National Proliferation Financing
Risk Assessment

February 2022

Department of the Treasury

National Proliferation Financing

Risk Assessment

Table of Contents

Executive Summary

Since the 2018 National Proliferation Financing Risk Assessment (NPFRA), the United States has seen continued efforts by proliferation financing (PF) networks to exploit the U.S. financial system to raise and move revenue and procure goods for their weapons of mass destruction (WMD) programs. Based on a review of the relevant data since 2018, the following trends have marked the PF context for the United States:

- The size of the U.S. financial system, the centrality of the U.S. dollar in the payment infrastructure supporting global trade, and the role of U.S. manufacturers in the production of proliferation-related technology (including dual-use items) continue to make the United States a target of exploitation by PF networks.
- The Democratic People's Republic of Korea (DPRK), followed by Iran, continues to pose the most significant PF threats for the United States, and the United States has prioritized preventing PF networks linked to those governments from exploiting the U.S. financial system. Since the 2018 NPFRA, China and, to a lesser extent, Russia continue to engage in PF activities by expanding their efforts to acquire U.S.-origin goods in violation of relevant export control laws.
- This period saw continued illicit use of correspondent banking relationships in PF efforts, with PF networks creating multiple front and shell companies to conduct their trade. The maritime sector continues to see significant revenue-generating activity by proliferating states in violation of international and U.S. law, including illicit natural resources trade conducted through ship-to-ship transfers. Additionally, PF networks are increasingly exploiting the digital economy, including by engaging in the systematic mining and trading of virtual assets and the hacking of virtual asset service providers (VASPs). The DPRK's capacity and willingness to engage in increasingly sophisticated malicious cyber activity, against both traditional financial institutions, such as central banks and private firms, and the virtual assets sector, have grown considerably since 2018. As described below, all this activity carries risks for the U.S. financial system.
- The COVID-19 pandemic offers new context for thinking about WMD proliferation risks. The pandemic has focused global attention on biological threats, whether naturally occurring, accidental, or deliberate. The disruption of economic activity linked to COVID-19 quarantine procedures affected the ability of proliferating states to engage in illicit trade, though those impacts were of a short-term nature. This disruption was particularly pronounced for the DPRK, which sealed its land border with China in January 2020. However, based on available evidence, some activity did continue, particularly through illicit ship-to-ship transfers. While these disruptions had economic and humanitarian consequences, they have not significantly affected the DPRK's ability to develop and test ballistic missile capabilities.

The 2022 NPFRA informs the context for the forthcoming 2022 National Strategy for Combating Terrorist and Other Illicit Financing (2022 Strategy), which will discuss how to further strengthen the U.S. anti-money laundering (AML), countering the financing of terrorism (CFT), and countering proliferation financing (CPF) (AML/CFT/CPF) regime.

INTRODUCTION

The 2022 NPFRA builds on the 2018 NPFRA,[1] identifying, discussing, and assessing the risks the United States faces from the financing of the proliferation of WMD and their delivery systems.[2] It also outlines how the U.S. CPF regime mitigates those risks and offers initial conclusions as to how the regime may be improved to address any residual risk and anticipate emerging threats. Published concurrently with the 2022 National Money Laundering Risk Assessment (NMLRA) and the 2022 National Terrorist Financing Risk Assessment (NTFRA),[3] these documents provide an overview of the most significant illicit finance risks facing the United States. All three documents inform the forthcoming 2022 Strategy, which will more fully discuss mitigation that could strengthen the U.S. AML/CFT/CPF regime.[4]

Preventing the proliferation of WMD and their delivery systems is a critical national security priority for the United States.[5] The current COVID-19 pandemic underscores the critical societal and economic disruptions that can arise from the spread of a deadly novel pathogen. This assessment is focused on the measures taken to assess and mitigate the underlying financing that enables the threat actors described below to begin or continue to acquire goods and technology or engage in revenue-raising activity that, in whole or in part, supports a WMD program.[6] These activities often have a nexus to the United States (especially the U.S. private sector) because of the size and global reach of the U.S. financial system and the attractiveness of certain U.S.-origin goods, technology, and knowledge as inputs for a WMD program. Given the national security implications of PF, the U.S. government uses a combination of laws, regulations, and other mechanisms to (1) track and control WMD components and related materials and (2) prevent proliferation networks from accessing U.S. banks and other financial services providers or purchasing proliferation-related components from U.S. manufacturers.[7] These include Executive Order (E.O.) 13382, a globally applicable nonproliferation financial sanctions authority, as well as country-specific sanctions authorities focused on the DPRK, Iran, Syria, and Russia. U.S. authorities can and have imposed civil and criminal penalties for violations of these restrictions.

A variety of obligatory measures, including AML/CFT/CPF, export control, and sanctions compliance measures, assist the U.S. private sector in implementing a risk-based approach to preventing PF. To that end, the United

1 The 2018 NPFRA is available at https://home.treasury.gov/system/files/136/2018npfra_12_18.pdf.

2 Unless otherwise noted, all references to weapons of mass destruction or WMD programs are inclusive of the research, development, and deployment of delivery systems, including ballistic missiles and unmanned aerial vehicles (UAVs). The definition of WMD encompasses chemical, biological, radiological, and nuclear weapons.

3 [Links forthcoming]. Readers are strongly encouraged to consult all three documents, as there are threats, vulnerabilities, and methodologies that cut across money laundering (ML), terrorist financing (TF), and proliferation financing (PF). The 2022 Strategy will identify key vulnerabilities and highlight additional steps to close legal and regulatory loopholes in the U.S. AML/CFT framework.

4 The National Strategy to Combat Terrorist and Other Illicit Financing is published pursuant to Sections 261 and 262 of the Countering America's Adversaries Through Sanctions Act, Pub. L. No.115-44 (2017).

5 In June 2021, the Financial Crimes Enforcement Network (FinCEN)—which is the primary administrator and regulator of U.S. AML/CFT laws, including the Bank Secrecy Act (BSA)—published the first national AML/CFT priorities, which identified PF as one of eight priorities. Department of the Treasury, Financial Crimes Enforcement Network, *Anti-Money Laundering and Countering the Financing of Terrorism National Priorities*, p. 11 (Jun. 30, 2021), https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf.

6 As the 2018 NPFRA explained, while the United States works globally to counter proliferation threats, including the underlying financing of such threats, this assessment focuses on how such financing touches the U.S. financial system.

7 "Proliferation-related components" can apply to a wide variety of goods and technology, including goods considered "dual-use" under relevant export control regimes (i.e., goods that have civilian and military uses). These goods also include unlisted goods that would still be subject to "catch-all" requirements because their end-use involves WMD or other military applications.

