 2017, North Korea has undertaken efforts to exploit cryptocurrencies.

The most highly publicised of North Korea's cryptocurrency-enabled activities to date is the May 2017 WannaCry ransomware attack, which generated only a modest amount of cryptocurrency for North Korean-affiliated cybercriminals who executed it, but caused widespread disruption and signalled North Korea's desire and ability to sponsor cryptocurrency-enabled cybercrime. While it is difficult to determine the exact scale and scope of North Korea's cryptocurrency-related activity, public reporting suggests that it has become more frequent and lucrative since the WannaCry attack, particularly in the form of large-scale hacking of cryptocurrency exchanges in South Korea.[2]

North Korea has, for a number of years, deployed sanctions evasion techniques in Southeast Asia. North Korean networks have engaged in fundraising and have evaded trade and financial restrictions through the use of front companies, agents and deceptive financial techniques at banks across the region. Because Southeast Asia is also host to a growing number of cryptocurrency businesses and users, countries in the region could prove vulnerable to North Korea's cryptocurrency-related activity as well.

1. This paper generally relies on the popular term 'cryptocurrency', but also uses it interchangeably with the terms 'cryptoasset', 'virtual currency' and 'virtual asset' when referring to specific sources and regulatory measures that employ those terms.
2. See Cointelegraph, 'North Korea News', <https://Cointelegraph.com/tags/north-korea>, accessed 26 March 2019; CoinDesk, 'Browsing the "North Korea" Tag', <https://www.coindesk.com/tag/north-korea>, accessed 26 March 2019.

To that end, countries in Southeast Asia may wish to consider the following recommendations to ensure resiliency against the risk of North Korean cryptocurrency activity.

- **Assess risk exposure.** Aligned with guidance issued by the Financial Action Task Force (FATF),[3] individual countries in Southeast Asia should undertake risk assessments of their exposure to financial crime threats involving cryptocurrencies. Regional partners should also consider undertaking a coordinated, region-wide risk assessment exercise to measure cross-cutting vulnerabilities that expose Southeast Asian states to the types of cryptocurrency-enabled cybercrime that North Korea has perpetrated.
- **Close regulatory and security gaps.** Countries in Southeast Asia that have yet to do so should implement regulation around cryptocurrencies that is consistent with the FATF's October 2018 call for countries to regulate with urgency.[4] Those countries that have already implemented regulation should ensure that regulatory frameworks are supported by clear guidance and robust enforcement capabilities.
- **Enable interagency collaboration.** Countries in Southeast Asia should ensure they have appropriate interagency collaborative mechanisms at the local level for pooling interagency resources necessary for mitigating cryptocurrency-related risks.
- **Develop coordinated regional responses.** In addition to ensuring collaboration at the domestic level, countries in Southeast Asia may wish to coordinate strategies for mitigating vulnerabilities to cryptocurrency-related financial crime, including cybercrime, in which North Korea is engaged.
- **Enhance law enforcement knowledge and capacity.** Countries in the region should also consider expanding training and capacity-building efforts for equipping law enforcement agencies to investigate and act against illicit activity involving cryptocurrencies.
- **Promote private sector education and awareness.** Governments in Southeast Asia may wish to encourage and facilitate educational and awareness-building efforts among local cryptocurrency industry participants to ensure a robust first line of defence against North Korea's illicit activity in cryptocurrencies.
- **Facilitate public–private partnership.** The public sector throughout Southeast Asia should enlist the local cryptocurrency industry in supporting the above objectives.

This paper sets out practical guidance for achieving the objectives outlined above. It is organised as follows.

Chapter I highlights key risks of North Korea's cryptocurrency-enabled activity and presents relevant factors for regional stakeholders to consider. It draws on a literature review that considers press reports and studies by private security analysis firms. Non-attributable author interviews held with experts in cryptocurrencies, North Korean sanctions-evasion techniques and cybercrime capabilities, and related topics constitute the data-collection phase of the study.

3. The FATF is the global standard-setting body for anti-money-laundering and counterterrorist-financing (AML/CTF) regulation.
4. FATF, 'Regulation of Virtual Assets', 19 October 2018.

Given the sensitivity of their work on this topic, the identities of interviewees were witheld, but information about their relevant expertise is provided for transparency.

Chapter II considers specific vulnerabilities that Southeast Asian countries face from illicit cryptocurrency activity, providing a brief overview of the nature of cryptocurrency adoption and activity throughout the region.

Chapter III provides detailed, practical guidance for regional stakeholders to both mitigate the risks and reduce the vulnerabilities outlined in Chapters I and II. It builds on previous counter-proliferation finance (CPF) guidance produced by RUSI,[5] illustrating how international anti-money laundering/counterterrorist financing (AML/CTF) and CPF measures can be applied to cryptocurrency-related activity.

5. See Anagha Joshi, 'Model Provisions to Combat the Financing of the Proliferation of Weapons of Mass Destruction: Second Edition', RUSI, October 2018; Emil Dall, Tom Keatinge and Andrea Berger, 'Countering Proliferation Finance: An Introductory Guide for Financial Institutions', RUSI Guidance Paper, April 2017.

I. North Korea's Cryptocurrency Activity: Key Threats and Risks

THIS CHAPTER PROVIDES observations regarding North Korea's use of cryptocurrencies within the context of its broader sanctions-evasion and cybercrime activity, noting key risks and threats.

Observation 1: Motivations

Pressure from international sanctions has led North Korea to pursue complex evasion techniques, which increasingly rely on sophisticated cybercrime operations.

North Korea is subject to extensive international sanctions, including measures imposed by the UN, the US, the EU and others. These measures include: prohibitions on the provision of financial services to designated North Korean individuals and entities, as well as entities affiliated with them; restrictions on the trade of raw materials (such as coal) with North Korea; and restrictions on the provision of luxury goods to the North Korean regime. Individuals or entities who violate these restrictions and engage in prohibited business with North Korea can face civil and criminal penalties (see Box 1 for a detailed summary of restrictions).

To circumvent these restrictions, North Korea has employed numerous techniques to raise and move funds, and to access prohibited goods and services. These sanctions-evasion methods allow North Korea to finance its weapons of mass destruction (WMD) programmes directly, and to raise funds for its ongoing operations, such as procuring luxury goods and other prohibited items, or paying salaries to overseas affiliates and middlemen. These methods are sophisticated and wide-ranging. As the US Department of the Treasury has claimed:

> Although U.S. and international sanctions have served to significantly isolate North Korean banks from the international financial system, the North Korean government continues to access the international financial system to support its WMD and conventional weapons programs. This is made possible through its use of aliases, agents, foreign individuals in multiple jurisdictions, and a long-standing network of front companies and North Korean embassy personnel which support illicit activities through banking, bulk cash, and trade ... North Korean-linked front companies … are often registered by non-North Korean citizens, and ... conceal their activity through the use of indirect payment methods and circuitous transactions disassociated from the movement of goods or services.[6]

6. US Department of the Treasury Financial Crimes Enforcement Network (FinCEN), 'Finding that the Democratic People's Republic of Korea is a Jurisdiction of Primary Money Laundering Concern', *Federal Register* (Vol. 81, No. 106, 2 June 2016), pp. 35, 442.

North Korea's sanctions evasion activity relies on its ability to exploit both witting and unwitting participants in third countries. China, which receives over 90% of North Korean exports,[7] has featured most significantly in North Korea's sanctions-evasion techniques. However, Southeast Asia has also featured prominently. North Korea has accessed goods and services locally through several methods, including: establishing front companies;[8] exploiting regional ports to re-export prohibited goods such as coal;[9] acquiring luxury goods from Southeast Asian businesses;[10] obtaining passports and identity documents from local countries to conceal links to North Korea;[11] and deploying smuggling networks to carry bulk cash and gold across borders.[12]

Box 1: Overview of International Sanctions Measures Targeting North Korean WMD Proliferation

The UN and individual jurisdictions have imposed sanctions against North Korea. These measures do not specifically mention cryptocurrencies, but apply to activity facilitated using any method, including cryptocurrencies.

UN: Since North Korea's first nuclear test in 2006, the UN Security Council (UNSC) has unanimously passed nine rounds of sanctions and created a Panel of Experts to support sanctions implementation among member states. UNSC sanctions have expanded in response to North Korea's nuclear and missile tests, and now include bans on arms trade, military equipment, dual-use technology, transport vehicles, certain luxury goods, natural gas imports, industrial machinery and metals. Activity-based restrictions apply, including restrictions on establishing joint ventures with North Korean entities, on North Korean banks' foreign operations, and on North Korean embassies conducting non-diplomatic business. The UNSC has also prohibited the provision of financial and other services to individuals and entities involved in North Korea's weapons programmes and others designated on the UN sanctions list.

US: The US has significantly increased North Korean sanctions since 2016. In 2017, Treasury Secretary Steven Mnuchin stated that 'foreign financial institutions are now on notice that, going forward, they can choose to do business with the United States or with North Korea, but not both'. US sanctions include: designations of individuals and entities involved with North Korea's WMD programme; arms trade; and mineral or metal trades. President Donald Trump expanded these sanctions to allow the US to freeze the assets of any individual, entity, vessel, or aircraft involved in trading in goods, services,

7. Eleanor Albert, 'The China–North Korea Relationship', Council on Foreign Relations Backgrounder, 13 March 2018.
8. Daniel Salisbury and Endi Mato, 'How North Korea Evades Sanctions in Southeast Asia: The Malaysia Case', *The Diplomat*, 20 July 2017.
9. Bertil Lintner, 'North Korea Eludes Coal Export Ban Via Vietnam', *Asia Times,* 8 February 2018.
10. Karishma Vaswani, 'UN Draft Report Claims Singapore Firms Illegally Sent Luxury Goods', *BBC News*, 12 March 2018.
11. Andrea Berger and Ching N Fung, 'Business or Pleasure? A N. Korean–Cambodian Arrested in Hawaii', *NKNews.org,* 7 August 2015.
12. Andrea Berger, 'A House Without Foundations: The North Korea Sanctions Regime and its Implementation', *Whitehall Report*, 3-17 (June 2017), p. 37.

or technology with North Korea. The US Department of State has designated North Korea as a state sponsor of terrorism, which subjects it to further sanctions, such as controls on the provision of dual-use goods. According to the US Department of State, 'To designate a country as a State Sponsor of Terrorism, the Secretary of State must determine that the government of such country has repeatedly provided support for acts of international terrorism'.

EU: Since 2006, the EU has implemented the UN's restrictive measures against North Korea and has adopted autonomous measures to reinforce the UNSC resolutions. The EU has imposed a ban on trade in gold, precious metals and diamonds with the North Korean government. The EU has also designated individuals involved in North Korea's weapons programmes, who are subject to EU asset-freezing measures.

South Korea: South Korea imposed sanctions against North Korea in 2010, following the sinking of a South Korean warship. Sanctions include a ban on North Korean ships from entering South Korean waters, a halt on many economic and cultural exchanges, and a suspension of trade.

Japan: Japan has restricted diplomatic and commercial exchanges with North Korea. Remittances to North Korea are prohibited.

Australia: Australia has added autonomous sanctions to the UN sanctions programme, including restrictions on the export or supply of specified goods and services and restrictions on commercial activities, vessels, aircraft, scientific and technical cooperation, and North Korean bank accounts.

Sources: For UN: United National Security Council (UNSC) Resolution 2207, 4 March 2015, S/RES/2207; UNSC Resolution 2270, 2 March 2016, S/RES/2270; UNSC Resolution 2276, 24 March 2016, S/RES/2276; UNSC Resolution 2321, 30 November 2016, S/RES/2321; UNSC Resolution 2345, 23 March 2017, S/RES/2345; UNSC Resolution 2356, 2 June 2017, S/RES/2356; UNSC Resolution 2371, 5 August 2017, S/RES/2371; UNSC Resolution 2375, 11 September 2017, S/RES/2375; UNSC Resolution 2397, 22 December 2017, S/RES/2397; UNSC Resolution 2407, 21 March 2018, S/RES/2407. For US: US Department of the Treasury, 'North Korea Sanctions,' last updated 31 January 2019, <https://www.treasury.gov/resource-center/sanctions/Programs/pages/nkorea.aspx>, accessed 14 March 2019; Steven Mnuchin, 'Remarks by Secretary Mnuchin on President Trump's Executive Order on North Korea', speech given at UN General Assembly Press Briefing, New York, 21 September 2017, <https://www.treasury.gov/press-center/press-releases/Pages/sm0162.aspx>, accessed 14 March 2019; US Department of State, 'Chapter 2: State Sponsors of Terrorism', Country Reports on Terrorism 2017, 2017, <https://www.state.gov/j/ct/rls/crt/2017/282847.htm>, accessed 14 March 2019. For EU: European Council and Council of the European Union, 'EU Restrictive Measures Against North Korea', last reviewed 14 February 2019, <https://www.consilium.europa.eu/en/policies/sanctions/history-north-korea/>, accessed 14 March 2019. For South Korea: Joyce Lee and Hyonhee Shin, 'South Korea Says No Change on North Korean Sanctions', Reuters*, 11 October 2018; Justin McCurry, 'Seoul Shuts Down Joint North–South Korea Industrial Complex',* The Guardian*, 10 February 2016;* BBC News*, 'What is the Kaesong Industrial Complex?', 10 February 2016. For Japan: Reiji Yoshida, 'Japan Reimposes Ban on Visits by North Korean Nationals and Ships',* Japan Times*, 10 February 2016;* BBC News*, 'Japan Expands Unilateral Sanctions Against North Korea', 15 December 2017. For Australia:*

Australian Government Department of Foreign Affairs and Trade, 'Sanctions: Democratic People's Republic of Korea (North Korea)', <https://dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/north-korea/Pages/default.aspx>, accessed 14 March 2019.

More recently, North Korea's sanctions-evasion methods have evolved to include financially motivated cybercrime.

Over the past decade, North Korea has developed a sophisticated cybercrime apparatus that enables it to engage in disruptive activity short of actual conflict. As Mathew Ha and David Maxwell of the Foundation for the Defense of Democracies have noted, '[t]hese capabilities complement North Korea's conventional and unconventional military weapons in a highly effective manner. North Korea's cyber operations broaden the Kim family regime's toolkit for threatening the military, economic, and even the political strength of its adversaries and enemies'.[13]

North Korea's cybercrime operations are extensive and well organised, although their exact structure remains unclear. In 2015, South Korean intelligence estimated that North Korea employs up to 6,000 cyber-warfare experts, a number that has likely grown since then.[14] Among these experts are the Lazarus Group, a group of hackers working under the 6th Technical Bureau, within North Korea's Reconnaissance General Bureau.[15] The Lazarus Group is often also referred to as Unit 180 or Bureau 121, although experts debate whether these are all indeed the same group.