States prioritizes engagement with the private sector through guidance (public and private) and public-private information-sharing mechanisms.[8] Finally, the United States recognizes that PF networks operate across multiple jurisdictions and actively seeks to work with allied and other partner countries, including through various formal and informal multilateral forums, to build a stronger global CPF regime. For example, during its Presidency of the Financial Action Task Force (FATF), the global standard setter for AML/CFT/CPF, in 2018-2019, the United States supported the adoption of important updates to the FATF Standards and new guidance for jurisdictions and their private sectors on PF risk assessment and mitigation.[9]

PARTICIPANTS

In drafting this assessment, the Department of the Treasury's Office of Terrorist Financing and Financial Crimes (TFFC) consulted with staff from the following U.S. government agencies, who also reviewed this report:

- **Department of Commerce**
  - Bureau of Industry and Security (BIS)
- **Department of Defense**
  - Office of the Under Secretary of Defense for Policy
- **Department of Homeland Security**
  - Countering Weapons of Mass Destruction/Strategy, Plans & Policy
  - Homeland Security Investigations
- **Department of Justice**
  - Criminal Division
  - Federal Bureau of Investigation
  - National Security Division
- **Department of State**
  - Bureau of International Security and Nonproliferation
- **Department of the Treasury**
  - Office of Terrorism and Financial Intelligence (TFI)
    - Financial Crimes Enforcement Network (FinCEN)
    - Office of Foreign Assets Control (OFAC)
    - Office of Intelligence and Analysis (OIA)
    - Office of Terrorist Financing and Financial Crimes
- **Staff of the federal functional regulators[10]**

8 These include the Bank Secrecy Act Advisory Group (BSAAG) and the information-sharing provisions of Sections 314(a) and 314(b) of the USA PATRIOT Act, administered by FinCEN. The FATF PF Risk Assessment Guidance outlines the usefulness of such mechanisms, including the extent to which public sectors can provide relevant private sector entities with typologies, sanctions evasion indicators, and best practices for compliance. Financial Action Task Force, *Guidance on Proliferation Financing Risk Assessment and Mitigation*, p. 36 (Jun. 2021) (FATF PF Risk Assessment Guidance), http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf.

9 Financial Action Task Force, *Objectives for FATF -XXX (2018-2019), Paper by the Incoming President: United States Presidency Priorities for the Financial Action Task Force (FATF)*, (n.d.), https://www.fatf-gafi.org/publications/fatfgeneral/documents/objectives-2018-2019.html; FATF PF Risk Assessment Guidance.

10 This includes staff of the Commodity Futures Trading Commission (CFTC), the Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System (FRB), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Securities and Exchange Commission (SEC).

SCOPE AND DEFINITION

In June 2021, the FATF published non-binding guidance to assist jurisdictions and their private sectors in conducting national or institutional risk assessments (FATF PF Risk Assessment Guidance).[11] The guidance highlights the important methodology, information gathering, and coordination considerations that should inform the assessment process. The 2022 NPFRA recognizes the utility of the FATF PF Risk Assessment Guidance and seeks to incorporate those suggested best practices, while acknowledging there is no one-size-fits-all approach to conducting a risk assessment.[12] U.S. financial institutions and other U.S. businesses are generally already assessing and mitigating sanctions evasion risk related to the DPRK and Iran given the domestic AML/CFT framework described above, which is in line with recent amendments to the FATF Standards.

To establish a baseline for a comprehensive CPF regime, the United States uses the FATF's definition from its 2021 PF Risk Assessment Guidance:

> The financing of proliferation refers to the risk of raising, moving, or making available funds, other assets or economic resources, or financing, in whole or in part, to persons or entities for purposes of WMD proliferation, including the proliferation of their means of delivery or related material (including both dual-use technologies and dual-use goods for non-legitimate purposes).[13]

Proliferation Finance and the U.S. Nexus

The threat to the United States from proliferation networks arises from two factors particular to the U.S. national context: the role of the U.S. dollar for a variety of cross-border financial activities and the sophistication of U.S.-origin proliferation technology (including dual-use items). According to the Bank for International Settlements, the U.S. dollar share of cross-border loans, international debt securities, foreign exchange transactions volume, official foreign exchange reserves, trade invoicing, and Society for Worldwide Interbank Financial Telecommunication (SWIFT) payments each exceed 40 percent or more of the global total based on an analysis of 2019 and 2020 data.[14] While this provides the United States with significant economic advantages, it also means that proliferation-related financial activity is likely to touch the United States at some point, often through correspondent banking relationships that allow foreign banks access to dollar-denominated financial services.

The second factor is that PF networks acquire or attempt to acquire specific goods for WMD programs, some of which, depending on the specific needs of the proliferator, are of U.S. origin and subject to the U.S. export control regime.[15] The sophistication of the U.S. technology sector, particularly for goods with potential military applications, makes it, along with the technology sector in Western Europe, a priority source of components for countries who wish to build WMD capability if they lack the ability to develop these components themselves.

---

11 FATF PF Risk Assessment Guidance, pp. 10-12.

12 For this reason, private sector entities are encouraged to consult any published risk assessments in the jurisdictions in which they are operating to understand the risk factors unique to that country and its financial system. Supervisors in these jurisdictions may also have published or communicated sectoral risk assessments that would be important for private sector firms to consult.

13 FATF PF Risk Assessment Guidance, p. 8, footnote 7.

14 This trend showed no signs of abating during the COVID-19 pandemic, as the economic dislocations from global lockdowns led to an increased demand for U.S. dollar-denominated assets, long considered a safe haven in times of macroeconomic turbulence. See Bank for International Settlements, Committee on the Global Financial System, *U.S. dollar funding: an international perspective*, Report prepared by a Working Group chaired by Sally Davies (Board of Governors of the Federal Reserve System) and Christopher Kent (Reserve Bank of Australia) (Jun. 2020), https://www.bis.org/publ/cgfs65.pdf.

15 For this reason, summaries of export control violations and related prosecutions are an important source of information about PF typologies. See, for example, Department of Justice, "Summary of Major U.S. Export Enforcement, Economic Espionage, and Sanctions-Related Criminal Cases, (January 2016 to the present: updated November 2019)," (Nov. 2019), https://www.justice.gov/nsd/page/file/1044446/download; Department of Commerce, Bureau of Industry and Security, *Annual Report to Congress for Fiscal Year 2020*, https://www.bis.doc.gov/index.php/documents/pdfs/2711-2020-bis-annual-report-final/file.

METHODOLOGY

The 2022 NPFRA follows the 2018 NPFRA in its methodology, while also considering the 2021 FATF PF Risk Assessment Guidance. While the threat, vulnerability, and consequence discussion in the 2021 FATF PF Risk Assessment Guidance is predominantly presented in the context of United Nations (UN) targeted financial sanctions, the general themes are relevant to any country, including the United States, that seeks to take a broader view of PF risk.

For the NPFRA, risk is a function of the following:

- **Threat:** A threat refers to individuals or entities, or activity undertaken by those individuals and entities, with the potential to cause a defined harm. The threats, which may include nation-state authorities, those acting under their control or on their behalf, or those wittingly or unwittingly supporting either, are the ones who exploit the U.S. financial system to move funds, assets, or other economic resources that could be used to (1) directly acquire WMDs or their delivery systems or the goods, technology, or know-how to allow them to build WMDs or their delivery systems or (2) support a WMD program through a variety of revenue-raising activities, which are often done to evade the prohibitions of U.S. or multilateral sanctions.
- **Vulnerability:** To acquire or expand their WMD capabilities, threat actors must exploit aspects of a jurisdiction or private sector entity to obtain components or financial services they would otherwise be prohibited from acquiring. These vulnerabilities may arise from weaknesses or loopholes in national laws or regulations, effectiveness issues handicapping the ability of national authorities to properly investigate or disrupt proliferation networks, or unique circumstances that make a particular jurisdiction especially vulnerable to this kind of activity.
- **Consequence:** A consequence derives directly from a threat capitalizing on a vulnerability. In the context of PF, the consequence would be the harms inflicted on U.S. citizens, the U.S. economy, and U.S. national security interests if funds, assets, or other economic resources are being made available to a proliferation network are such that it can be used to acquire or augment a specific WMD capability. As stated in the 2018 NPFRA, it is generally impossible to distinguish the relative consequence of a given individual act of procurement from general activities meant to support a WMD program. Therefore, for the purposes of this assessment, we will place greater focus on analyzing threats and vulnerabilities as the most clearly distinguishable characteristics of PF risk.
- **Risk is a function of threat, vulnerability, and consequence.** It represents a summary judgment, taking into consideration the effect of mitigating measures including regulation, supervision, and enforcement.

The 2022 NPFRA is based on a review of a variety of public and private sector publications, government data,[16] and analyses. Data collected are current as of December 31, 2021.[17] These sources include the following:

- A review of relevant Bank Secrecy Act (BSA) data collected by FinCEN that was potentially indicative of proliferation or sanctions evasion activity as seen by U.S. financial institutions;
- U.S. sanctions designations and enforcement actions related to WMD activity (including evasion by proliferating entities or states), as well as relevant source material that supported the designations;
- Export control violation cases, particularly where a financing element related to WMD was present or the item being procured was identified as being controlled for WMD or military end-use or end-user reasons;

16 As with the 2018 NPFRA, the authors consulted classified sources of information to verify conclusions reached through a consultation of information available in the public domain.

17 With respect to information collected from pending cases, the charges contained in an indictment are merely allegations. A defendant is presumed innocent unless, and until, proven guilty beyond a reasonable doubt in a court of law. A seizure warrant is merely an allegation. A defendant is presumed innocent until, and unless, proven guilty, and the burden to prove forfeitability in a civil forfeiture proceeding is upon the government.

- Publicly available law enforcement documentation relating to criminal cases arising from WMD procurement or sanctions evasion, including prosecutions of money laundering cases where the specified unlawful activity was a violation of the International Emergency Economics Powers Act (IEEPA) and related regulations or relevant export control laws;
- Civil and criminal asset forfeiture complaints related to property that had an alleged connection to WMD procurement or sanctions evasion; and
- Reports and analyses prepared by international organizations, including the UN and the FATF, think tanks, academic and research organizations, and media reporting.

SECTION I. THREATS

The starting point for an analysis of the PF risks facing the United States requires identifying the WMD proliferation threats to the United States. State-sponsored proliferation programs continue to pose the most significant PF threat to the United States. These programs can leverage significant technical expertise to design and execute clandestine procurement and fundraising strategies at scale, even if those countries are subject to comprehensive multilateral sanctions or export controls. While the United States remains concerned about the ability of non-state actors to obtain WMD capabilities, more recent cases, such as the Islamic State of Iraq and Syria's (ISIS's) chemical weapons efforts, involve non-state actors using chemical weapons or precursor chemicals found on the battlefield or developing rudimentary capabilities from industrial products. These efforts have not involved the exploitation of the U.S. financial system or the acquisition of U.S.-origin goods in the same way that most state-sponsored or affiliated actors have done.[18]

State-sponsored or affiliated actors may include those pursuing nuclear capabilities outside of the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) or countries within the treaty illegally procuring U.S-origin goods, technologies, or knowledge to augment their capabilities contrary to U.S. foreign policy. As discussed in the Vulnerabilities and Risks section below, these states often need to access the U.S. financial system in some way. For example, they may seek to procure specific U.S.-origin goods needed for their WMD programs, which often involves U.S. dollar transactions with U.S.-based businesses or transacting in U.S. dollars as part of revenue-generating sanctions evasion schemes.

PF networks use a variety of methods to obscure links between their procurement and fundraising activities and the entities on whose behalf or under whose control they are operating, many of whom are subject to sanctions or other measures, such as export controls, designed to prevent WMD proliferation. These methods include the use of front and shell companies, trade-based money laundering, and the illicit diversion of physical goods.

The following section provides an overview of the threats posed by each of these actors, including financing methodologies that are the hallmarks of their proliferation networks.

DPRK

The DPRK constitutes the most complex PF threat globally and to the United States specifically. It continues to operate sophisticated sanctions evasion schemes to raise revenue, which contributes directly to advancing its nuclear and ballistic missile capabilities.[19] According to analyses by the UN and the United States, all organs of the DPRK prioritize these activities, from intelligence agencies operating sophisticated cyber hacking capabilities targeting private companies and governments alike to DPRK diplomats using their legal presence in third countries to act as overseas banking representatives and revenue generators for the regime.

According to the 2021 Annual Threat Assessment of the U.S. Intelligence Community, "North Korea will be a WMD threat for the foreseeable future, because Kim [Jong-un] remains strongly committed to the country's nuclear weapons, the country is actively engaged in ballistic missile research and development, and Pyongyang's CBW

18 According to independent analysis published by the Combating Terrorism Center at the United States Military Academy at West Point, "there is no evidence in the pattern of the Islamic State's recorded use of chemical agents to suggest that the group acquired anything beyond rudimentary precursor chemicals." See Columb Strack, "The Evolution of the Islamic State's Chemical Weapons Efforts," CTC Sentinel, 10:9 (Oct. 2017), https://www.ctc.usma.edu/the-evolution-of-the-islamic-states-chemical-weapons-efforts/.