According to Kim Heung-kwang, a former professor of computer science in North Korea, candidates for these elite groups are often selected from schools and trained in cyber operations at a university, such as Pyongyang University of Automation. They then operate on behalf of the North Korean government from both domestic and international facilities, sometimes residing and working in China, Malaysia, Russia or South Korea.[16] They may have covers, such as providing internet services, or working at trading firms or overseas branches of North Korean companies.[17]

13. Mathew Ha and David Maxwell, 'Kim Jong Un's "All Purpose Sword": North Korean Cyber-Enabled Economic Warfare', Foundation for Defense of Democracies, October 2018, p. 7, <https://s3.us-east-2.amazonaws.com/defenddemocracy/uploads/documents/REPORT_NorthKorea_CEEW.pdf>, accessed 14 March 2019.
14. Julian Ryall, 'North Korea Doubles its Cyber Warfare Team to 6,000 Troops', *The Telegraph,* 7 January 2015.
15. Authors' telephone interview with a North Korea expert, 2 November 2018; *Group-IB,* 'Lazarus Arisen', 5 May 2017, <https://www.group-ib.com/blog/lazarus>, accessed 14 March 2019.
16. Ju-min Park and James Pearson, 'Exclusive: North Korea's Unit 180, the Cyber Warfare Cell that Worries the West', *Reuters,* 21 May 2017.
17. Sam Kim, 'Inside North Korea's Hacker Army', *Bloomberg,* 7 February 2018.

The Lazarus Group has been linked to the WannaCry ransomware campaign, the Bangladesh Bank heist (see Box 2), and other cybercrime activities. Another group referred to as APT37, thought to be part of Lazarus, has also been identified by US private security company FireEye as a North Korean intelligence unit engaged in cybercrime activities, primarily in Southeast Asia and the Middle East.[18]

North Korea's cybercriminal activity has grown to include widespread attacks on the global financial sector.[19] North Korean organisations have directly hacked major financial institutions (see Box 2). According to the US Department of Homeland Security, North Korea has also developed malware for targeting ATM networks in Africa and Asia as part of its illicit cash-generation efforts.[20]

Expert opinions vary on the objectives of North Korea's attacks against financial infrastructure. Some suggest that North Korea's motivation is purely financial and the attacks serve no broader strategic objective.[21] However, some experts on North Korean affairs consulted during the research for this paper suggested that North Korean cybercrime targeting the financial sector forms part of a broader effort to develop a robust cyber warfare capability that could be operationalised in conflicts with its adversaries.[22]

Seen in this light, attacks on financial sector infrastructure may satisfy some of North Korea's near-term financial goals, while also serving as longer-term test runs for exploiting new attack vectors abroad.

Box 2: The Bangladesh Bank Heist

In February 2016, hackers targeted the Society for Worldwide Financial Telecommunications (SWIFT) network to withdraw $951 million from the account of the Central Bank of Bangladesh (Bangladesh Bank) held at the Federal Reserve Bank of New York (NY Fed). SWIFT is used by over 11,000 banks and companies worldwide and is considered to be the world's most secure payment messaging system.

18. FireEye, 'APT37 (Reaper): The Overlooked North Korean Actor', 20 February 2018, <https://www.fireeye.com/blog/threat-research/2018/02/apt37-overlooked-north-korean-actor.html>, accessed 14 March 2019.
19. Yalman Onaran, 'North Korea Hackers Tried to Take $1.1 Billion in Bank Attacks', *Bloomberg*, 8 October 2018; FireEye, 'APT38: Un-usual Suspects', 2018, <https://content.fireeye.com/apt/rpt-apt38>, accessed 14 March 2019.
20. United States Computer-Alertness Readiness Team (US-CERT), 'HIDDEN COBRA – FASTCash Campaign', US Department of Homeland Security Alert (TA18-275A), 2 October 2018, <https://www.us-cert.gov/ncas/alerts/TA18-275A>, accessed 14 March 2019.
21. Authors' telephone interview with UK-based cybercrime experts, 22 November 2018.
22. Authors' telephone interview with US-based North Korea affairs expert, 1 November 2018; authors' interview with North Korea sanctions evasion expert, London, 2 November 2018.

The hackers had extensive knowledge of the Bangladesh Bank. Experts claim that the sophisticated attack indicated a level of expertise, planning and resources achievable only by a state or group of professionals. The attack involved 35 fraudulent transfer requests, of which five were processed, netting the hackers $101 million, which they then laundered through Sri Lanka and the Philippines. The remaining transactions were blocked by the NY Fed, following suspicions over spelling errors in the transfer requests.

In September 2018, the US Department of Justice charged North Korean hacker Park Jin-hyok for his involvement in the heist. At of the time of writing, $81 million laundered during the bank heist was still unaccounted for.

Sources: Joshua Hammer, 'The Billion-Dollar Bank Job', New York Times*, 3 May 2018; Nicole Perlroth and Michael Corkery, 'North Korea Linked to Digital Attacks on Global Banks',* New York Times*, 27 May 2016; authors' telephone interview with London-based cyber-security expert, 22 November 2018; Jamie Schram, 'Congresswoman Wants Probe of "Brazen" $81M Theft from New York Fed',* New York Post*, 22 March 2016.*

Observation 2: Scope and Scale

North Korea's cryptocurrency activity is increasing in value and complexity and is likely to persist as part of its technology-enabled fundraising and sanctions-evasion activity.

Recently, North Korea has expanded its cybercrime tactics to include exploitation of the global cryptocurrency infrastructure, which sits outside the more established banking sector.

North Korea's use of cryptocurrencies first became apparent in May 2017, when hundreds of thousands of computers worldwide, including critical systems across the UK's National Health Service (NHS), were infected with the WannaCry 2.0 ransomware strain.[23] Researchers from independent cyber security research firms identified the attack as originating from the North Korean-linked Lazarus Group.[24] The US government confirmed North Korea's involvement in the attack in December 2017, and in September 2018 attributed individual responsibility to North Korean cybercrime agent and Lazarus Group member Park Jin-hyok.[25]

23. Chris Graham, 'NHS Cyber Attack: Everything You Need to Know About the "Biggest Ransomware" Offensive in History', *The Telegraph,* 20 May 2017.
24. *Symantec Security Response*, 'WannaCry: Ransomware Attacks Show Strong Links to Lazarus Group', 22 May 2017.
25. US Department of Justice, 'North Korean Regime-Backed Programmer Charted with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions', 6 September 2018, <https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and>, accessed 14 March 2019.

Like other ransomware strains, the computers of WannaCry victims displayed a message instructing them to pay Bitcoin to specified Bitcoin addresses to have their compromised files decrypted (see Figure 1). Analysis of the Bitcoin blockchain indicates that in the months following the attack, several hundred victims paid approximately $300 to $600 each to the perpetrator's Bitcoin addresses.[26] By December 2017, the perpetrators had accumulated Bitcoin worth approximately $144,000.[27] The funds were eventually moved from the attackers' Bitcoin wallets to ShapeShift, a Swiss cryptocurrency exchange service, where they were converted from Bitcoin to Monero, a highly anonymous cryptocurrency that, unlike Bitcoin, is extremely difficult to trace.[28]

Figure 1: WannaCry Ransomware Message

Source: Wikimedia Commons, 2017.

26. *BBC News,* 'WannaCry Ransomware Bitcoins Move from Online Wallets', 3 August 2018.
27. Angela Moscaritolo, 'Hackers Cash Out WannaCry Bitcoin Wallets', *PC News*, 3 August 2017.
28. Patrick Howell O'Neill, 'WannaCry's Bitcoin's Were Converted to Monero, Researchers Say', *Cyberscoop*, 3 August 2017.

Although the WannaCry attack did not provide North Korea with a significant financial windfall compared to other ransomware strains,[29] it signalled North Korea's interest in, and ability to exploit, cryptocurrencies. It also caused disproportionate damage. The NHS estimates the cost of repairing damage to its IT systems affected by the attack at £92 million.[30]

Since the WannaCry attack, other instances of cryptocurrency-enabled activity have been reliably attributed to North Korea, as outlined in Table 1. The table includes events attributed to North Korea by government agencies or reputable private cyber security firms.

Table 1: Cryptocurrency-Enabled Events Reliably Attributed to North Korea

Event	Date	Description	Estimated Value (at the time of the event)	Source of Attribution
Youbit hack #1	22 April 2017	Theft of Bitcoin from a South Korean cryptocurrency exchange.	3,816 bitcoins ($5 million)	Korea Internet Security Agency
WannaCry ransomware attack	12 May 2017	Hackers demanded $300–$600 in bitcoins from each victim. The Bitcoin was laundered by exchanging it for Monero through the Swiss exchange service ShapeShift.	52 bitcoins ($144,000)	US, UK, Canadian, Japanese and New Zealand governments
Bitcoin mining	17 May 2017	North Korea-based Bitcoin mining operations were detected.	Undetermined	Recorded Future
Bithumb hack #1	29 June 2017	Hackers demanded $5.5 million from South Korean exchange Bithumb to return leaked personal information they had stolen.	Bitcoin worth $7 million	South Korea National Intelligence Service (NIS)
Attempted South Korean exchange hacks	May–October 2017	North Korean cybercriminals posing as security specialists sent phishing emails to 25 employees at four South Korean Bitcoin exchanges in 10 separate instances. The emails included document attachments that would infect the victims' computers if opened. However, all attempts were unsuccessful.	None obtained	South Korea's National Police agency; FireEye
Monero cryptojacking	Summer 2017	North Korean-linked cybercriminals seized a South Korean company's server to mine Monero.	70 Monero ($25,000)	South Korean Financial Security Institute

29. For example, the CryptoWall ransomware strain generated as much as $2.2 million for the cybercriminals who deployed it. See *MIT Technology Review*, 'True Scale of Bitcoin Ransomware Extortion Revealed', 19 April 2018.
30. UK Department of Health and Social Care, 'Securing Cyber Resilience in Health and Care: Progress Update October 2018', 2018, p. 14.

Event	Date	Description	Estimated Value (at the time of the event)	Source of Attribution
Coinis hack	23 September 2017	Theft of Bitcoin from a South Korean cryptocurrency exchange.	Undisclosed	NIS
YouBit hack #2	19 December 2017	Theft of Bitcoin from a South Korean Bitcoin exchange.	Undisclosed	Recorded Future
Coincheck hack	January 2018	Theft of cryptocurrency from a Japanese cryptocurrency exchange.	523 million units of NEM cryptocurrency ($534 million)	Group-IB
Bithumb hack #2	19 June 2018	Theft of numerous cryptocurrencies from a South Korean Bitcoin exchange. Stolen Bitcoin were laundered through Russian exchange YoBit. Attributed to the Lazarus Group.	1,993 bitcoins ($13 million) and as much as $30 million in other cryptocurrencies	Alien Vault
Marine Chain	12 April 2018–17 September 2018	According to the UN's Panel of Experts on North Korea, a member state identified Marine Chain as a Hong Kong-registered company that claimed to use the Ethereum blockchain to undertake cryptocurrency transactions to procure vessels. The company, which had a Singaporean national CEO, was reportedly advised by a North Korean national.	Undetermined	UN Security Council Panel of Experts Established Pursuant to Resolution 1874; Recorded Future

Sources: Joyce Lee and Heekyong Yang, 'North Korean Hackers Behind Attacks on Cryptocurrency Exchanges, South Korean Newspaper Reports', Reuters*, 16 December 2017; The White House, 'Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea', 19 December 2017, <https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/>, accessed 14 March 2019;* Reuters*, 'Britain Joins U.S. in Blaming North Korea for "WannaCry" Attack', 19 December 2017;* CBS News*, 'White House Says WannaCry Attack was Carried out by North Korea', 19 December 2017; Insikt Group, 'North Korea's Ruling Elite are not Isolated', Recorded Future Blog, 25 July 2017, <https://www.recordedfuture.com/north-korea-internet-activity/>, accessed 14 March 2019;* BBC News*, 'North Korea "Hacked Crypto-Currency Exchange in South"', 16 December 2017; Nikhilesh De, 'Police Confirm North Korean Connection in Bitcoin Exchange Phishing',* CoinDesk*, 2 October 2017; Luke McNamara, 'Why is North Korea so Interested in Bitcoin?', FireEye, 11 September 2017; Sam Kim, 'North Korean Hackers Hijack Computers to Mine Cryptocurrencies',* Bloomberg*, 2 January 2018; Juan Andres Guerrero-Saade and Priscilla Moriuchi, 'North Korea Targeted South Korean Cryptocurrency Users and Exchange in Late 2017 Campaign', Recorded Future Blog, 16 January 2018, <https://www.recordedfuture.com/north-korea-cryptocurrency-campaign/>, accessed 14 March 2019; Tom Robinson, 'North Korean Hackers and the Russian Cryptocurrency Exchange: Following the Money from the Bithumb Hack', Elliptic, 9 October 2018; Group-IB, '14 Cyber Attacks on Crypto Exchanges Resulted in a Loss of $882 Million', 17 October 2018, <https://www.group-ib.*

com/media/gib-crypto-summary/>, accessed 15 March 2019; UN Security Council, 'Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)', S/2019/171, <https://undocs.org/S/2019/171>, p. 21, accessed 15 March 2019; Insikt Group, 'Shifting Patterns in Internet Use Reveal Adaptable and Innovative North Korean Ruling Elite,' Recorded Future Blog, 25 October 2018, <https://www.recordedfuture.com/north-korea-internet-usage/>, accessed 15 March 2019.

Beyond the cases noted above, there are only anecdotal indications of other cryptocurrency-related incidents in which North Korea might have been involved. Indeed, the difficulty of attribution is a feature of cybercrime activity that likely makes it extremely appealing to North Korea.

Nonetheless, some experts have estimated the likely value of North Korea's cryptocurrency holdings. Priscilla Moriuchi, a former analyst at the US National Security Agency and currently a director at security analysis firm Recorded Future, estimates that North Korea's cryptocurrency holdings could total between $15 million and $210 million, judging by the total amounts of cryptocurrencies amassed through North Korea-attributed events. Depending on when the cryptocurrency was changed into fiat currency, this estimation can vary considerably.[31]

Moriuchi's estimates do not include the largest event described in Table 1, the Coincheck exchange hack in Japan, an event that the security analysis firm Group-IB has separately attributed to the Lazarus Group. In that instance, hackers stole units of NEM cryptocurrency from Coincheck totalling approximately $530 million. According to one report, South Korean intelligence services have suggested North Korea could have been involved in the incident, though they have not publicly made a formal attribution.[32] When combined with Moriuchi's estimates of other instances attributable to North Korea, this would suggest North Korea's cryptocurrency holdings reach a potential range of approximately $545 million to $735 million, depending on the value of cryptocurrencies at the time of the various events.

Important caveats must accompany these estimates. It remains unclear whether North Korea and those working for it have been successful in 'cashing out' the bulk of its cryptocurrencies by exchanging them for dollars, euros or other hard fiat currency that North Korea, its agents and affiliates can then spend (a question examined in further detail below). There is some indication that they are likely having success in doing so – although it cannot be concluded with certainty that the cryptocurrency obtained from each of the incidents in Table 1 has been successfully monetised and has not been lost or otherwise compromised.

Whatever the exact figure, if the instances of North Korean cryptocurrency activity noted in Table 1 are in fact all attributable to North Korea, it is likely that the value of the cryptocurrency it obtained between 2017 and 2018 has reached at least $545 million. Even without the

31. Priscilla Moriuchi, 'North Korea Turning to Cryptos to Counter Economic Sanctions', *The Hill*, 22 January 2018.
32. Cynthia Kim and Kaori Kaneko, 'South Korean Intelligence Says N. Korean Hackers Possibly Behind Coincheck Heist – Sources', *Reuters*, 5 February 2018.

largest single event included in those estimates, as a lower-bound estimate, North Korea's cryptocurrency holdings likely total at least $15 million, if not more. And given North Korea's sophistication as a cyber actor, it is possible that other instances of North Korean cryptocurrency activity have occurred beyond those specific instances identified to date.