19 As cited in the 2018 NPFRA, credible reports posit that the vast majority of foreign currency earnings is budgeted for military expenditures in the DPRK. 2018 NPFRA, p. 11.

[chemical and biological warfare] efforts persist."[20] DPRK leader Kim Jong-un has declared that his country would never give up its nuclear weapons so long as the United States maintains its "hostile policy" and that "the development of nuclear weapons be pushed forward without interruption."[21] The reach of DPRK PF activity is global, but as previously referenced, it most often indirectly implicates the U.S. financial system through U.S. financial institutions' correspondent banking relationships with foreign financial institutions that hold accounts of entities linked to the DPRK, or through commercial transactions where U.S. manufacturers ultimately export to entities linked to the DPRK.

The UN Panel of Experts' reporting from 2021 confirms that the DPRK remains committed to using international banking connections to further its WMD development. The September 2021 report concluded that the DPRK had seen "no appreciable decline" in its access to global financial institutions.[22] This conclusion echoed findings from the March 2021 report of the UN Panel of Experts that "the Democratic People's Republic of Korea continues to access international financial systems […] The illicit revenue generated from sanctions evasion activities and laundered through these networks both directly and indirectly supports the country's WMD and ballistic missile programs."[23]

Methods and Patterns Common to DPRK PF Activity

Since the publication of the 2018 NPFRA, the U.S. Departments of Justice, State, and the Treasury have used diplomatic tools and asset forfeiture, sanctions, and other legal authorities to disrupt these networks (see illustrative examples in the Vulnerabilities and Risks section). Interagency partners have supported broader multilateral efforts to raise awareness about DPRK-linked proliferation networks, including for financial institutions, companies operating in the shipping sector (including freight forwarding and insurance), and manufacturers of WMD components.[24] For example, in September 2020, the Departments of State, the Treasury, and Commerce published the North Korea Ballistic Missile Procurement Advisory, highlighting the deceptive techniques that are the hallmarks of Pyongyang's PF schemes.[25] While this advisory is focused on one aspect of the DPRK's weapons program, the tactics are found across its wider procurement and sanctions evasion schemes.[26]

---

20 Office of the Director of National Intelligence, Annual Threat Assessment of the U.S. Intelligence Community, p. 15, (Apr. 9, 2021, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf) (ODNI Threat Assessment).

21 Joshua Berlinger and Yoonjung Seo, "Kim Jong Un says North Korea is developing tactical nukes, new warheads and a nuclear-powered submarine," CNN.com, (Jan. 9, 2021), https://www.cnn.com/2021/01/09/asia/north-korea-nuclear-development-intl-hnk/index.html.

22 1718 Sanctions Committee (DPRK) Panel of Experts, *September 2021 Panel of Experts Report*, p. 46, (Sep. 2021), https://undocs.org/S/2021/777.

23 1718 Sanctions Committee (DPRK) Panel of Experts, *Final Report of the Panel of Experts submitted pursuant to resolution 2511 (2020)*, p. 51, (Mar. 2021), https://undocs.org/S/2021/211. The FATF PF Risk Assessment Guidance also stresses DPRK-linked activity, and the bibliography lists previous UN Panel of Experts reports that comprehensively document DPRK activities as important sources for jurisdictions and relevant private sector entities to understand these activities.

24 For examples of recent guidance, see Department of State, Department of the Treasury, Department of Commerce, *North Korea Ballistic Missile Procurement Advisory*, (Sep. 1, 2020) (North Korea Ballistic Missile Procurement Advisory), 20200901_nk_ballistic_missile_advisory.pdf (treasury.gov) and the Department of the Treasury, Department of State, and Coast Guard, *Sanctions Advisory for the Maritime Industry, Energy and Metals Sectors, and Related Communities: Guidance to Address Illicit Shipping and Sanctions Evasion Practices,* (May 14, 2020), https://home.treasury.gov/system/files/126/05142020_global_advisory_v1.pdf.

25 See North Korea Ballistic Missile Procurement Advisory. In addition, see FinCEN's 2017 advisory on how DPRK-linked actors access the international financial system: Department of the Treasury Financial Crimes Enforcement Network, "FinCEN Advisory on North Korea's Use of the International Financial System," (Nov. 2, 2017), https://www.fincen.gov/sites/default/files/advisory/2017-11-02/DPRK Advisory FINAL 508 C.pdf.

26 See, for example, the January 2022 designations of Chinese and Russian individuals and entities for DPRK-linked procurement. Department of the Treasury, Office of Foreign Assets Control, "Treasury Targets Democratic People's Republic

These methods include the following:

- Extensive overseas networks of agents, including DPRK diplomats, who can arrange transactions on behalf of the government;
- Use of third-country nationals and companies, many of whom wittingly participate in these schemes or have compliance failures that allow exploitation by DPRK proliferation networks;[27]
- Obscuring the end-user of their purchases through mislabeling goods or consolidating and repackaging shipments for ultimate delivery to the DPRK, with China remaining a commonly used location for transshipment across its land border or via ship-to-ship transfer;[28] and
- Procuring goods that are not listed on relevant export control lists but would otherwise be subject to "catch-all" controls.

The DPRK's malicious cyber activities are an important source of revenue generation for its military budget. In April 2020, the Departments of State, the Treasury, Homeland Security, and Justice published a DPRK Cyber Threat Advisory[29] which highlighted the DPRK's malicious cyber activities and how the DPRK has targeted financial institutions and other private sector actors to fulfill foreign policy ends. These include (1) disrupting critical infrastructure, (2) targeting those critical of the regime, (3) engaging in cyber-enabled financial theft and money laundering, and (4) compromising computers and network systems to generate virtual assets (a technique known as "cryptojacking"). DPRK state-sponsored cyber actors are subordinate to the Reconnaissance General Bureau (RGB), the DPRK's main intelligence agency and a UN- and U.S.-designated entity. In addition to providing regulatory guidance in line with the FATF Standards, this advisory highlights resources for financial institutions to better understand the technical exploits and threats used by the DPRK. The DPRK's cyber efforts and exploitation of the maritime sector are discussed more in depth in the Vulnerabilities and Risks section.[30]

Iran

The United States remains concerned that Iran still seeks WMD capabilities that would further threaten regional stability in the Middle East.[31] The Biden-Harris Administration's commitment to pursuing a return to mutual compliance with the Joint Comprehensive Plan of Action (JCPOA), also known as the Iran nuclear deal, does not diminish the focus on proliferation-related activity of Iranian entities and individuals. The United States also prioritized these efforts while it was still a participant in the JCPOA.

The proliferation threat from Iran is most acutely underscored by Tehran's potential nuclear "breakout capacity,"

---

of Korea Individuals Supporting Weapons of Mass Destruction and Ballistic Missile Programs," (Jan. 12, 2022), https://home.treasury.gov/news/press-releases/jy0555.

27 To cite one example from the September 2021 U.N. Panel of Experts report, many jurisdictions with corporate registry services do not adopt sufficient due diligence practices to collect and verify ultimate beneficial ownership information. This includes cases where unaffiliated individuals were registered as ultimate beneficial owners (UBOs) of corporate entities without their knowledge. 1718 Committee Panel of Experts, September 2021 Report, pp. 46-47.

28 UN reporting indicated that the COVID-19 pandemic severely limited cross-border trade between China and the DPRK, 1718 Committee Panel of Experts, March 2020 report, p. 4.

29 Department of State, Department of the Treasury, Department of Homeland Security, and Department of Justice, *Guidance on the North Korean Cyber Threat*, (Apr. 15, 2020), https://home.treasury.gov/system/files/126/dprk_cyber_threat_advisory_20200415.pdf.

30 Department of State, Department of the Treasury, and U.S. Coast Guard, "North Korea Sanctions Advisory: Updated Guidance on Addressing North Korea's Illicit Shipping Practices," (Mar. 21, 2019), https://home.treasury.gov/system/files/126/dprk_vessel_advisory_03212019.pdf.

31 President Joseph R. Biden, Jr., *Interim National Security Strategic Guidance*, p. 8, (Mar. 2021), https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

marked by enrichment of weapons-grade uranium, married with significant ballistic missile capabilities.[32] Since the United States ceased participation in the JCPOA in 2018, Iran has tested the limits of the nuclear deal, pressuring the remaining participants to provide tangible economic benefits in order for Iran not to engage in further violations.[33] Perceptions of increasing international hostility to Iran, the influence of the Islamic Revolutionary Guard Corps (IRGC), a designated WMD proliferator,[34] and domestic hardliners, including Iran's new president, have also contributed to the rationale for an expanded Iranian enrichment program.

An integral part of monitoring these developments is investigating the extent to which Iran continues to engage in sanctions evasion schemes to raise revenue and procure goods for these military capabilities.[35] Iranian entities continue to engage in illicit oil exports to raise revenue, some of which may contribute to spending on augmenting the country's military capabilities.[36] This spending derives from significant and complex schemes U.S. law enforcement attributes to the IRGC. For example, the United States filed a forfeiture complaint in February 2021, alleging that all oil aboard a Liberian-flagged vessel, the motor tanker (M/T) *Achilleas*, was subject to forfeiture based on U.S. terrorism forfeiture laws. The complaint alleged a scheme involving multiple entities affiliated with Iran's IRGC and the IRGC-Qods Force (IRGC-QF) to ship Iranian oil to a customer abroad covertly. The documents alleged that profits from oil sales support the IRGC's full range of nefarious activities, including the proliferation of WMD, support for terrorism, and a variety of human rights abuses, at home and abroad.[37]

Iran's exploitation of the maritime sector is a priority concern.[38] In September 2019, OFAC, which administers and enforces U.S. economic and trade sanctions programs, published a shipping advisory that highlighted the risk that those transacting with the Iranian shipping or petroleum sectors may ultimately be providing support to the IRGC, noting specifically the IRGC's involvement in terrorism and WMD proliferation.[39] In May 2020, the Departments of the Treasury and State and the United States Coast Guard released a Sanctions Advisory for the Maritime Industry, Energy, and Metals Sectors, and Related Communities,[40] which provided the industry with advice on preventing illicit finance threats in key sectors, including the shipping sector.

The United States continues to enforce relevant prohibitions to disrupt Iranian illicit financial activity. For

32 "Breakout capacity" generally refers to the timeline for Iran to produce a useable nuclear weapon, commencing with a political decision to do so and including sufficient time to produce enough weapons-grade enriched uranium and to complete technical steps for testing a device. U.S. officials have assessed the estimated timeline for Iran to do so at numerous points since the 1990s. For a summary of those estimates, see Paul K. Kerr, "Iran's Nuclear Program: Status," Congressional Research Service, (Updated Dec. 20, 2019), https://crsreports.congress.gov/product/pdf/RL/RL34544.

33 Russia, China, the United Kingdom, France, and Germany.

34 To the extent that the IRGC is among those entities responsible for Iran's ballistic missile development, its ability to use the U.S. financial system is a critical risk for the United States.

35 The United States remains concerned about Iranian developments of drone and precision missile strike capabilities.

36 For an overview of the link between Iran's oil export revenue and defense spending, see Defense Intelligence Agency, *Iran Military Power: Ensuring Regime Survival and Securing Regional Dominance*, (2019) https://www.dia.mil/Portals/110/Images/News/Military_Powers_Publications/Iran_Military_Power_LR.pdf, pp. 18.

37 Department of Justice, "Complaint Seeks Forfeiture of Iranian Oil Aboard Tanker Based on Connection to Terror Group," (Feb. 3, 2021), https://www.justice.gov/opa/pr/complaint-seeks-forfeiture-iranian-oil-aboard-tanker-based-connection-terror-group. For a copy of the complaint, see: https://www.justice.gov/opa/press-release/file/1364021/download.

38 See, for example, the June 2020 updated designations of dozens of Iranian vessels under counter-WMD authorities for their association with IRISL. Department of the Treasury, Office of Foreign Assets Control, "Non-Proliferation Designations; Iran-related Designations Updates," (Jun. 8, 2020), https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20200608.

39 Department of the Treasury, Office of Foreign Assets Control, *OFAC Advisory to the Maritime Petroleum Shipping Community: Sanctions Risk Related to Shipping Petroleum and Petroleum Products from Iran*, (Sep. 4, 2019), https://home.treasury.gov/system/files/126/iran_advisory_09032019.pdf.