Ultimately, the more important lesson is that cryptocurrency-related activity forms a part of North Korea's broader attempts to bolster its technological capabilities for engaging in illicit financial activity and is likely to continue as long as the rewards outweigh the costs.

Observation 3: Methods of Accessing Cryptocurrencies

North Korea exploits cryptocurrencies using several known methods. It could use cryptocurrencies for more wide-ranging and sophisticated purposes over time.

Although the WannaCry attack has garnered the most public attention of North Korea's cryptocurrency-enabled cybercrime efforts, as Table 1 indicates, it is also the only ransomware attack reliably attributed to North Korea. North Korea's preferred method of acquiring cryptocurrencies is not ransomware, but the hacking of cryptocurrency exchanges, particularly those located in South Korea.

Nearly every case of cryptocurrency-related activity attributed to North Korea involves the theft of cryptocurrency from South Korean exchanges, many of which are highly vulnerable to cyber attack. In addition to being located within the borders of North Korea's biggest political threat, South Korean exchanges are a plentiful source of cryptocurrencies, by some estimates accounting for as much as 16% of all global cryptocurrency trading, with only the US dollar and Japanese yen trading at higher volumes.[33]

For a capable cyber actor, cryptocurrency exchanges are an attractive target. By one estimate, criminals stole as much as $1.1 billion in cryptocurrencies from exchanges worldwide in the first half of 2018, in part because of poor security practices.[34] Many cryptocurrency exchanges have been called out by security experts and regulators for their insufficient cyber security standards (such as a failure to require strong passwords or employ two-factor authentication when customers log on), as well as poor practice in safeguarding customer funds.[35] Some observers also note that security and storage practices among many individual cryptocurrency users are generally poor.[36]

33. CryptoCompare, 'CCCAGG Exchange Review', 31 October 2018, p. 6, <https://blog.bitmex.com/wp-content/uploads/2018/11/cryptocompare_exchange_review_october_2018.pdf>, accessed 14 March 2019.
34. Carbon Black, 'Cryptocurrency Gold Rush on the Dark Web', June 2018, <https://www.carbonblack.com/resource/cryptocurrency-gold-rush-dark-web>, accessed 14 March 2019.
35. Kai Sedgwick, '54% of Cryptocurrency Exchanges Have Security Holes', Bitcoin.com, 2 October 2018.
36. Carbon Black, 'Cryptocurrency Gold Rush on the Dark Web'.

North Korea has been quick to exploit these vulnerabilities. Hacks of exchanges are a low-cost enterprise,[37] but can bring high rewards if carried off successfully. As Table 1 shows, North Korea has been linked to six successful exchange hacks that occurred between April 2017 and June 2018 and has attempted to launch as many as 10 other hacking campaigns during that same period, which ultimately proved unsuccessful.

But attacks against cryptocurrency exchanges are not the only method of acquisition. Mining operations are another. Mining is the process of supplying computing resources to validate cryptocurrency transactions and ensuring consensus regarding the record of activity that appears on cryptocurrency blockchains. Miners receive a reward in the form of newly generated coins for the services they provide to cryptocurrency networks. Mining has consequently become a large and lucrative line of business internationally.

Recorded Future has identified that North Korea has mined Bitcoin, if briefly.[38] North Korea's established mining operations could offer an advantage over cybercrime insofar as mining newly minted cryptocurrencies with no indication that they have been tainted or associated with criminal activity attracts less attention.

Cryptojacking refers to the deployment of malware that infects a user's computer or mobile device and draws on its resources to mine cryptocurrencies surreptitiously – allowing the criminal to reap the newly generated coins without paying the cost of supplying the computing power required to mine. Cybercriminals have taken to cryptojacking campaigns, as, unlike ransomware and hacking, victims may not even be aware that they have been attacked, while the criminal is able to generate new units of cryptocurrencies out of thin air. By one estimate, cryptojacking campaigns increased more than 400-fold across 2018.[39]

As noted in Table 1, North Korea has been linked to the unauthorised use of a South Korean company's computer servers to undertake Monero mining. While this is the only public attribution of North Korea's use of cryptojacking, researchers from Recorded Future have suggested that North Korea has the capabilities and tools required for 'effectively creating and managing a network of covert cryptocurrency miners' who could generate a substantial volume of funds.[40]

Illicit online marketplaces that accept cryptocurrencies are an example of other methods of acquiring cryptocurrencies that could prove vulnerable to North Korean exploitation. Certain

37. Malware needed for hacking exchanges can be obtained on illicit marketplaces for an average of $224, and sometimes far less. See Carbon Black, 'Cryptocurrency Gold Rush on the Dark Web'.
38. Insikt Group, 'North Korea's Ruling Elite are not Isolated'.
39. Cyber Threat Alliance, 'CTA Cryptomining Paper: Key Findings', <https://www.cyberthreatalliance.org/wp-content/uploads/2018/09/CTA-Illicit-CryptoMining-Key-Findings.pdf>, accessed 14 March 2019.
40. Andrei Barysevich, Priscilla Moriuchi and Daniel Hatheway, 'Proliferation of Mining Malware Signals a Shift in Cybercriminal Operations', p. 11, <https://go.recordedfuture.com/hubfs/reports/cta-2017-1011.pdf>, accessed 14 March 2019.

illicit items in which North Korea has been known to deal, such as drugs,[41] are available on dark web marketplaces that rely on Bitcoin and Monero as their primary forms of payment.

Dark web markets also facilitate the provision of crime-as-a-service (CaaS), which involves criminals offering their know-how and technical support to other criminals. Cybercriminals rely on CaaS to provide malware and hacking services to other criminals. It is possible that North Korea's cybercrime agents could provide such services in return for cryptocurrencies.[42] North Korea could also potentially pay for online criminal services using cryptocurrencies. While there is no specific evidence indicating that North Korea deals in dark web marketplaces, illicit online markets could enable North Korean agents or affiliates to acquire and utilise cryptocurrencies.

As North Korea has succeeded in acquiring and exploiting cryptocurrencies, an important further question for discussion is how it may be using the cryptocurrency it has acquired or could acquire in the future.

In general, ways that North Korea could seek to deploy cryptocurrencies as part of its sanctions evasion efforts include:

- **Fundraising**: To sustain its ongoing needs for cash, North Korea may obtain cryptocurrencies with the aim of converting them to fiat currencies in the short term and using fiat currencies to finance both permitted and prohibited activity.
- **Stockpiling**: North Korea could accumulate reserves of cryptocurrencies with the objective of eventually spending them or converting them into fiat currency at some undetermined future date.
- **Circumvention**: North Korea could pay directly in cryptocurrencies for goods, services and resources that are explicitly prohibited by international sanctions.

Observation 4: Fundraising

The ability to convert cryptocurrencies into fiat currency makes them attractive for North Korea's near-term fundraising efforts.

North Korea likely sees cryptocurrencies primarily as an immediate source of revenue, much as it has exploited other economic activities to replenish its depleted currency reserves.[43] Counterfeiting US dollars, smuggling bulk cash and gold, and selling illicit contraband such as cigarettes, narcotics, weapons and ivory are among the criminal techniques North Korea has employed in the past to obtain much-needed financing and hard cash.[44]

41. Isaac Stone Fish, 'Inside North Korea's Crystal Meth Trade', *Foreign Policy*, 21 November 2013.
42. Authors' telephone interview with US-based North Korean security expert, 1 November 2018.
43. Jiyeun Lee, 'Kim Jong Un Comes Around to Talks as His Currency Reserves Shrink', *Bloomberg,* 7 March 2018, last updated on 8 March 2018.
44. Reported by Joonho Kim and Sunghui Moon, translated by Leejin Jun, written in English by Richard Finney, 'North Korean Tobacco Factories, Smuggled Cigarettes Bring in Cash for Pyongyang',

Obtaining cryptocurrencies through any of the methods described earlier – whether through cybercrime, mining operations or other techniques – provides North Korea with an advantage, insofar as its agents do not necessarily need to set up a bank account or other regulated service to initially obtain value. A North Korean actor can generate cryptocurrency addresses[45] and begin receiving cryptocurrency from a variety of sources in a manner that is irreversible[46] and avoids reliance on third-party intermediaries.[47]

However, to realise the value of cryptocurrencies, criminal actors generally must 'cash out'. That is, they must convert cryptocurrencies into fiat currencies, such as US dollars, euros, yen or yuan.

The reason is simple: cryptocurrencies are not widely accepted as payment for day-to-day goods and services. Most cryptocurrency use is speculative, with users trading them as their values rise and fall against fiat currencies.

The cryptocurrency conversion process involves a cryptocurrency exchange service that transfers converted funds onward to a bank account, from which the funds can be spent or transferred further onward. Popular exchange services such as Binance, Coinbase, Huobi and others conduct hundreds of millions of dollars' worth of cryptocurrency trades daily. For a cash-strapped actor, cryptocurrencies' primary value in the near term is that they can be converted into fiat currencies relatively rapidly.

For example, as noted in Table 1, in late June 2018 the South Korean-based exchange Bithumb was hacked, losing Bitcoin worth nearly $13 million, an incident that security analysis firm AlienVault has indicated is likely attributable to the Lazarus Group.[48] By August 2018, less than two months after the attack, the funds were sent using a complex series of hundreds of transactions to YoBit, an exchange service based in Russia. The aim of the hackers seems to have been to convert and cash out the entirety of the large amount of cryptocurrency they had stolen, rather than spending the acquired cryptocurrency directly on goods and services.

Radio Free Asia, 16 November 2017; *Maritime Executive*, 'North Korean Diplomats Smuggle Ivory, Cigarettes and Gold', 25 September 2017; Larry Wortzel, 'North Korea's Connection to International Trade in Drugs, Counterfeiting, and Arms', 20 May 2003, Heritage Foundation, <https://www.heritage.org/testimony/north-koreas-connection-international-trade-drugs-counterfeiting-and-arms>, accessed 14 March 2019.

45. A cryptocurrency address is an alphanumeric identifier that pseudonymously represents a user's identity and is associated with the user's Bitcoin balance of funds.
46. Because cryptocurrencies operate as decentralised open-source software and are not controlled by a central party, no single entity can cause a transaction to be reversed in the way a bank or other financial institution could reverse a fiat currency transaction. For this reason, cryptocurrency transactions are often described as 'censorship resistant'.
47. Because they are P2P technologies, cryptocurrencies enable individuals to transfer value to each other without the presence of a bank or other financial institution intermediary.
48. Chris Doman, Fernando Martinex and Jaime Blasco, 'Malicious Documents from Lazarus Group Targeting South Korea', AT&T Cybersecurity, 22 June 2018.

As discussed in Chapters II and III, ensuring appropriate oversight over cryptocurrency exchanges is therefore essential for mitigating exposure to North Korean cryptocurrency activity.

Observation 5: Stockpiling

North Korea may opt to stockpile some of its cryptocurrencies for future use, both to safeguard funds and to avoid certain challenges of cashing out.

Another possibility is that, rather than cashing out immediately, North Korean actors may choose to stockpile cryptocurrency holdings, content to cash out or spend them later. Stockpiling cryptocurrencies by keeping them in wallets for an extended period could have two advantages over rapid conversion.

First, it could allow North Korea to maintain a stash of value beyond the reach of its adversaries, unlike funds sitting in a bank account that could be more easily subject to blocking, freezing or asset confiscation. Mining certain cryptocurrencies, such as Monero, can prove to be a low-cost and potentially high-reward activity should the value of the mined coins rise over time. North Korea therefore might wish to hold onto a stockpile of mined cryptocurrencies, one that it can attempt to use as future needs dictate. As described in Chapter III, one way for countries to mitigate this risk is to conduct risk assessments that include a survey of mining activity conducted domestically with the aim of determining whether North Korean-affiliated actors may be involved in mining.

A second benefit of hoarding is that it would allow North Korea to avoid challenges that could arise from cashing out very large volumes of cryptocurrencies. While, as described earlier, there are numerous methods for cashing out cryptocurrencies, the high-profile instances of North Korea's cybercrime activity suggest a potential vulnerability: because certain cryptocurrencies, especially Bitcoin, are highly traceable on public blockchains, a criminal actor's transactions are visible for the world to see. Particularly when large volumes of cryptocurrencies are involved – such as in the June 2018 hack of the Bithumb exchange – criminals can prove susceptible to detection and monitoring.

As such, maintaining stockpiles of cryptocurrencies that appear clean in origin could allow North Korea to cash out more slowly, with the aim of being less susceptible to detection.

However, stockpiling faces at least one important limitation: the value of cryptocurrencies is highly volatile, so holding them for an extended period could result in substantial losses. Therefore, insofar as North Korea could engage in the stockpiling of cryptocurrencies, this would likely complement efforts to cash out for fundraising purposes in the near term.

Observation 6: Circumvention

The potential for North Korea to engage in large-scale sanctions circumvention by accessing prohibited goods and services directly with cryptocurrencies is a risk that could grow in significance.

Cryptocurrency adoption for everyday spending and payments remains relatively limited, and there are several obstacles to its practical use. High price volatility and delays in processing payments generally make cryptocurrencies difficult to use for purchasing goods and services in many contexts,[49] leading to use of the term 'crypto-asset' or 'virtual asset' by some observers, who suggest that a primarily speculative instrument with little other practical application does not meet the definition of a 'currency'.

As such, just like the average cryptocurrency user, North Korea and its agents might struggle to spend cryptocurrencies practically. This may limit cryptocurrencies' near-term viability for enabling North Korea to circumvent trading restrictions on items such as coal, electricity and minerals that require large-scale financial transfers. North Korea's tactics for evading sanctions on such heavy-duty commodities and goods often involve complex trade-based money-laundering schemes that might prove difficult to undertake with an unreliable and volatile payment method like cryptocurrencies.[50]

Nonetheless, it is possible to obtain goods and services using cryptocurrencies, if in a limited number of contexts, and North Korea could use them to make otherwise prohibited payments outside the regulated sector. There is some suggestion they may have attempted to do so in at least one instance. According to the UNSC's Panel of Experts on North Korea, a UN member state reported in October 2018 that it had identified a Hong Kong-registered company named Marine Chain that claimed to have issued its own cryptocurrency to allow it to engage in transactions for procuring vessels. The member state indicated that one of Marine Chain's advisers was a North Korean national, and expressed concern that the entity could be used to evade restrictions on North Korea's access to vessels.[51] According to the Panel of Experts, the company, whose chief executive officer was a Singaporean national, abruptly went out of business in September 2018, only five months after it was established.[52] It is unclear whether Marine Chain ever actually utilised cryptocurrencies or succeeded in procuring vessels with them, but according to security analysis firm Recorded Future, the Singaporean individual behind the company 'has been connected to Singaporean companies that have assisted North Korean sanctions circumvention efforts since at least 2013'.[53]

---

49. Jeff Desjardins, 'The Future of Crypto Payments in the Retail Market', *Visual Capitalist*, 18 April 2018.
50. FinCEN, 'Advisory on North Korea's Use of the International Financial System', 2 November 2017, <https://www.fincen.gov/sites/default/files/advisory/2017-11-02/DPRK%20Advisory%20FINAL%20508%20C.pdf>, accessed 14 March 2019.
51. *Ibid.*
52. *Ibid.*
53. Insikt Group, 'Shifting Patterns in Internet Use', p. 14.

Other opportunities exist for North Korea to use cryptocurrencies for directly purchasing goods and services. For example, luxury goods are increasingly accessible using cryptocurrencies. Some high-value goods dealers such as sports-car dealerships, jewellers, auctioneers and estate agents now accept payments in cryptocurrencies.[54] While research for this report did not identify evidence of North Korea using cryptocurrencies to pay for prohibited luxury goods, it is worth considering how it might do so.

As noted in Box 1, UN sanctions prohibit the export of luxury goods to North Korea, with the aim of preventing the regime from obtaining exclusive items that it covets, such as cars, jewellery and artwork.

Luxury goods can be purchased using services such as prepaid cards that link to cryptocurrency wallets. These allow customers to fund their card with Bitcoin or other cryptocurrencies but then enable the merchant to receive the payment in fiat currencies. Much as it currently uses smuggling networks to conceal the importation of luxury goods, North Korea could employ agents acting on its behalf to purchase high-value items from abroad using cryptocurrencies for eventual importation into North Korea.

North Korea could also use cryptocurrencies to pay for trading services, such as making payments to shipping companies, brokers or other intermediaries who might be willing to accept payment in cryptocurrencies. Other sanctioned jurisdictions have explored the potential utility of cryptocurrencies to fulfil similar requirements, though with varying degrees of success (see Box 3).

And while their utility for everyday use is presently limited, cryptocurrencies' use in standard payments could expand relative to current levels. Market research firm NetCents indicates that the number of retailers accepting Bitcoin globally grew by 30% across 2017.[55]

If cryptocurrencies become more practical for everyday spending and transfers, North Korea would likely seek to use them for those purposes.

Box 3: Sanctioned Countries and the Use of Cryptocurrencies

North Korea has shown interest in using cryptocurrencies to evade sanctions, but so have other sanctioned countries. Iran, Russia and Venezuela, sometimes even collaboratively, have stated their intention to utilise cryptocurrencies.

54. Victoria Burrows, 'Bitcoin Billionaires Translate Digital Wealth into Real-World Assets', *South China Morning Post Style Magazine*, 14 July 2018.
55. Desjardins, 'The Future of Crypto Payments in the Retail Market'.

In general, these efforts have had limited success, and it is unclear whether cryptocurrencies will provide a sustainable sanctions circumvention solution for these countries; but their efforts point to the desire of sanctioned jurisdictions to find innovative methods of evasion.

Iran: In October 2018, the US Treasury's Financial Crimes Enforcement Network (FinCEN) published an advisory detailing the Iranian regime's attempts to exploit the financial system, including through the use of cryptocurrencies. In the advisory, FinCEN stated that Iran's 'use of virtual currency includes at least $3.8 million worth of bitcoin-denominated transactions per year', an amount that is relatively small but implies cryptocurrency is an emerging system for sanctions evasion, especially following the decision by SWIFT, the financial messaging system crucial for facilitating international bank transfers, to remove Iranian banks in November 2018. Iran has reportedly begun piloting a national cryptocurrency backed by the Iranian rial, and the government has recognised cryptocurrency mining as an industry for generating revenue. Iran's information and communications technology minister stated in May 2018 that 'all cryptocurrencies are capable of circumventing sanctions because they are not under supervision of the US financial regulatory body, and the national digital currencies are naturally capable of this'. In addition, reports suggest that Iranians citizens are using Bitcoin to get around sanctions while studying in the UK.

Venezuela: Venezuela is now known for its Petro coin, a national cryptocurrency launched by the government and reportedly backed by Venezuela's oil, gas, gold and diamond reserves. While the Petro's stability (and even existence) are questionable, President Nicolás Maduro recently said that '[i]n 2019, [Venezuela has] a schedule for [oil] to be sold in Petros and in this way continue to free us from a currency that the elite of Washington uses'. Likewise, the bolivar soberano, Venezuela's currency as of August 2018, has reportedly been pegged to the Petro. Due to extreme hyperinflation and economic instability in the country, many Venezuelans view cryptocurrency to be safer than the bolivar.

Russia: Similarly, Russia has also expressed interest in a national cryptocurrency, referred to as the CryptoRuble. Although discussions began in 2015, the CryptoRuble has yet to appear, but in theory would be pegged to the Russian ruble and would not be mined. Sergei Glazev, one of President Vladimir Putin's economic advisers, claimed in January 2018 that cryptocurrency 'suits [Russia] very well for sensitive activity on behalf of the state. [Russia] can settle accounts with [its] counterparties all over the world with no regard for sanctions'. In addition, reports have asserted that Russia is helping Iran and Venezuela in their cryptocurrency development projects. Russia is currently developing cryptocurrency regulations within the country, as the daily volumes of cryptocurrency trading in Moscow range between $10 million–$50 million.

Source: For Iran: FinCEN, 'Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System', 11 October 2018, <https://www.fincen.gov/sites/default/files/advisory/2018-10-11/Iran%20Advisory%20FINAL%20508.pdf>, accessed 14 March 2019; Michael Peel, 'Swift to Comply with US Sanctions on Iran in Blow to EU', Financial Times*, 5 November 2018;* Reuters*, 'Iran Cryptocurrency Project on Track Despite Cenbank Ban, Minister Says', 28 April 2018;* Ibena.ir*, 'Iranian National Cryptocurrency to be Granted to Commercial Banks', 9 November 2018; Jeffrey Gogo, 'Iran Officially Recognizes Cryptocurrency Mining',* Bitcoin News*, 4 September 2018;*

TrustNodes*, 'Iranian Crypto Token Will Be Backed by Assets Says Minister, "All Cryptocurrencies are Capable of Circumventing Sanctions"', 1 May 2018; Mark Townsend, 'UK University Tells Iranian Student: Go Home and Get Tuition Fees in Cash',* The Guardian*, 15 December 2018. For Venezuela: Alexandra Ulmer and Deisy Buitrago, 'Enter the "Petro": Venezuela to Launch Oil-Backed Cryptocurrency',* Reuters*, 3 December 2017; Brian Ellsworth, 'Special Report: In Venezuela, New Cryptocurrency is Nowhere to be Found',* Reuters*, 30 August 2018; Yogita Khatri, 'Venezuela to Sell Oil for Petro Cryptocurrency in 2019, Says Maduro',* CoinDesk*, 7 December 2018; Daniel Palmer, 'Venezuela's New National Currency Will be Tied to the Petro, Says President',* CoinDesk*, 26 July 2018; Simon Chandler, 'How Venezuela Came to be One of the Biggest Markets for Crypto in the World',* Cointelegraph*, 2 September 2018. For Russia: Stephen O'Neal, 'CryptoRuble: How Stable Could Russian National Stablecoin Be?',* Cointelegraph*, 17 November 2018; Max Seddon and Martin Arnold, 'Putin Considers "Cryptorouble" as Moscow Seeks to Evade Sanctions',* Financial Times*, 2 January 2018; Molly Jane Zuckerman, 'Iran and Russia Discuss Transacting in Crypto to Avoid International Sanctions',* Cointelegraph*, 19 May 2018; Molly Jane Zuckerman, 'Russia's "Disappointing" Cryptocurrency Legislation: Why Experts Consider the Bill a Failure',* Cointelegraph*, 29 September 2018; Lubomir Tassev, 'Cash to Crypto Trade Blooming in Moscow, Reports Say',* Bitcoin News*, 12 September 2018.*

II. Assessing Risks and Vulnerabilities in Southeast Asia

THIS CHAPTER CONSIDERS specific cryptocurrency-related risks and vulnerabilities in Southeast Asia. It describes the current scale of cryptocurrency use country by country in the region, as well as the status of related regulatory and law enforcement measures, assessing the implications of these developments.

Observation 1: Cryptocurrency Adoption and Infrastructure

Countries across Southeast Asia feature growing cryptocurrency activity that could prove vulnerable to North Korean exploitation.

The picture of cryptocurrency use and the size of the cryptocurrency industry across Southeast Asia varies greatly. But in general, Southeast Asian countries feature growing cryptocurrency industries and increasing cryptocurrency use.

Below is an overview of cryptocurrency use and the scale of cryptocurrency infrastructure across select Southeast Asian countries.[56]

Cambodia

Reliable statistics are lacking, but cryptocurrency use in Cambodia is generally believed to be minimal. The first cryptocurrency exchange applied to operate in Cambodia in August 2018,[57] but other exchange businesses have not been permitted to operate in Cambodia to date.

Indonesia

Some observers suggest Indonesia may be ripe for cryptocurrencies adoption given its large population, increasing levels of smartphone penetration, and significant number of citizens who

56. These countries have been selected on the basis of RUSI's previous proliferation finance work in Southeast Asia. While Myanmar, Brunei and East Timor may be considered part of the Southeast Asian region, they have not been included in this study. Myanmar, Brunei and East Timor have not been part of RUSI's previous counter-proliferation financing work. This does not mean there is no risk there.
57. *Cointelegraph,* 'Cambodian Crypto Exchange Applies for a License to Become the First Legally Certified'*,* 23 August 2018.

do not have access to bank accounts, who could find cryptocurrencies an attractive alternative financing method.[58] Indonesian Bitcoin exchange Indodax features among the top 100 exchanges globally in terms of trading volumes, processing trades in excess of $8 million daily.[59]

Laos

Like Cambodia, Laos has only a small amount of known cryptocurrency activity. Vientiane Exchange Money is the first certified crypto exchange in Laos, with seven currencies available.[60]

Malaysia

Malaysia features the largest volumes of trading among Southeast Asian countries on LocalBitcoins. Daily trade volumes across 2018 were as high as $650,000 (or an annualised rate of over $200 million).[61] There are presently more than 50 cryptocurrency exchanges in Malaysia.[62]

Philippines

There are currently six exchanges registered in the Philippines, mainly aimed at providing remittances and facilitating global payments. Cryptocurrencies play a small but growing role in the remittance market in the Philippines.[63] In August 2018, the government announced the creation of a cryptocurrency and blockchain hub in the Cagayan Special Economic Zone and Freeport to attract technology companies.[64]

Singapore

Singapore has attempted to position itself as a leader in cryptocurrency and blockchain innovation.[65] Binance, the world's largest cryptocurrency exchange, has announced its beta

58. Sharon Lam, 'Indonesia is Ripe for Cryptocurrency Disruption – Could It Be Asia's Next Bitcoin Hub?', *Forbes*, 1 November 2017.
59. See CoinMarketCap, '24 Hour Volume Rankings (Exchange)', entry for Indodax, <https://coinmarketcap.com/exchanges/volume/24-hour/>, accessed 14 March 2019.
60. Zachary, 'First Certified Bitcoin Exchange Launches in Laos', *BitcoinNews.com*, 11 June 2018.
61. See Coin Dance figures for LocalBitcoins trading in Malaysia, <https://coin.dance/volume/localbitcoins/MYR/BTC>, accessed 14 March 2019.
62. Vincent Fong, 'Meet the 56 Cryptocurrency Exchanges in Malaysia Registered with BNM', *FinTech Malaysia*, 28 February 2019.
63. Joseph Young, 'Bitcoin Powers 20 Percent of Remittances from Korea to Philippines', *Cointelegraph*, 28 October 2016.
64. Mikhail Flores, 'Asian Countries Vie to Set Up Region's "Crypto Valleys"', *Nikkei Asian Review*, 20 August 2018.
65. Prerna Suri, 'Behind Singapore's Meteoric Rise as a Top Blockchain Hub', *Tech in Asia*, 19 April 2018.

launch of a Singapore fiat/cryptocurrency exchange.[66] Other large exchanges have begun to establish branches in Singapore as well.[67]

Thailand

Three cryptocurrency exchanges were granted working licenses to operate in Thailand in January 2019.[68] The largest Thai exchange, BX Thailand, ranks among the 100 largest cryptocurrency exchanges globally, with a daily trading volume of approximately $3 million.[69] Daily trading volumes on LocalBitcoins in Thailand were as high as $300,000 during 2018, amounting to over $100 million annually.[70]

Vietnam

A September 2017 estimate states that there are around 1 million cryptocurrency users in Vietnam.[71] The most popular local exchange by volume is Bitcoin Vietnam, but Vietnamese users are also among the top users of exchanges located outside Vietnam.[72]

These figures suggest the region faces vulnerabilities to the types of risk described in detail in Chapter I. First, exchanges in the region could prove vulnerable to hacking and theft of the type North Korea has engaged in. Thailand, Indonesia and Malaysia, for example, have cryptocurrency exchanges that rank among the top 200 exchanges globally in terms of trading volumes, facilitating trade worth more than $1 million per day.[73] The Thai baht, Indonesian rupiah and Vietnamese dong are among the top 20 currencies exchanged for Bitcoin globally on exchanges as well.[74] These trading volumes suggest that exchanges locally could be an attractive target for cybercrime attacks by an actor such as North Korea seeking access to cash reserves.

66. David Hundeyin, 'Binance to [Beta] Launch Singapore Fiat Crypto Exchange Tomorrow', *CCN,* 17 September 2018.
67. Joseph Young, 'Singapore's Crypto Market Blooms as Korea's Largest Exchange Moves In', *CCN*, 19 September 2018.
68. Layla Harding, 'Adoption: Three Cryptocurrency Exchanges Granted License in Thailand', *Coinnounce*, 9 January 2019.
69. See CoinMarketCap.com, '24 Hour Volume Rankings (Exchanges)', entry for BXThailand, <https://coinmarketcap.com/exchanges/volume/24-hour/>, accessed 14 March 2019.
70. See Coin Dance figures for LocalBitcoins trading in Thailand, <https://coin.dance/volume/localbitcoins/THB/BTC>, accessed 14 March 2019.
71. *Vietnam Net Bridge,* 'Jury Still Out on Cryptocurrency in Vietnam', 19 September 2017.
72. Mai Thanh, 'Vietnamese Interest in Bitcoin in Top 5 Among Global Trading Floors', *Vietnam Net Bridge*, 30 December 2017.
73. See, for example, CoinMarketCap, '24 Hour Volume Rankings', entries for Indodax, Luno, BXThailand, and Bitkub, <https://coinmarketcap.com/exchanges/volume/24-hour/>, accessed 14 March 2019.
74. *Coinhills*, 'Most Traded National Currencies for Bitcoin', <https://www.coinhills.com/market/currency/>, accessed 16 December 2018.

Second, North Korea could attempt to cash out its cryptocurrencies at exchanges in the region, relying on local networks of users to exploit exchanges. Vietnam, for example, has a cryptocurrency user base of over 1 million individual users.[75] Vietnam also ranks among the top five countries globally in terms of the number of online logins to major cryptocurrency exchanges.[76] Across portions of Southeast Asia where mainstream banking services are limited, cryptocurrency adoption may appeal as an alternative payments system. One cryptocurrency exchange in the Philippines claims to have 5 million individual users,[77] and although precise figures are difficult to come by, anecdotal claims suggest cryptocurrencies may have a growing role in the Philippines' enormous remittances market, as well as elsewhere in the region.[78]

North Korea could cash out its cryptocurrency profits by relying on its extensive overseas financial networks to open and operate accounts at cryptocurrency exchanges in the region. Such activity would be consistent with North Korea's other deceptive practices. North Korea sanctions and non-proliferation expert Andrea Berger has noted that when evading sanctions through the formal banking sector:

> In jurisdictions where it is possible to use a local Chinese identification document to establish companies or bank accounts, North Koreans with such an ID form tend to use it instead of their North Korean passport … A similar desire to avoid revealing the North Korean nationality of the individuals behind a company also leads them to partner with local national facilitators when setting up companies and bank accounts. … In certain circumstances, trusted foreign nationals operate independently of any locally based North Korean coordinator.[79]

Using individuals with citizenship and residency documents from other counties to open accounts at even legitimate cryptocurrency exchanges would enable North Korea to establish a network of cryptocurrency traders abroad with no obvious links back to it.