40 Sanctions Advisory for the Maritime Industry.

instance, most recently, in July 2021, the Department of Commerce added four individuals and companies located in Lebanon and Iran to the Entity List[41] for their involvement in the export of U.S.-origin goods to Iran without obtaining the appropriate licenses.[42] Since the 2018 NPFRA, the Departments of State and the Treasury have also imposed sanctions on dozens of entities with links to Iran's uranium enrichment or ballistic missile development activities. On September 21, 2020, the Departments of State, the Treasury, and Commerce announced the widest-ranging set of sanctions and export control restrictions on Iran's nuclear, missile, and conventional arms activities, including the designation of 31 individuals and entities pursuant to E.O.s 13382 and 13949.[43] In November 2020, OFAC targeted a network of companies that supported an Iranian military firm subordinate to Iran's Ministry of Defense and Armed Forces Logistics.[44] The companies had sought electronic components with military applications from China and the United Arab Emirates (UAE), including goods that were of U.S. origin. In a December 2020 action, OFAC designated an Iranian entity, the Shahid Meisami Group, and its director for conducting chemical weapons research, including testing and production of chemical agents, on behalf of Iran's conventional military.[45] Many of these designations targeted geographically disperse procurement networks, which will be highlighted more in depth in the Vulnerabilities and Risks section.[46]

China & Russia

Since 2018, the United States has significantly increased its scrutiny of technological developments undertaken by China and Russia. This focus includes the blending of military and civilian research spheres and military modernization efforts that may use U.S.-origin inputs. China's Military Civil Fusion is a national strategy to augment its military capabilities by eliminating the barriers between China's civilian research and development efforts and those of its military and defense industrial sectors.[47] Russia similarly has prioritized military

41 Pursuant to Section 744.11(b) of the Export Administration Regulations (EAR), the Entity List identifies persons or organizations reasonably believed to be involved, or to pose a significant risk of being or becoming involved, in activities contrary to the national security or foreign policy interests of the United States. The EAR imposes additional license requirements on, and limits the availability of most license exceptions for, exports, re-exports, and transfers (in-country) to listed entities. For the most significant actors engaged in these activities, the Department of Commerce may set out a license review policy that includes a "presumption of denial" or, less severely, a review on a case-by-case basis for specific categories of goods.

42 Department of Commerce, Bureau of Industry and Security, "Commerce Department Adds 34 Entities to the Entity List to Target Enablers of China's Human Rights Abuses and Military Modernization, and Unauthorized Iranian and Russian Procurement," (Jul. 9, 2021), https://www.commerce.gov/news/press-releases/2021/07/commerce-department-adds-34-entities-entity-list-target-enablers-chinas. The Federal Register notice is available at https://www.federalregister.gov/documents/2021/07/12/2021-14656/addition-of-certain-entities-to-the-entity-list-revision-of-existing-entry-on-the-entity-list.

43 Department of the Treasury, Office of Foreign Assets Control, "Treasury Sanctions Key Actors in Iran's Nuclear and Ballistic Missile Programs," (Sep. 21, 2020), https://home.treasury.gov/news/press-releases/sm1130.

44 Department of the Treasury, Office of Foreign Assets Control, "Treasury Sanctions Procurement Network Supplying Iranian Military Firm," (Nov. 10, 2020), https://home.treasury.gov/news/press-releases/sm1180.

45 Department of the Treasury, Office of Foreign Assets Control, "Treasury Designates Entity Subordinate to Iran's Military Firm," (Dec. 3, 2020), https://home.treasury.gov/news/press-releases/sm1200.

46 See, for example, Department of the Treasury, Office of Foreign Assets Control, "Treasury Sanctions Global Iranian Nuclear Enrichment Network," (Jul. 18, 2019), https://home.treasury.gov/news/press-releases/sm736; Department of the Treasury, Office of Foreign Assets Control, "Treasury Targets Procurement Network Supporting Iran's Missile Proliferation Programs," (Aug. 28, 2019), https://home.treasury.gov/news/press-releases/sm759; and Department of the Treasury, Office of Foreign Assets Control, "Treasury Sanctions Procurement Network Supplying Iranian Military Firm," (Nov. 10, 2020), https://home.treasury.gov/news/press-releases/sm1180.

47 Department of State, "Military-Civil Fusion and the People's Republic of China," (n.d.), https://www.state.gov/wp-content/uploads/2020/05/What-is-MCF-One-Pager.pdf.

modernization to counter perceived U.S. superiority in both conventional and nuclear weapons.[48] The 2018 NPFRA summarized the threat from Chinese and Russian PF as

> largely limited to procurement-based schemes designed to acquire sensitive goods and technologies, rather than sanctions-evasion schemes necessary to finance and move funds on behalf of weapons programs in states that are already recognized nuclear weapons powers. Even on the procurement front, there are relatively few publicly reported cases of these threat actors seeking to exploit the United States to finance WMD-related programs, versus other types of industrial espionage or trafficking in goods with broader military applications.[49]

As described in the Vulnerabilities and Risks section, that pattern seems to be continuing. Chinese and Russian military modernization is being built partially through the illegal acquisition of U.S.-origin goods and technology. Unlike the DPRK and Iran, China and Russia are existing significant military powers and NPT nuclear weapons states with sophisticated indigenous production, research, and development capacities. They do not need to engage in the same revenue-generating activity that violates U.S. sanctions as the DPRK and Iran. China and Russia can largely produce WMD and delivery systems on their own but seek out certain U.S.-origin goods. The Vulnerabilities and Risks section highlights relevant examples where this activity implicates U.S. financial institutions or other private sector firms.

As part of U.S. scrutiny of these activities, in January 2021, the Department of Commerce announced new controls on U.S. technology and specific activities undertaken by U.S. persons that support military end-users in China, Cuba, Russia, and Venezuela, as well as those more generally supporting unauthorized WMD programs, including certain types of weapons delivery systems, production facilities, and maintenance, repair, or overhaul.[50]

China

Since the publication of the 2018 NPFRA, the U.S. government continues to take an all-tools approach to protecting U.S. national security from Chinese attempts to acquire U.S.-origin goods, technology, and expertise across a variety of economic sectors. The Department of the Treasury, as the gatekeeper for the U.S. financial system, seeks to promote a transparent financial system and open investment environment while protecting U.S. national security interests and countering the exploitation of our financial system and economy by strategic adversaries.

From a PF perspective, China represents a distinct threat as compared to Iran or the DPRK because it does not face a comprehensive U.S. embargo and remains among the United States' largest trading partners.[51] However, it is a near-peer U.S. competitor that has used instruments of its national power to acquire U.S.-origin goods or technology with important military applications, including, but not limited to, WMD.[52]

For the purposes of the NPFRA, cases are highlighted where the U.S. financial system may see a transaction chain linked to procurement of WMD-related goods that benefits China's military development, including drawing U.S. firms into violations of export controls.

---

48 ODNI Threat Assessment, p. 10.

49 NPFRA 2018, p. 27.

50 Department of Commerce, Bureau of Industry and Security, "Commerce Tightens Controls to Prevent Support of Foreign Military-Intelligence and WMD Activities," (Jan. 14, 2021), https://2017-2021.commerce.gov/news/press-releases/2021/01/commerce-tightens-controls-prevent-support-foreign-military.html.

51 Census Bureau, "Top Trading Partners – October 2021," https://www.census.gov/foreign-trade/statistics/highlights/toppartners.html.

52 According to the 2021 Annual Threat Assessment, p. 4, "China is increasingly a near-peer competitor, challenging the United States in multiple arenas—especially economically, militarily, and technologically—and is pushing to change global norms."