What's more, North Korea could rely on existing local evasion networks to engage in cryptocurrency-enabled circumvention activity, as it appears to have done in the case of the aforementioned Marine Chain company that relied on a Singaporean national who has been associated with other North Korean front companies.

Over-the-counter (OTC) and P2P markets in Southeast Asia are also generally large and potentially exploitable. Examples of these P2P platforms include LocalBitcoins, Paxful and XCoin. On these

75. Siviraj Pragasm, 'The Rise of Cryptocurrency in Vietnam', *City Pass Guide*, 10 December 2018, <https://www.citypassguide.com/en/travel/vietnam/blog/blog/the-rise-of-cryptocurrency-in-vietnam>, accessed 14 March 2019.
76. Thanh, 'Vietnamese Interest in Bitcoin in Top 5 Among Global Trading Floors'.
77. C Edward Kelso, 'Philippines' Crypto Wallet Reaches 5 Million Users, Adds More Coins', *Bitcoin.com*, 31 May 2018.
78. Tanya Mariano, 'How Bitcoin is Disrupting Southeast Asia's Remittance Industry', *INC. Southeast Asia*, 22 August 2016.
79. Berger, 'A House Without Foundations', pp. 14–15.

sites, sellers of cryptocurrencies post advertisements that buyers can respond to directly, just as common goods are bought and sold on popular sites such as Craigslist. Where they agree to transact, the seller sends the Bitcoin directly to the buyer, who pays the seller using a pre-agreed method, such as by cash, PayPal or wire transfer.

In Malaysia, daily trades on the P2P cryptocurrency website LocalBitcoins totalled as much as $650,000 (see Figure 2) – suggesting sufficient liquidity is available there for an illicit actor to transfer a meaningful volume of criminal proceeds. Thailand features smaller levels of trading on LocalBitcoins than Malaysia, although daily volumes still exceeded $300,000 at times across 2018.[80] Indonesia, the Philippines, Singapore and Vietnam are also among the top 50 countries globally for LocalBitcoins trading volumes.[81]

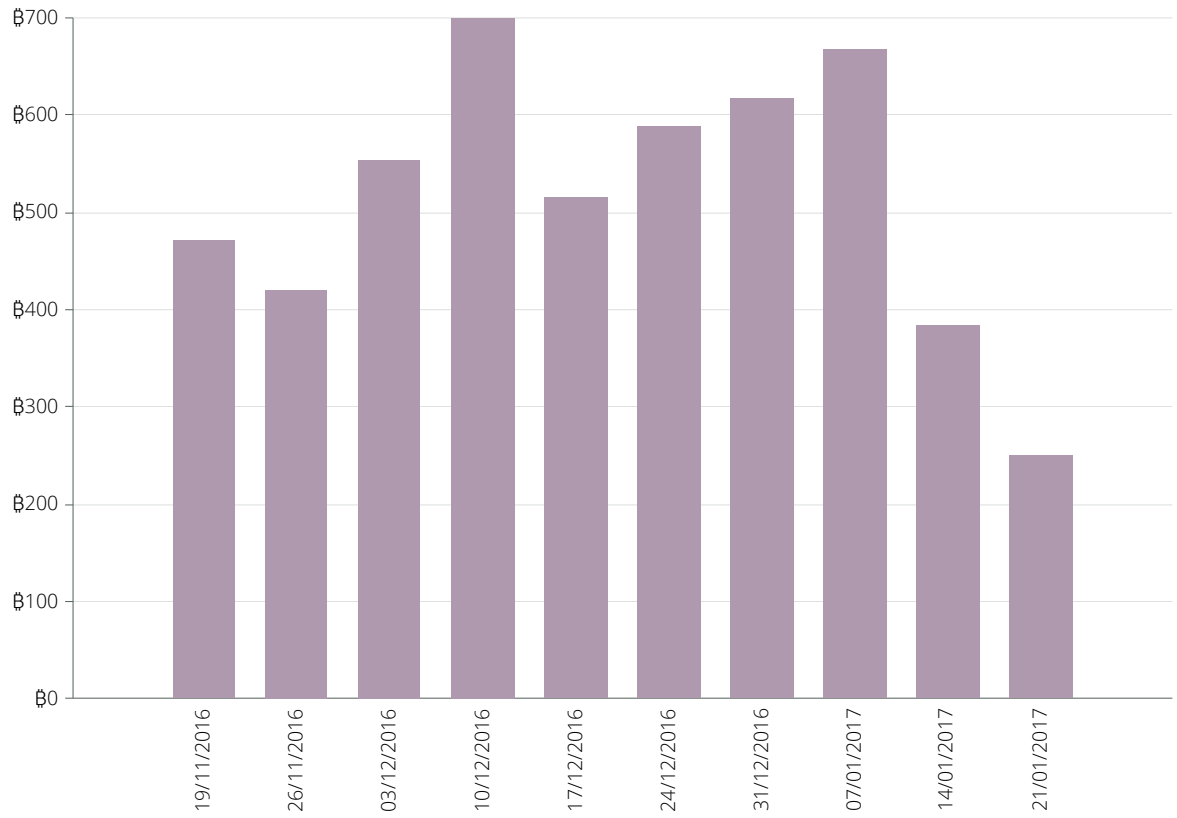
P2P platforms may present two distinct advantages for an illicit actor over using centralised exchange services. First, while LocalBitcoins has recently indicated that it now collects Know Your Customer (KYC) and other AML information about users of its platform,[82] many other P2P platforms still do not require traders to provide KYC or other information, allowing users an enhanced degree of anonymity. Second, some of these underground trading markets tend to thrive in the face of government efforts to crack down on large, centralised exchanges.

For example, across 2017 and 2018, the Chinese government undertook an aggressive campaign to ban cryptocurrency exchanges, requiring them to suspend customer trading, and prohibiting Chinese individuals from accessing exchanges abroad.[83] While many large Chinese exchanges were shut down, OTC markets and platforms such as LocalBitcoins continue to thrive in China to meet local demand for cryptocurrencies.[84]

While still not as large in volume or usage as in countries such as China, South Korea and Japan, cryptocurrency markets in Southeast Asia are sufficiently large that North Korea could exploit them on a meaningful scale.

80. See Coin Dance figures for LocalBitcoins trading in Thailand, <https://coin.dance/volume/localbitcoins/THB/BTC>, accessed 14 March 2019.
81. *FinTech Futures*, 'Infographic: Which Country Trades the Most Bitcoin?', 20 August 2018, <https://www.bankingtech.com/2018/08/infographic-which-country-trades-the-most-bitcoin/>, accessed 14 March 2019.
82. Local Bitcoins Blog, 'AML Regulation and New Features Update', 25 March 2019, <https://localbitcoins.com/blog/aml-features-update/>, accessed 26 March 2019.
83. Rosie Perper, 'China is Moving to Eliminate all Cryptocurrency Trading with a Ban on Foreign Exchanges', *Business Insider*, 5 February 2018.
84. Jamie Redman, 'Chinese Investors Continue to Obtain Bitcoin Using Thriving OTC Platforms', *Bitcoin.com*, 30 January 2018.

Figure 2: Weekly LocalBitcoins Volumes in Malaysia (Denominated in Number of Bitcoins Traded Per Day)



Source: Coin Dance, 'LocalBitcoins Volume (Malaysia)', <https://coin.dance/volume/localbitcoins/MYR/BTC>, accessed 24 December 2019.

Observation 2: Regulatory Approaches

Countries across Southeast Asia vary widely in the nature and scope of regulatory approaches to cryptocurrencies they have in place, creating systemic risks North Korea could exploit.

As the following breakdown indicates, countries in Southeast Asia have widely differing approaches to regulating cryptocurrencies.

Cambodia

The National Bank of Cambodia, Securities and Exchange Commission of Cambodia, and General-Commissariat put out a joint statement in May 2018, stating that 'the propagation,

circulation, buying, selling, trading and settlement of Crypto Currencies without obtaining license from competent authorities are illegal activities'.[85]

Indonesia

The Indonesian Central Bank banned the use of cryptocurrencies in October 2017, citing that they do not represent a recognised legal tender in the country.[86] However, Indonesia has said they are planning to release crypto legislation and guidance to combat AML and CTF threats.

Laos

The Bank of Laos issued a notice in August 2018 warning the public against the use of cryptocurrencies. The notice referred to cryptocurrencies as 'unregulated', citing Bitcoin, Ethereum and Litecoin as examples.[87] Laos's current Law on Payment Systems claims that cryptocurrencies do not meet the minimum standards required to be considered legal tender.

Malaysia

Malaysia requires all exchanges operating within the country to declare their business to Bank Negara and adhere to local AML/CTF requirements.[88] They are also drafting legislation for both initial coin offerings (ICOs)[89] and cryptocurrency, to be completed and enforced in early 2019, under the remit of the Malaysian Securities Commission.[90]

85. Kingdom of Cambodia, 'Joint Statement Between the National Bank of Cambodia, the Securities and Exchange Commission of Cambodia and the General-Commissariat of National Police', 11 May 2018, <https://www.nbc.org.kh/download_files/news_and_events/news_eng/5070Joint_statementNBC_SECC_POLICE_11_May_2018_english.pdf>, accessed 14 March 2019.
86. Samburaj Das, 'Indonesia's Central Bank is Planning to Ban Bitcoin in 2018: Report', *CCN,* 4 December 2017.
87. Samburaj Das, 'Laos Central Bank Warns Public Against Cryptocurrency Trading', *CCN,* 3 September 2018.
88. Bank Negara Malaysia, 'Digital Currencies: Notice to Persons Operating a Business Related to Digital Currencies', <http://www.bnm.gov.my/index.php?ch=en_digital_currency&lang=en>, accessed 14 March 2019.
89. An ICO generally refers to the issues of a cryptocurrency as a form of equity stake in a company, project or undertaking.
90. William Suberg, 'Malaysia Plans to Enact Crypto Regulation in Q1 2019, Finance Minister Reports', *Cointelegraph*, 28 November 2018.

Philippines

The Central Bank of the Philippines (Bangko Sentral Ng Pilipinas) has issued guidelines for crypto exchanges and requires them to adhere to AML/CTF requirements.[91] Similarly, the Securities and Exchange Commission (SEC) has begun drafting regulations for ICOs.[92]

Singapore

In 2014, Singapore was one of the first countries to regulate cryptocurrency use, and some think it is on track to be the first country to fully integrate cryptocurrency into its financial system.[93] Singapore has also offered incentives for crypto firms, such as assistance with opening bank accounts. In late 2018, Singapore began the process of considering a Payment Services Bill that would bring a wide range of cryptocurrency service providers within the supervision of the Monetary Authority of Singapore.[94]

Thailand

Despite announcements in February 2018 that banks must cease crypto-related dealings, in August 2018, the government began allowing local banks to invest in cryptocurrencies, provide brokerage services, run crypto-related businesses and issue digital tokens via subsidiaries. Transactions must only be with businesses approved by the Thailand SEC and Office of Insurance Commission.[95] Cryptocurrencies are viewed legally as 'digital assets and digital tokens' under the purview of the SEC.[96] Exchanges in Thailand must adhere to AML/CTF requirements and obtain an operating licence from the SEC.

Vietnam

In October 2017, the State Bank of Vietnam (SBV) banned Bitcoin as a payment method, and later prohibited industry firms from engaging in crypto-related activities.[97] SBV also plans to suspend

91. Tom Noda, 'Meet the 6 Cryptocurrency Exchanges in Philippines Registered with BSP', *Fintech News Singapore,* 21 September 2018.
92. Nathalie Stucky, 'Philippine SEC Approves Draft Rules for ICOs and Crypto', *Bitcoin.com,* 2 August 2018.
93. Paula Baciu, 'Singapore May Become First Country to Fully Embrace Cryptocurrencies', *Bitcoinist,* 23 September 2018.
94. Mark Emem, 'Singapore: Bill Tabled to Place Crypto Payment Services Under Central Bank Oversight', *CCN*, 27 November 2018.
95. Helen Partz, 'Bank of Thailand Allows Banks to Open Subsidiaries for Crypto Dealings', *Cointelegraph*, 4 August 2018.
96. *Bangkok Post*, 'Cryptocurrency Law Takes Effect', 13 May 2018.
97. Samburaj Das, 'Vietnam Bans Bitcoin as Payment Method; Adopters Face $9,000 Penalty', *CCN,* 30 October 2017.

imports of all cryptocurrency mining equipment.[98] While Prime Minister Nguyen Xuan Phuc has shown interest in cryptocurrencies and has reportedly begun drafting a legal framework for them, some regulators have warned against cryptocurrencies.[99]

Some countries, such as Malaysia, the Philippines and Thailand, have already taken steps to bring cryptocurrency exchanges under their local AML/CTF regulatory frameworks, in a manner generally aligned with guidance issued to date by the FATF. Others, however, such as Indonesia and Vietnam, have prohibited the use of cryptocurrency for payments in addition to mining, but have not fully extended the scope of their local AML/CTF regulation to cover cryptocurrency exchanges. Still other countries in the region have yet to clarify their regulatory approaches.

The FATF has pointed to discrepancies in regulatory approaches as a systemic vulnerability. Some jurisdictions, such as Japan, the EU and the US, regulate cryptocurrency exchange services, requiring that exchanges within their jurisdiction comply with AML/CTF requirements, such as obligations to perform KYC checks, monitor transactions and file suspicious activity reports where they suspect money laundering may be occurring.

However, in many parts of the world, cryptocurrency exchanges remain unregulated and are not required to gather KYC information or impose other AML/CTF measures on customers. In a survey of 23 countries conducted in early 2018, the FATF found that only seven countries had adopted regulation on cryptocurrency exchanges. Extrapolating these numbers more broadly, the FATF notes that this situation 'may make it challenging to ensure a consistent global approach, which could increase risks. Given the highly mobile nature of [cryptocurrencies], there is a risk of regulatory arbitrage or flight to unregulated safe havens'.[100]

If there is an uneven approach to cryptocurrency regulation in Southeast Asia, North Korea could target platforms and users in those countries that do not yet have comprehensive AML/CTF regulatory frameworks in place.

Fortunately, policymakers in the region are laying a foundation for addressing regulatory unevenness across the region. In November 2018, the 4th Regional Counter-Terrorism Financing Summit, an initiative involving Southeast Asian countries and Australia, produced a communiqué that included a call for the development of a region-wide approach to address risks around cryptocurrencies. The communiqué calls for 'understanding the differences and gaps in the region's regulatory frameworks that govern virtual currencies, and working with regional regulators to reduce this regulatory arbitrage'.[101]

98. Samburaj Das, 'Vietnam's Central Bank Approves Call to Suspend Import of Cryptocurrency Miners', *CCN,* 20 July 2018.
99. Lubomir Tassev, 'Vietnam at Crossroads on Cryptocurrency Regulations', *Bitcoin.com,* 11 November 2018.
100. FATF, 'FATF Report to the G20 Finance Ministers and Central Bank Governors', July 2018, p. 3.
101. 4th Regional Counter-Terrorism Financing Summit, 'The Bangkok Communiqué', Bangkok, November 2018, pp. 3–4, <http://www.austrac.gov.au/sites/default/files/Bangkok%20

This recognition of the need for greater regulatory harmonisation is an important step towards mitigating regional vulnerabilities. Chapter III will consider in detail some concrete ways the region could achieve this.

Observation 3: Law Enforcement

Countries across Southeast Asia are undertaking important initial efforts to build law enforcement knowledge and capacity to act against cryptocurrency-related risks. Further efforts can ensure long-term resilience.

Cryptocurrency investigations require that law enforcement agencies have the knowledge and tools at their disposal to successfully conduct forensic analysis and execute legal action in live cases.

Countries in Southeast Asia have taken some important initial steps to educate their local law enforcement agencies on techniques for investigating cryptocurrency-related crimes. For example, in September 2017, the United Nations Office on Drugs and Crime (UNODC) provided training on law enforcement methods for investigating cryptocurrency activity related to terrorist financing, which was attended by delegates from Indonesia, Malaysia, Thailand and the Philippines.[102] In July 2017, UNODC provided training to Thai law enforcement agencies on techniques for tracking and tracing cryptocurrencies.[103]

These are also examples of real-world successes for law enforcement. For example, In February 2018, Thai police seized 100,000 bitcoins (worth approximately $822 million) from a Russian cyber-criminal.[104]

However, given the rapidly evolving nature of the cryptocurrency sector and the range of challenges involved in law enforcement investigations, ensuring that further capacity-building measures are delivered throughout the region will be essential if local partners wish to maintain a resilient defence against a range of illicit finance threats, including those posed by North Korea.

Communique%20-%202018%20CTF%20Summit_2.pdf>, accessed 14 March 2019.

102. United Nations Office on Drugs and Crime (UNODC), 'SE Asian Law Enforcement Agencies Enhance Capacities to Address Virtual Currency Risks in Terrorist Financing', 27 September 2017, <https://www.unodc.org/southeastasiaandpacific/en/2017/09/cryptocurrency-terrorist-financing/story.html>, accessed 14 March 2019.
103. UNODC, 'Thailand Strengthens Capacity to Trace and Investigate Cryptocurrencies', 31 July 2017, <https://www.unodc.org/southeastasiaandpacific/en/2017/07/cryptocurrencies/story.html>, accessed 14 March 2019.
104. Sam Bourgi, 'Thailand Seizes 100,000 Bitcoins in Arrest of Infraud Kingpin Sergey Medvedev', *Hacked*, 12 February 2018.

III. Guidance for Countering the North Korean Cryptocurrency Threat

THIS CHAPTER PROVIDES practical guidance to assist countries in Southeast Asia in mitigating the risk of exposure to, and impact from, North Korea's illicit cryptocurrency use. This guidance reflects RUSI's approach to CPF guidance and is complementary to it,[105] but is designed to address the specific risks presented by cryptocurrencies. It demonstrates how international AML/CTF and CPF standards, including guidance and standards issued by bodies such as the FATF, can be practically implemented to mitigate North Korean-related cryptocurrency risks.

This chapter also offers examples of good practice as evidenced by regulatory and law enforcement actions in various jurisdictions.

Assessing Risk Exposure

As a first step, countries in Southeast Asia should undertake risk assessments at both the local and regional levels to identify vulnerabilities to illicit cryptocurrency activity.

Country-Specific Risk Assessments

The FATF has underscored the importance of countries conducting AML/CTF risk assessments to understand the nature of illicit finance risks they face from cryptocurrencies.

In its June 2015 'Guidance for a Risk-Based Approach: Virtual Currencies', the FATF advised that countries:

> should consider undertaking a coordinated risk assessment of [virtual currency] products and services that (1) enables all relevant authorities to understand how specific [virtual currency] products and services function, fit into, and impact all relevant regulatory jurisdictions for AML/CTF purposes … and (2) promotes similar AML/CTF treatment for similar products and services having similar risk profiles.[106]

105. See Andrea Berger and Anagha Joshi, 'Countering Proliferation Finance: Implementation Guide and Model Law for Governments', RUSI Guidance Paper, July 2017; Dall, Keatinge and Berger, 'Countering Proliferation Finance: An Introductory Guide for Financial Institutions'.
106. FATF, 'Guidance for a Risk-Based Approach: Virtual Currencies', June 2015, p. 8.

In a June 2018 statement, the FATF strengthened this message by calling on all countries to 'urgently take legal and practical steps to prevent the misuse of virtual assets. This includes assessing and understanding the risks associated with virtual assets in their jurisdictions'.[107]

As a general principle, before a country can take effective action to regulate a new product or service, it must first understand the related risks.

Approaches to conducting cryptocurrency-focused risk assessments may draw on methodologies and principles outlined in RUSI's CPF guidance,[108] or the FATF's methodologies for conducting financial crime risk assessments more broadly.[109]

Building on these, below are questions that countries should consider in identifying and assessing their exposure to the types of cryptocurrency-specific risks and vulnerabilities outlined in Chapters I and II of this paper.[110]

Cryptocurrency Infrastructure

- What is the nature of the local cryptocurrency industry? Are there numerous products and services available? If so, which ones?
- How many estimated cryptocurrency users are there locally, and what are the primary purposes for which they use cryptocurrencies?
- What is the local scale of retail use of cryptocurrencies? Do any dealers of high-value goods (such as jewellery stores, auto dealerships and other vendors of luxury items) accept cryptocurrencies as payment?
- How many cryptocurrency exchanges exist locally, and what volumes of cryptocurrency trading do they facilitate?
- Do local cryptocurrency exchanges consistently and sufficiently apply KYC and other AML/CTF requirements?
- Do any cryptocurrency exchanges operating locally offer trading in less traceable cryptocurrencies, such as Monero?
- What other cryptocurrency-related products and services are available and used locally (for example, cryptocurrency prepaid card providers)?
- Are P2P and OTC markets operating locally? If so, at what scale? Do any of these platforms require that users provide KYC information prior to trading?

---

107. FATF, 'Regulation of Virtual Assets'.
108. Berger and Joshi, 'Countering Proliferation Finance: Implementation Guide and Model Law for Governments', pp. 9–10.
109. FATF, 'Methodology: For Assessing Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems', February 2013.
110. For more information regarding how to identify the appropriate government agencies and regulators to conduct a risk assessment, see Berger and Joshi, 'Countering Proliferation Financing', pp. 25–26.

- Is cryptocurrency mining permitted locally? If mining occurs locally, is it known who conducts this mining activity? Is there any indication that local mining pools may include the presence of North Korean individuals, or that North Korea might access local servers or other IT infrastructure locally to facilitate mining activity?
- Does the jurisdiction have any previous cases involving proliferation networks or sanctions evasion related to proliferation? Are North Korean networks known to have operated locally, and could these networks access cryptocurrency-based products and services?

Illicit Finance Risks

- Have any significant cases of money laundering, terrorist financing, proliferation financing or other financial crimes featuring cryptocurrencies occurred locally?
- What is the nature of predicate offences that have accompanied any known criminal cases involving cryptocurrencies?
- How has law enforcement responded to any instances of criminal use of cryptocurrencies locally?

Cyber Security Risks

- How aware are local cryptocurrency platform operators and administrators of cyber security risks?
- Do local platforms have crisis mitigation plans in place for responding to hacks?
- Have any local cryptocurrency exchanges or other platforms been hacked? If so, what was the size of the consequent theft? How did the impacted platform(s) respond?
- How aware are individual users of cryptocurrencies of the risks involved, and do they know how to protect themselves from hacking and theft?
- Are there any known instances of North Korean networks operating locally that could pose a risk to local cryptocurrency service providers and could compromise their systems, for example by embedding individuals among staff at a cryptocurrency exchange?

Regulatory Frameworks

- What is the nature of the local regulatory framework and how does it compare to the FATF's guidance issued to date?
- Does the local regulatory framework contain any exploitable gaps? For example, are crypto-to-crypto exchanges that allow users to swap transparency cryptocurrencies like Bitcoin for privacy coins like Monero covered by local regulation?
- How knowledgeable are local regulators about cryptocurrencies and do they possess the appropriate resources for ensuring adequate supervision?

Box 4: Best Practice – Domestic Cryptocurrency Risk Assessments

Some countries have begun to consider the risks cryptocurrencies pose to their financial systems.

In its 2017 *National Risk Assessment of Money Laundering and Terrorist Financing*, the UK government evaluated risks arising from cryptocurrencies. It assessed the risks as low based on the low volumes traded domestically, but noted the likelihood that these risks could increase given the use of cryptocurrencies in cybercrime cases. Other EU countries that have assessed cryptocurrency risks at the local level include Belgium, France, the Netherlands and Ireland.

Sources: HM Treasury and the Home Office, National Risk Assessment of Money Laundering and Terrorist Financing 2017 *(London: The Stationery Office, October 2017), p. 38; Belgian Financial Intelligence Processing Unit, '24th Annual Report', 2017, p. 26, <http://www.ctif-cfi.be/website/images/EN/annual_report/ar%202017%20en%20final.pdf>, accessed 14 March 2019; TRACFIN, 'Regulating Virtual Currencies: Recommendations to Prevent Virtual Currencies from Being Used for Fraudulent Purposes and Money Laundering', June 2014, <https://www.economie.gouv.fr/files/regulatingvirtualcurrencies.pdf>, accessed 14 March 2019; Anti Money Laundering Centre, 'The Bitcoin Trader: A Facilitating Role in the Cash Out of Criminal Proceeds', August 2017, <https://www.fiu-nederland.nl/sites/www.fiu-nederland.nl/files/documenten/note_the_bitcoin_trader_amlc_september_2017.pdf>, accessed 14 March 2019; Department of Finance and Department of Justice and Equality, 'National Risk Assessment for Ireland: Money Laundering and Terrorist Financing', October 2016, <http://www.justice.ie/en/JELR/National_Risk_Assessment_Money_Laundering_and_Terrorist_Financing_Oct16.pdf/Files/National_Risk_Assessment_Money_Laundering_and_Terrorist_Financing_Oct16.pdf>, accessed 26 March 2019.*

Region-Wide Risk Assessments

In addition to country-specific risk assessments, stakeholders in Southeast Asia should undertake a joint regional risk assessment on cryptocurrencies.

Regional risk assessments can identify cross-cutting gaps and points of vulnerability impacting numerous countries, allowing regional partners to develop coordinated strategies for addressing challenges. This is particularly important when dealing with a cross-border, decentralised technology such as cryptocurrencies.

Southeast Asia has experience in conducting region-wide risk assessments on other AML/CTF matters and can build on those to assess regional cryptocurrency risks. For example, under the framework of Regional CTF Summits held since 2015, Southeast Asian governments have collaborated with Australia to examine terrorist-financing risks facing the region and to develop collaborative CTF approaches. In 2016, this led to the publication of a Regional Risk Assessment

on Terrorism Financing,[111] and in 2018 the release of a regional risk assessment exercise focused on terrorist-financing risks in the not-for-profit sector.[112]

Countries in Southeast Asia can use the methodologies deployed in these previous regional risk assessments to identify and understand any cross-cutting risks posed by cryptocurrencies, including those that relate to North Korean proliferation financing risk.

Box 5: Best Practice – Regional Risk Assessments on Cryptocurrencies

In June 2017, the EU published findings of a supranational risk assessment (SRA) exercise it conducted to understand the collective money-laundering and terrorist-financing risks facing Europe. The SRA contains a section on virtual currencies.

The SRA judged the threat posed by virtual currencies as moderately significant at the time, given low levels of adoption, but noted that the EU was highly vulnerable to illicit activity owing to the lack of a regulatory framework for virtual currency exchange services. These findings helped to support the adoption of the EU's Fifth Anti-Money Laundering Directive (5AMLD), which brings fiat-to-cryptocurrency exchanges within the scope of AML requirements.

Source: European Commission, 'Report from the Commission to the European Parliament and the Council on the Assessment of the Risks of Money Laundering and Terrorist Financing Affecting the Internal Market Relating to Cross-Border Activities', 26 June 2017, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017SC0241>, accessed 14 March 2019.

Closing Regulatory and Security Gaps

As the FATF suggests, countries should use risk assessment exercises to develop appropriate risk-based regulatory frameworks for cryptocurrencies. Where designed and implemented successfully, these frameworks can contribute to curbing North Korean proliferation financing risks.

Determining what constitutes an appropriate framework will vary from country to country based on local cryptocurrency risk exposure and the nature of existing AML/CTF legal and regulatory arrangements.

111. Commonwealth of Australia, 'Regional Risk Assessment 2016: Terrorism Financing, Southeast Asia and Australia', 2016, <http://www.austrac.gov.au/sites/default/files/regional-risk-assessment-SMALL_0.pdf>, accessed 14 March 2019.
112. Commonwealth of Australia, 'Regional Risk Assessment 2017: Non-Profit Organisations and Terrorism Financing', 2017, <http://www.austrac.gov.au/sites/default/files/regional-NPO-risk-assessment-WEB-READY_ss.pdf>, accessed 14 March 2019.

However, there are certain general principles that countries should consider when choosing how to regulate the cryptocurrency space.

Designing a Regulatory Framework

Countries should consider whether to rely on existing regulatory measures, or whether the creation of new, bespoke regimes is required.

The US has taken the former approach. In March 2013, FinCEN issued guidance indicating that it regards virtual currency exchange providers as money transmitters under existing US AML/CTF measures.[113] As a result, cryptocurrency exchanges and other platforms must apply AML/CTF requirements as set out in the US Bank Secrecy Act (1970). Recently, North American exchanges have been found to have a lower percentage of illicit activity as compared to European exchanges not subject to these requirements.[114]

Japan has taken a similar approach to the US, legislating in April 2017 to regulate cryptocurrency exchanges within the scope of its Financial Services Act (FSA).[115] Japan has since provided licenses to 16 cryptocurrency exchanges to date under these measures.[116]

The extension of existing frameworks to the cryptocurrency space can prove advantageous insofar as it generally allows regulators to apply requirements relatively swiftly, and within the scope of measures they have experience implementing.

By contrast, some jurisdictions have established entirely new, bespoke frameworks for cryptocurrencies. These jurisdictions have determined that their existing AML/CTF frameworks are not sufficient to mitigate the full range of risks related to cryptocurrencies and that new approaches are necessary. Examples include:

- **New York state, US**: In 2015, the New York Department of Financial Services launched its BitLicense framework,[117] which requires providers of cryptocurrency services to seek

113. FinCEN, 'FinCEN Issues Guidance on Virtual Currencies and Regulatory Responsibilities', 18 March 2013, <https://www.fincen.gov/sites/default/files/news_release/20130318.pdf>, accessed 14 March 2019.
114. Yaya J Fanusie and Tom Robinson, 'Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services', 12 January 2018, <https://www.fdd.org/wp-content/uploads/2018/01/MEMO_Bitcoin_Laundering.pdf>, accessed 14 March 2019.
115. Library of Congress, 'Regulation of Cryptocurrency: Japan', last updated 18 June 2018, <https://www.loc.gov/law/help/cryptocurrency/japan.php>, accessed 14 March 2019.
116. Samburaj Das, 'Japan's 16 Licensed Cryptocurrency Exchanges Launch Self-Regulatory Body', *CCN*, 24 April 2018.
117. Nikiforos Mathews and Jonas Robison, 'NYDFS Finalises BitLicense Regulations', Orrick, 11 June 2015, <https://blogs.orrick.com/derivatives/2015/06/11/nydfs-finalizes-bitlicense-regulation/#_ftn1>, accessed 14 March 2019.

regulatory approval prior to providing any proscribed activities within, or to persons resident in, New York state.