Russia

Russian procurement schemes exist to obtain specific components, including proliferation-sensitive items from U.S. manufacturers subject to export controls. In addition to sanctions designations imposed by the Departments of State and the Treasury, the Department of Commerce has also placed Russian and third-country firms supporting Russia's activities on the Entity List. In March 2021, the Department of Commerce added 14 parties from Russia, Germany, and Switzerland to the Entity List for their support of Russia's chemical weapons program.[53] It followed up on this action again in July 2021, adding Russian entities that were seeking U.S.-origin electronic components for likely use by Russia's military.[54] The Vulnerabilities and Risks section discusses how these threats use front companies, transshipment hubs, and other obfuscation methods.

Additionally, Russia's documented use of chemical weapons to target regime opponents is a concern. However, these activities do not present the same PF threat with respect to U.S. entities because the weapons do not require U.S.-origin inputs to develop and deploy, or exploitation of the U.S. financial system. Nonetheless, the United States has used multiple sanctions authorities, including those under the Chemical and Biological Weapons Control and Warfare Elimination Act of 1991 (CBW Act), to target Russian entities involved in these activities. Because Russia's willingness to erode international norms[55] surrounding the use of WMD has profound implications for the prospect of other countries building this capability, the United States has not hesitated to pursue targeted actions.[56]

Syria

As detailed in the 2018 NPFRA, the United States maintains a robust sanctions program against the Bashar al-Assad regime in Syria for its conduct in the Syrian civil war, including its well-documented use of chemical weapons, which stands in violation of longstanding global norms. In April 2021, the Conference of the States Parties to the Chemical Weapons Convention (CWC) adopted a decision to suspend Syria's voting rights at the Organisation for the Prohibition of Chemical Weapons (OPCW), the implementing body of the CWC, stemming from the Assad regime's possession and use of chemical weapons in violation of its obligations under the CWC.[57] This decision followed an April 2020 report of the OPCW's Investigation and Identification Team that there were "reasonable grounds" to determine the Assad regime used chlorine and sarin in three separate March 2017 attacks.[58]

---

53 Department of Commerce, Bureau of Industry and Security, "Department of Commerce Adds 14 Parties to the Entity List for Support of Russian Weapons of Mass Destruction Programs and Chemical Weapons Activities," (Mar. 2, 2021), https://www.commerce.gov/news/press-releases/2021/03/us-department-commerce-adds-14-parties-entity-list-support-russian.

54 Department of Commerce, Bureau of Industry and Security, "Commerce Department Adds 34 Entities to the Entity List to Target Enablers of China's Human Rights Abuses and Military Modernization, and Unauthorized Iranian and Russian Procurement," (Jul. 9, 2021), https://www.commerce.gov/news/press-releases/2021/07/commerce-department-adds-34-entities-entity-list-target-enablers-chinas.

55 With respect to the use of chemical weapons, the global norm originates with the Chemical Weapons Convention, the general obligations of which include that each State Party undertakes to not "develop, produce, otherwise acquire, stockpile or retain chemical weapons, or transfer, directly or indirectly, chemical weapons to anyone" and not to use chemical weapons. Organisation for the Prohibition of Chemical Weapons, Article I: General Obligations, (n.d.), https://www.opcw.org/chemical-weapons-convention/articles/article-i.

56 Department of the Treasury, Office of Foreign Assets Control, "Treasury Sanctions Russian Operatives and Entities Linked to the Poisoning of Aleksey Navalny, Chemical Weapons Program," (Aug. 20, 2021), https://home.treasury.gov/news/press-releases/jy0328.

57 Organisation for the Prohibition of Chemical Weapons, "Conference of the States Parties adopts Decision to suspend certain rights and privileges of the Syrian Arab Republic under the CWC," (Apr. 22, 2021), https://www.opcw.org/media-centre/news/2021/04/conference-states-parties-adopts-decision-suspend-certain-rights-and.

58 Organisation for the Prohibition of Chemical Weapons, Note by the Technical Secretariat, *First Report by the OPCW Investigation and Identification Team Pursuant to Paragraph 10 of Decisions C-SS-4/Dec.3 "Addressing the Threat from Chemical*

The United States considers the use of chemical weapons and the Assad regime's lack of responsiveness to the OPCW as a threat because it is in the United States' interest to protect the global norm against their use. In December 2019, Congress passed new legislation, the Caesar Syria Civilian Protection Act of 2019, to further target the financial networks that support the Assad regime.[59] The 2018 NPFRA included examples of procurement schemes designed to obtain specialized equipment for Syria, including for entities like the Syrian Scientific Studies and Research Center, in violation of both U.S. sanctions and export controls.[60] As the U.S. sanctions authorities targeting Syria have expanded, there has been increased attention on those who deal directly with the Assad family, the government of Syria, and the many state-owned or -controlled enterprises that ultimately support Assad. The United States continues to enforce sanctions against international entities that seek to provide the Assad regime with the resources to maintain its chemical weapons program. This includes the Syrian government's efforts to use the international financial system. In June 2019, for example, OFAC designated Samer Foz and his business network, which includes companies in the UAE and Lebanon.[61] In December 2021, OFAC designated two Syrian military officials for their involvement in chemical weapons attacks against Syrian civilians.[62]

As with Iran, Syria was the subject of a maritime-related sanctions advisory, in March 2019.[63] The Department of Commerce has also added several individuals and companies, including those based in Lebanon and Syria, to the Entity List for seeking U.S.-origin goods on behalf of Syria's WMD program.

Pakistan

Pakistan has a nuclear weapons program, but it is not a party to the NPT. Therefore, large portions of its nuclear activities are not under international safeguards, and the United States and other NPT parties are prohibited by the treaty from supporting these activities in any way. Pakistan's threat perception of India drives its development of nuclear weapons and advanced missile capabilities.[64] To fulfill its stated military planning and deterrence requirements, Pakistan likely seeks U.S.-origin goods, technology, and expertise to augment its existing nuclear and conventional capabilities, including advanced ballistic missiles, cruise missiles, and unmanned aerial vehicles (UAVs).

Due to these factors, Pakistan's longstanding procurement and diversion of sensitive items to these programs is of particular concern to the United States. In 2019, the Department of Commerce published a due diligence guide for

---

Weapons Use" Ltamenah (Syrian Arabian Republic) 24, 25, and 30 March 2017, (Apr. 8, 2020), https://www.opcw.org/sites/default/files/documents/2020/04/s-1867-2020%28e%29.pdf.

59 U.S. Congress, The Caesar Syria Civilian Protection Act (The Caesar Act), Pub. L. 116-92, div. F, title LXXIV, (Dec. 2019), https://home.treasury.gov/system/files/126/caesar_act.pdf.