- **Malta**: In early 2018, Malta adopted the Virtual Financial Assets Act,[118] which requires cryptocurrency platforms to register with approved agents prior to obtaining authorisation to operate locally.
- **Bermuda**: In July 2018, Bermuda adopted the Virtual Currency Business Act,[119] which sets out a licensing and registration scheme for cryptocurrency businesses similar to Malta's regime.
- **Gibraltar**: In January 2018, Gibraltar adopted the Distributed Ledger Technology Regulatory Framework,[120] which brings cryptocurrency exchanges and other platforms within the scope of its AML requirements and establishes a bespoke licensing regime.

Bespoke regimes may present an advantage by providing a framework for enabling oversight of a new set of service providers and by tailoring licensing and examination requirements to meet the demands of supervising a new and complex industry.

Ensuring a Comprehensive Regulatory Framework

After determining the appropriate approach, countries should ensure that their framework is comprehensive. In October 2018, the FATF adopted a new definition of virtual asset service providers and suggested that countries should have measures in place to apply AML/CTF regulation to those platforms and services that facilitate:

- the exchange between virtual assets and fiat currencies;
- the exchange between one or more forms of virtual assets;
- the transfer of virtual assets;
- the safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; or
- the participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.[121]

It is important in drafting regulation that countries ensure their frameworks cover the full range of services described in the FATF. Failure to do so can result in significant regulatory gaps.

118. See 'Virtual Financial Assets Act 2018 (Malta)'.
119. See 'Virtual Currency Business Act 2018 (Bermuda)'.
120. Gibraltar Financial Services Commission, 'Distributed Ledger Technology Regulatory Framework', <http://www.gfsc.gi/dlt>, accessed 14 March 2019.
121. FATF, 'The FATF Recommendations', October 2018, p. 125.

For example, the EU's 5AMLD regulates cryptocurrency exchange businesses that enable conversion between cryptocurrencies and fiat currencies; however, the EU's measures do not presently apply to businesses that facilitate exchange between different cryptocurrencies.[122]

Hence, activities such as the exchange of Bitcoin for Monero – activity North Korea undertook to obfuscate the proceeds of the WannaCry attack – are not presently regulated in the EU.

Box 6: Best Practice – Comprehensive Regulation

The US has in place a framework that applies AML/CTF requirements to a broad range of cryptocurrency service providers. The US's regulations apply to cryptocurrency exchange services that facilitate not only the exchange of cryptocurrency for fiat currency, but also those platforms that enable customers to swap among different types of cryptocurrencies.

US regulators have also indicated that platforms that issue and facilitate the exchange of initial ICOs fall within the scope of US AML/CTF requirements.

Sources: FinCEN, 'Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies', 18 March 2013, <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf>, accessed 14 March 2019; Letter from US Assistant Secretary for Legislative Affairs Drew Maloney to Senator Ron Wyden, 13 February 2018, <https://coincenter.org/files/2018-03/fincen-ico-letter-march-2018-coin-center.pdf>, accessed 14 March 2019.

Given the significant cyber-security risks around cryptocurrencies, to ensure comprehensiveness countries should also consider requiring cryptocurrency exchanges to have specific cyber-security measures in place to protect against hacking and theft.

Several jurisdictions already require this. For example, New York state and Bermuda both require that cryptocurrency businesses have in place crisis response and mitigation measures to protect against cyber-security risks.[123]

Furthermore, countries should leverage financial and economic sanctions authorities in ensuring effective oversight of cryptocurrency activity, including as it relates to the types of illicit activity conducted by North Korea.

122. See Tom Keatinge, David Carlisle and Florence Keen, *Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses* (Brussels: European Parliament, May 2018).
123. Protiviti, 'Cybersecurity Regulation Overview', 2017, <https://www.protiviti.com/sites/default/files/japan/insights/cybersecurity-regulation-overview-e.pdf>, accessed 14 March 2019; Banking & Insurance by Sia Partners, 'Bermuda's Virtual Currency Business Act: Analysis of Key Points', 30 July 2018, <http://en.finance.sia-partners.com/20180730/bermudas-virtual-currency-business-act-analysis-key-points>, accessed 19 March 2019.

In early 2018, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) issued guidance clarifying that US sanctions requirements apply to cryptocurrencies, just as they do to fiat currencies.[124] In November 2018, OFAC then issued sanctions against two Iranian individuals involved in facilitating Bitcoin transactions for ransomware attackers. In sanctioning the two individuals, OFAC included on its sanctions list the Bitcoin addresses belonging to them.

By providing these addresses, OFAC has made clear that US persons may not transact with those two specific Bitcoin addresses; breaches of those sanctions would result in significant penalties for US persons, and non-US persons that transact with those listed addresses could find themselves subject to sanctions as well.[125]

Similar action taken against North Korean actors – such as perpetrators of cybercrime attacks, or financial facilitators of the North Korean regime known to be facilitating business in cryptocurrencies – could impact North Korea's ability to use cryptocurrencies.

Implementing a Regulatory Framework

Once a cryptocurrency regulatory framework is chosen, it must be implemented effectively. The FATF has indicated that by June 2019 it will issue further guidance on implementing supervisory regimes for cryptocurrencies.[126] Until then, there are several points that countries should consider.

Countries should provide detailed guidance to the private sector to enable cryptocurrency exchange businesses and other platforms to implement compliance and risk mitigation requirements. In the US, FinCEN has issued numerous pieces of regulatory guidance to clarify the scope of measures related to cryptocurrencies and to alert financial institutions to risks related to cryptocurrencies.[127]

Australia has also issued substantive and meaningful regulatory guidance on cryptocurrencies. Shortly after bringing cryptocurrency exchange platforms within the scope of its AML/CTF requirements, AUSTRAC, the Australian financial intelligence unit (FIU), issued written

124. See US Department of the Treasury, 'OFAC FAQs: Sanctions Compliance', last updated 6 February 2019, <https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#vc_faqs>, accessed 19 March 2019.
125. US Department of the Treasury, 'Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses', press release, 28 November 2018, <https://home.treasury.gov/news/press-releases/sm556>, accessed 19 March 2019.
126. Qadir AK, 'Paris Based FATF to Bring Out Cryptocurrency Regulations by June 2019', *Coin Pedia*, 20 October 2018.
127. See, for example, FinCEN, 'Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System'.

guidance for financial institutions and provided live video consultations.[128] These live sessions allowed AUSTRAC to explain the implications of regulatory requirements to stakeholders in the cryptocurrency industry, and allowed industry participants to ask questions directly of regulators.

Ensuring the effectiveness of regulation also requires robust enforcement of measures. Countries should be able to issue fines, penalties and other putative measures where cryptocurrency businesses violate AML/CTF and CPF requirements. Enabling robust enforcement can entail several elements, including:

- ensuring that legal arrangements provide for proportionate penalties;
- ensuring that enforcement bodies are adequately staffed and knowledgeable to identify and act upon violations by cryptocurrency businesses;
- ensuring that supervisory bodies regularly conduct onsite visits of exchanges;
- and ensuring that enforcement bodies have access to advanced analytical tools that can allow them to monitor illicit activity involving cryptocurrencies, enabling them to spot violations in practice.

Box 7: Best Practice – Effective Enforcement of Cryptocurrency Regulation

The US and Japan have applied robust and proportionate enforcement on detecting regulatory violations in the cryptocurrency space.

For example, in July 2017, the US acted against BTC-e, a cryptocurrency exchange, and one of its owners, Alexander Vinnik, for wilful violations of US AML/CTF requirements. FinCEN assessed a $110 million civil penalty against BTC-e for its failure to obtain appropriate identifying information and for processing illegal transactions for dark web vendors and cyber-criminals. The action coincided with a US law enforcement action against BTC-e that resulted in Vinnik's arrest.

In March 2018, Japanese regulators responded to the hack of the Coincheck cryptocurrency exchange by undertaking a review of security practices in the sector. Regulators suspended the licences of two Japanese cryptocurrency exchanges for a 30-day period and issued business improvement orders to a further five local cryptocurrency exchanges, requiring them to improve security practices.

Sources: US Department of Justice, 'Russian National and Bitcoin Exchange Charged in 21-Count Indictment for Operating Alleged International Money Laundering Scheme and Allegedly Laundering Funds from Hack of Mt. Gox', press release, 26 July 2017, <https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged>, accessed

128. AUSTRAC, 'Digital Currency Exchange Providers', last updated 20 December 2018, <http://www.austrac.gov.au/digital-currency-exchange-providers>, accessed 14 March 2019; AUSTRAC, 'SMR and Digital Currency Exchange Provider Webinar Recording', last updated 7 August 2018, <http://www.austrac.gov.au/smr-and-digital-currency-exchange-provider-webinar-recording>, accessed 14 March 2019.

14 March 2019; Jake Adelstein, 'Japan Shuts Down Two Cryptocurrency Exchanges but it May be Good News for the Industry', Forbes*, 8 March 2018.*

Another factor to consider in assessing the effectiveness of regulatory responses is whether regulation enables and aligns with other policy goals.

For example, fostering financial inclusion is a policy objective that the FATF, and numerous individual countries, have suggested must be reconciled with AML/CTF and CPF requirements.[129] Regulatory responses that seek to ban cryptocurrency exchanges and other services from operating could result in cryptocurrency platforms becoming inaccessible to many people – which could run counter to financial inclusion efforts. In many jurisdictions, banks have cited the lack of a regulatory framework as a factor leading them to deny banking services to cryptocurrency businesses – a trend that may only lead cryptocurrency businesses to seek banking services in more opaque jurisdictions.[130]

Therefore, it is important to consider how regulatory bodies can address and resolve the sometimes challenging and competing aims of ensuring robust AML and CPF measures while promoting financial innovation and inclusion. Singapore, as an example, has indicated its intention to assist cryptocurrency businesses in obtaining bank accounts to avoid de-risking of the sector.[131] De-risking refers to the process of banks denying access to or withdrawing the provision of services from wide sections of the financial sector due to higher compliance risks in those populations.

The 2018 Southeast Asia CTF Summit communiqué also highlights the need to reconcile the needs of combating financial crime with preventing de-risking as a regional aim, noting that it is essential to 'address the risks of virtual currencies whilst embracing their opportunities by promoting financial inclusion and seeking to prevent "de-risking" occurring in the private and NGO sectors'.[132]

These considerations around effectiveness are particularly important for countries that decide to take a prohibitive stance on cryptocurrencies – including going so far as banning the trading and use of cryptocurrencies all together. China, for example, has banned cryptocurrency exchanges from operating within its jurisdiction and has enacted severe restrictions on mining and other

129. FATF, Asia/Pacific Group on Money Laundering and the World Bank, 'FATF Guidance: Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion', February 2013.
130. Martin Arnold, 'Cryptocurrency Companies Forced to Bank Outside UK', *Financial Times*, 23 October 2017.
131. Matthew Beedham, 'Singapore's Financial Regulator Wants its Banks and Blockchains to be Friends', *Next Web*, 11 October 2018.
132. 4th Regional Counter-Terrorism Financing Summit, 'The Bangkok Communiqué', p. 3.

related activities. The Chinese government has indicated that these restrictions are essential in enabling it to meet certain policy goals.

The FATF has acknowledged that banning cryptocurrencies may be an appropriate response to managing related risks, but has stressed that where countries choose to do so, they should ensure that bans are effectively enforced.[133]

However, publicly available information sheds doubt on claims that banning cryptocurrency activity is effective in mitigating illicit financing risks.

For example, as noted earlier, P2P and OTC cryptocurrency markets have thrived in countries such as China that have attempted to restrict formalised cryptocurrency businesses. This suggests, firstly, that users will generally find ways to fulfil their demand for cryptocurrency despite prohibitions, and secondly, that one result of banning cryptocurrency activity may merely be the migration of activity to less transparent OTC channels, where crime may be more difficult to detect and monitor.

Enabling Interagency Collaboration

In its 2015 guidance, the FATF outlined the need for interagency cooperation to manage cryptocurrency risks. It advised that:

> Countries may consider putting in place mechanisms, such as inter-agency working groups, to enable policy-makers, regulators, supervisors, the financial intelligence unit (FIU), and law enforcement authorities to cooperate with each other and any other relevant competent authorities to develop and implement effective policies, regulations and other measures to address [cryptocurrency-related money-laundering and terrorist-financing] risks.[134]

Furthermore, the FATF Recommendations point to the importance of interagency coordination for ensuring the effectiveness of AML/CTF and CPF risks more generally. FATF Recommendation 2 states that:

> Countries should ensure that policy-makers, the [FIU], law enforcement authorities, supervisors and other relevant competent authorities, at the policy-making and operational levels, have effective mechanisms in place which enable them to cooperate, and, where appropriate, coordinate and exchange information domestically with each other concerning the development and implementation of policies and activities to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.[135]

133. FATF, 'Regulation of Virtual Assets'.
134. FATF, 'Guidance for a Risk-Based Approach: Virtual Currencies', p. 9.
135. FATF, 'The FATF Recommendations', p. 9.

Interagency cooperation allows authorities to share information on risks they identify and to design more effective regulation based on a shared understanding of risks. Interagency efforts can focus on issues including:

- understanding the nature of cryptocurrency risk, including North Korea-related activity, faced locally;
- identifying security gaps that exist and developing concrete measures to address those gaps;
- discussing and developing regulatory approaches to cryptocurrencies;
- sharing information on investigations involving cryptocurrencies; and
- developing an intelligence picture around the illicit use of cryptocurrencies locally.

To enable interagency collaboration on these and related topics, countries must, first, identify appropriate participants, and, second, establish appropriate fora.

Identifying Participants

Owing to the highly technical nature of cryptocurrencies, it is important that interagency collaboration efforts draw expertise across public sector agencies. This can include, but are not necessarily limited to:

- FIUs;
- regulators;
- supervisory authorities;
- competent authorities with responsibility for implementing financial and economic sanctions measures;
- cyber-security agencies, particularly those with experience in investigating cryptocurrency-enabled crimes such as ransomware;
- agencies with responsibility for designing and implementing CPF measures;
- law enforcement agencies with involvement in digital forensics;
- intelligence agencies with responsibility for gathering information on North Korea (or other state actors);
- law enforcement bodies with experience investigating cryptocurrency use in dark web marketplaces; and
- NGOs, think tanks, and public–private alliances (discussed further below).

Participants will vary country by country based on their unique circumstances and governing arrangements, but the aim should be to ensure that the appropriate individuals with relevant technical, regulatory and legal expertise are included.

Establishing Interagency Forums

Countries may rely on existing forums, such as pre-established CPF taskforces, for addressing cryptocurrency-related risks. Where these taskforces have operated successfully and have a

track record of delivering beneficial outcomes, integrating discussions of cryptocurrencies into them may be the most effective solution.

However, some countries may decide that establishing new arrangements is more appropriate. Rather than relying on existing forums or purely ad hoc interactions, establishing dedicated forums for enabling relevant participants to focus on cryptocurrency-related issues provides a benefit insofar as it permits stakeholders to develop and deepen expertise on the topic.

One model that some countries have adopted are cryptocurrency-focused taskforces (see Box 8). Domestic cryptocurrency task forces can serve several functions, including:

- ensuring that cryptocurrency issues are addressed with an appropriate level of urgency and receive high-level attention;
- providing a platform for ongoing engagement among stakeholders; and
- clarifying intentions among stakeholders and ensuring that overlapping requirements and aims are reconciled.

Box 8: Best Practice – Cryptocurrency Taskforces

In May 2018, the UK assembled an interagency Cryptoasset Taskforce, which pooled expertise from HM Treasury, the Financial Conduct Authority and the Bank of England to examine opportunities and risks related to cryptocurrencies.

The Taskforce's meetings included engagement with private sector stakeholders in the cryptocurrency industry. In October 2018, the Taskforce published a report of its findings. The report identified areas in which the UK could attempt to become an innovator in cryptocurrency-related activity and set out a road map for undertaking regulatory action.

Source: HM Treasury, Financial Conduct Authority and the Bank of England, Cryptoassets Taskforce: Final Report *(London: The Stationery Office, October 2018).*

Developing Coordinated Regional Responses

Because cryptocurrencies are international in nature, it is important that countries in Southeast Asia work collaboratively to address the risks they present and devise appropriate responses to counter cryptocurrency risk as part of a wider strategy of mitigating North Korean proliferation finance risks. Domestic efforts and initiatives are more effective when supported by region-wide efforts.

Regional efforts can provide the benefit of enabling countries to:

- share experiences and ideas;
- identify common challenges and risks;
- cooperate on joint investigations; and
- pool resources and facilitate knowledge transfer.

As noted earlier, in the form of the CTF Summit, Southeast Asia has already developed a promising collaborative framework that is undertaking initial exploration of cryptocurrency-related issues.

With time, regional partners may consider a regional cryptocurrency-focused forum that sits outside the CTF Summit framework. Europe has developed such a mechanism that may offer a useful model, as described in Box 9, and that could be tailored to enable discussion of CPF strategies aimed at North Korea.

Box 9: Best Practice – Developing Coordinated Regional Responses on Cryptocurrencies

In September 2016, Europol, Interpol and the Basel Institute on Governance founded a Digital Currencies Working Group. The working group has several aims, including:

- gathering and analysing non-operational information from law enforcement agencies on cryptocurrencies;
- organising workshops to enable law enforcement agencies across Europe to share experiences and expertise; and
- creating a network of practitioners among European law enforcement agencies and other relevant stakeholders in the region.

Source: Europol, 'Money Laundering with Digital Currencies: Working Group Established', press release, 9 September 2016, <https://www.europol.europa.eu/newsroom/news/money-laundering-digital-currencies-working-group-established>, accessed 14 March 2019.

Enhancing Law Enforcement Knowledge and Capacity

As noted earlier, countries in Southeast Asia are taking important steps to train law enforcement agencies on investigating cases of illicit cryptocurrency use.

But cryptocurrencies are a complex, rapidly evolving technology. Capacity-building efforts should be sustained, frequent and comprehensive. Issues that countries in the region should ensure are covered in training efforts include:

- the nature and types of cryptocurrency-enabled crime;
- typologies of North Korean use of cryptocurrencies;
- how to identify different types of wallets and other infrastructure (such as mining equipment) during an investigation;
- forensic techniques for investigating the flow of illicit cryptocurrencies;
- the nature of available investigative tools and for tracing illicit activity involving cryptocurrencies; and
- practices for the seizure and confiscation of cryptocurrencies in criminal cases.

Training efforts can be enhanced where they are coordinated with regional partners. Countries in the region should identify opportunities for collaborative training and consider establishing a formal mechanism for doing so.

As noted earlier, some regional partners have engaged in training with bodies such as the UNODC. Southeast Asian countries should pursue further training efforts while leveraging technical assistance from other international bodies, such as the Asia/Pacific Group on Money Laundering, that have experience in devising cryptocurrency-related regulatory and law enforcement responses. Country-to-country exchanges of best practice among partners in Southeast Asia can further these general capacity-building efforts as well.

Formalising training as part of ongoing, dedicated forums would help to ensure that capacity-building efforts are sustained.

Box 10: Best Practice – Law Enforcement Awareness and Capacity Building

In January 2018, the Digital Currencies Working Group established by Europol organised a two-day workshop that brought together law enforcement officers from 32 countries. The workshop focused on sharing information and best practices about the detection, investigation, seizure and confiscation of cryptocurrencies. In June 2018, Europol's European Cybercrime Centre held their 5th Virtual Currencies Conference, which included 300 participants from 40 countries, to discuss how to foster legitimate uses of cryptocurrencies. This conference brought together not only law enforcement personnel, but also cryptocurrency experts and private sector participants.

Sources: Europol, 'Global Workshop for Financial Investigators on Detection, Investigation, Seizure and Confiscation of Cryptocurrencies', press release, 26 January 2018, <https://www.europol.europa.eu/newsroom/news/global-workshop-for-financial-investigators-detection-investigation-seizure-and-confiscation-of-cryptocurrencies>, accessed 14 March 2019; Europol, 'Cryptocurrency Meets Law Enforcement at Europol's 5th Virtual Currencies Conference', 21 June 2018, <https://www.europol.

europa.eu/newsroom/news/cryptocurrency-meets-law-enforcement-europol%E2%80%99s-5th-virtual-currencies-conference>, accessed 14 March 2019.

Promoting Private Sector and Consumer Knowledge and Awareness

As noted in Chapter I, poor security practices by cryptocurrency exchanges, and even individual users of cryptocurrencies, represent a major vulnerability where they leave cryptocurrencies vulnerable to hacking and theft.

Promoting enhanced knowledge and awareness about security risks can prove an important method for bolstering a first line of defence against risks.

Educational improvement efforts can take several forms, including:

- including industry participants in law enforcement training sessions (see Box 10).
- conducting surveys of security practices among industry participants (see Box 11);
- launching informational campaigns about crimes such as ransomware and cryptojacking (see Box 12);

Box 11: Best Practice – Cryptocurrency Industry Surveys

In September 2018, the New York State Attorney General's Office issued a Virtual Markets Integrity Initiative Report, which provided consumers with information on cryptocurrency industry practices and assessed industry vulnerabilities to abuse, security breaches and market manipulation. The Attorney General's Office surveyed cryptocurrency exchanges to understand their security and market integrity practices.

The report found security lapses among New York cryptocurrency exchanges. Chief among these was the report's observation that 'protections for customer funds are often limited or illusory ... Customers are highly exposed in the event of a hack or unauthorized withdrawal'.

The report educates consumers of cryptocurrencies about risks they may face when using exchanges, but it also acts as an educational opportunity for cryptocurrency businesses to understand how to improve security practices.

Source: Office of the State Attorney General of New York, 'Virtual Markets Integrity Initiative Report', 18 September 2018, p. 7, <https://ag.ny.gov/sites/default/files/vmii_report.pdf>, accessed 14 March 2019.

Box 12: Best Practice – Informational Campaigns

To promote awareness about the risks of ransomware, Europol and the Dutch National Police collaborated with private security agencies to launch the No More Ransom! campaign.

The campaign provides public information on ransomware prevention techniques, as well as decryption tools to enable victims of ransomware to recover their files without having to pay ransoms that would ultimately benefit cybercriminals.

Source: European Cybercrime Centre, Politie and McAfee, 'No More Ransom!', <https://www.nomoreransom.org/en/index.html>, accessed 14 March 2019.

Facilitating Public–Private Partnerships

Educating the private sector about risks in an informal and ad hoc way has its uses. But it is important that formalised public–private partnerships (PPPs) are developed to tackle the illicit finance risks around cryptocurrencies.

PPPs in the cryptocurrency space can enable law enforcement, regulators and other public sector stakeholders to communicate concerns, challenges and objectives with the cryptocurrency industry. PPPs also enable industry participants to educate the public sector about features of the technology, and to share experiences regarding their direct encounters with illicit actors.

RUSI's previous CPF guidance papers note several advantages to establishing PPPs and set out considerations that can inform the decision about how best to establish and maintain PPPs.[136] The FATF has also set out guidance for the development of PPPs for combating financial crime more broadly.[137] Countries should consider how these principles can be most effectively applied to the cryptocurrency space.

An example of a cryptocurrency-focused PPP already underway is the Blockchain Alliance. Founded in 2015, the Blockchain Alliance's membership includes nearly three dozen cryptocurrency industry participants,[138] primarily cryptocurrency exchanges and cryptocurrency forensics analysis companies located in the US and Europe. Its membership includes law enforcement agencies in the US, such as the Department of Justice, the FBI and the Drug Enforcement Administration, as well as Europol and others.[139]

136. Joshi, 'Model Provisions'; Dall, Keatinge and Berger, 'Countering Proliferation Finance'.
137. FATF, 'FATF Guidance: Private Sector Information Sharing', November 2017.
138. See Blockchain Alliance, 'A Public–Private Forum to Help Combat Criminal Activity on the Blockchain', 2016, <https://blockchainalliance.org/>, accessed 14 March 2019.
139. Blockchain Alliance and Steptoe and Johnson, 'The Blockchain Alliance', presentation given to the Association of Certified Anti-Money Laundering Specialists (ACAMs) in Toronto, 7 February 2017.

The Blockchain Alliance allows members to share non-operational information about illicit activity in cryptocurrencies, and techniques and methods for ensuring the successful detection and disruption of illicit activity in cryptocurrencies. Members can also share alerts about new criminal methods and trends they observe.

Countries and cryptocurrency industry participants in Southeast Asia should seek to engage these established forums and to develop similar, localised forums to further North Korea-focused CPF efforts.

Conclusions

THE SCALE AND scope of North Korea's cryptocurrency activity has expanded since the May 2017 WannaCry ransomware attack. As a determined and sophisticated cyber actor in need of financial resources, North Korea is likely to continue to find ways of obtaining and exploiting cryptocurrencies. The prospect of North Korea engaging in large-scale sanctions circumvention using cryptocurrencies as a means of payment for prohibited service such as luxury goods or facilitating prohibited transfers is a risk that could grow as well.

Countries in Southeast Asia face several vulnerabilities to the types of illicit activity North Korea has engaged in using cryptocurrencies. The region's presently uncoordinated approaches to the regulation of cryptocurrencies creates a systemic risk such that its growing cryptocurrency industry may be exploited by North Korea and affiliated networks.

Countries in the region can take several steps to mitigate vulnerabilities.

First, they should assess local cryptocurrency risks and vulnerabilities that North Korea could exploit. This should include identifying whether North Korean proliferation networks operate locally and could exploit any local cryptocurrency infrastructure. Local risk assessments can also be complemented by a regional risk assessment aimed at identifying cross-cutting exposure to the types of cryptocurrency-related risks North Korea presents.

Second, countries in Southeast Asia should design appropriate regulatory responses that enable them to mitigate a range of AML/CTF and CPF risks, including those posed by North Korea. These frameworks should be sufficiently broad in scope to ensure that activity in which North Korea is engaged is subject to regulatory oversight.

Third, countries at the domestic level should ensure that they facilitate successful interagency collaboration. This can be accomplished by integrating discussions of cryptocurrencies into existing interagency CPF frameworks, or creating new cryptocurrency-dedicated forums that include discussion of North Korean-related risks.

Fourth, Southeast Asian countries should develop coordinated regional responses. This could include relying on the existing CTF Summit framework, or, conversely, establishing a regional cryptocurrency policy coordination framework.

Fifth, regional partners should ensure additional ongoing law enforcement training to enable the successful detection and prevention of North Korean-related cryptocurrency activity. Training should be ongoing and collaborative, including country-to-country exchanges of expertise and information, and leveraging technical assistance from international organisations and regional partners.

Sixth, private sector education and awareness-raising activities can draw attention to security risks and vulnerabilities so that cryptocurrency industry participants and individual consumers are better equipped to act as a first line of defence against risks.

Finally, partners in Southeast Asia should leverage public–private partnership arrangements, which can allow cryptocurrency industry participants to learn from local law enforcement and regulators about their experiences in encountering the types of cryptocurrency-related risks North Korea poses, and can enable participants to devise collective strategies for ensuring effective risk mitigation.

If carried out with the appropriate urgency and in line with global AML/CTF and CPF standards, countries in the region can succeed in making themselves less vulnerable to the risks of North Korean cryptocurrency activity.

Annex I: Further Reading

Financial Action Task Force (FATF) Guidance

- FATF, 'Guidance for a Risk Based Approach: Virtual Currencies', June 2015.
- FATF, 'Regulation of Virtual Assets', October 2018.
- FATF, 'Virtual Currencies: Key Definitions and Potential AML/CFT Risks', June 2014.
- FATF, 'Public Statement – Mitigating Risks from Virtual Assets', 22 February 2019.

UN Guidance

- United Nations Security Council, 'Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)', 21 February 2019, S/2019/171.

Example Cryptocurrency Regulations

- 'Digital Asset Business Act 2018 (Bermuda)'.
- Gibraltar Financial Services Commission, 'Distributed Ledger Technology Regulatory Framework (DLT Framework)', May 2017, <http://www.gfsc.gi/dlt>, accessed 9 April 2019.
- 'Virtual Financial Assets Act 2018 (Malta)'.
- US Department of the Treasury, Financial Crimes Enforcement Network (FinCEN), 'Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies', March 2013, <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf>, accessed 9 April 2019.

RUSI CPF Guidance

- Anagha Joshi, 'Model Provisions to Combat the Financing of the Proliferation of Weapons of Mass Destruction: Second Edition', Supplementary material for Guidance Paper, RUSI, October 2018.
- Andrea Berger and Anagha Joshi, 'Countering Proliferation Finance: Implementation Guide and Model Law for Governments', RUSI Guidance Paper, July 2017.

About the Authors

David Carlisle is a RUSI Associate Fellow who has produced papers on cryptocurrency-related risks and policy responses. He is the Head of Community at Elliptic, a London-based blockchain forensics firm, and has over a decade of experience in financial crime-related compliance and policy roles.

David's previous roles included service at the US Department of the Treasury's Office of Terrorism and Financial Intelligence. This included work in the Treasury's Office of Foreign Assets Control, where he was involved in the design and implementation of US financial and economic sanctions programmes involving countries such as North Korea and Iran. In subsequent roles, David advised senior Treasury officials on a wide range of topics related to sanctions, money laundering and terrorist financing, and acted as a liaison for the Treasury when engaging governments in the Asia-Pacific region on these topics.

Kayla Izenman is a Research Analyst at RUSI's Centre for Financial Crime and Security Studies. She joined RUSI in September 2018 following the completion of her Bachelor's degree in International Relations at Boston University, with a concentration in foreign policy and security studies. Her thesis focused on the threat posed by terrorist use of cryptocurrencies, and possible US national security responses.

Prior to joining RUSI, Kayla interned at both the US Department of Commerce and the US Department of State. She also interned at the DC-based think tank Foundation for Defense of Democracies within their Center for Sanctions and Illicit Finance, giving her a unique view of financial crime from both a governmental and non-governmental standpoint. Her work primarily looks at the intersection of financial technology and national security, as well as the changing landscape of terrorist finance.