60 The SSRC was among the first entities designated under E.O. 13382 when it was promulgated in 2005. U.S. Department of the Treasury, Office of Foreign Assets Control, "Non-Proliferation Designations; Issuance of a new Executive Order on Non-Proliferation," (Jun. 29, 2005), https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20050629.

61 According to the press release, Foz also sought business with an unnamed Russian bank to expand the international nature of their operations. Department of the Treasury, "Treasury Designates Syrian Oligarch Samer Foz and His Luxury Reconstruction Business Empire," (Jun. 11, 2019), https://home.treasury.gov/news/press-releases/sm704.

62 Treasury designated Major Generals Tawfiq Muhammad Khadour and Muhammad Youssef Al-Hasouri for their involvement in the April 7, 2018 chlorine attack on Eastern Ghouta and the April 4, 2017 sarin attack at Khan Shaykhun, respectively. U.S. Department of the Treasury, "Treasury Targets Repression and the Undermining of Democracy," (Dec. 7, 2021), https://home.treasury.gov/news/press-releases/jy0517.

63 Department of the Treasury, OFAC Advisory to the Maritime Petroleum Shipping Community, (Mar. 25, 2019).

64 2019 Annual Threat Assessment, p. 10. For a discussion of specific aspects of Pakistan's nuclear doctrine, see Paul K. Kerr and Mary Beth Nikitin, *Pakistan's Nuclear Weapons* (Congressional Research Service, Aug. 1, 2016), https://sgp.fas.org/crs/nuke/RL34248.pdf.

exporters that specifically focused on Pakistan's violations of U.S. export controls.[65] The guide recommends steps for manufacturers to apply scrutiny to new or unfamiliar customers, particularly those who are arranging shipment for their orders through freight forwarders or whose listed address for an end-user matches the address of a company on the Entity List. The guide highlighted how individuals and entities in third countries, like Saudi Arabia and the UAE, have attempted to procure goods for ultimate delivery to Pakistan. The Department of Commerce followed up on these actions with additions to its Entity List for companies or other entities that support Pakistan's unsafeguarded nuclear or missile activities.[66] For example, in November 2021, it added 16 entities and individuals operating in China and Pakistan for contributions to Pakistan's unsafeguarded nuclear activities or ballistic missile program.[67]

Non-State Actors and WMD Proliferation

The United States remains concerned about the prospect of a non-state actor, particularly a terrorist organization, obtaining WMD capabilities, as there remains a high degree of interest by these organizations in using chemical or biological weapons against U.S. interests abroad and potentially the U.S. homeland.[68] In 2018, the United States released a comprehensive National Strategy for Countering WMD Terrorism[69] to

- Update the country's efforts to deny terrorists' access to WMD and related materials;
- Target terrorist groups that may try to acquire these capabilities (including technical experts and facilitators who may be affiliated with or supporting terrorist groups); and
- Strengthen defenses at home and abroad against the use of a WMD.

The 2018 National Strategy for Countering WMD Terrorism noted that the most well-documented use of a WMD by a terrorist group remains ISIS's use of sulfur mustard, chlorine, and other toxic industrial chemicals in Syria.

Key Takeaways

Readers of the 2018 NPFRA may note that the threat actors that pose the most significant PF threats to the United States remain unchanged in the 2021 assessment. The steady nature of the threat should not suggest that these actors are using the same methods to conduct their activities. While many methodologies remain tried-and-true, some threats, like the DPRK, are increasing their focus on the virtual asset sector to generate funds and move resources. Additionally, the United States is increasingly concerned about Chinese and Russian military modernization. While neither country engages in the same revenue-generating activity as comprehensively sanctioned jurisdictions, including Iran and the DPRK, China and Russia are seeking U.S.-origin technology they cannot produce on their own and, as the case studies in the Vulnerabilities and Risk section demonstrate, often adopt similar methodologies.

65 Department of Commerce, Bureau of Industry and Security, *Pakistan Due Diligence Guidance*, (n.d.), https://www.bis.doc.gov/index.php/policy-guidance/pakistan-due-diligence-guidance.

66 Department of Commerce, FY2020 Annual Report, p. 9.

67 Department of Commerce, Bureau of Industry and Security, "Commerce Lists Entities Involved in the Support of PRC Military Quantum Computing Applications, Pakistani Nuclear and Missile Proliferation, and Russia's Military," (Nov. 24, 2021), https://www.commerce.gov/news/press-releases/2021/11/commerce-lists-entities-involved-support-prc-military-quantum-computing.

68 2021 Annual Threat Assessment, p. 24.

69 Executive Office of the President, *National Strategy for Countering Weapons of Mass Destruction Terrorism*, (Dec. 2018), https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/12/20181210_National-Strategy-for-Countering-WMD-Terrorism.pdf.

SECTION II. VULNERABLITIES AND RISKS

The primary proliferation threats that the United States faces use procurement and revenue-raising strategies that rely on networks. These networks comprise both state-linked and independent actors who knowingly or unknowingly conduct illegal activities for the benefit of WMD programs. When these threat actors interact with the U.S. financial system to procure items, such as dual-use goods, they obscure the connections to sanctioned jurisdictions or jurisdictions of concern and misrepresent the end-user for specific proliferation-sensitive goods.[70] Understanding the nature of PF networks requires a recognition that they know how to commit regulatory arbitrage and exploit the relative openness of the global financial system to accomplish their goals.

Proliferation networks generally hide their activities behind front or shell companies. They rely on the multiple nodes in an international commercial or financial transaction implicating uneven AML/CFT/CPF regimes. Networks exploit the geographical distance between the buyer and seller to increase the ease with which they can obscure end-users or destinations for goods, especially across multiple jurisdictions.

For the United States, the size of the U.S. financial system, its centrality in the payment infrastructure supporting global trade, and its production of proliferation-sensitive technology make it structurally vulnerable to the financing of proliferation. For other jurisdictions, their vulnerabilities could be found in their geographic proximity to a proliferating state, their status as a transshipment hub, or their access to certain natural resources useful to the needs of a WMD program.

For the private sector, these vulnerabilities may stem from the products and services a particular company offers that are useful to a proliferation network, compliance deficiencies, or a lack of awareness of the global proliferation supply chain and the role they may play within it. In the PF context, these private sector entities include manufacturers of dual-use goods or those involved in the trade of commodities that proliferating states exploit for revenue-raising activities.

In the context of export controls, the issue becomes one of state budgets directed to illegal acquisitions through their procurement networks for prohibited end-users involved in WMD development. While a WMD program engaged in export control violations may be constituted through funds from a nation-state budget, for those nation-states under comprehensive sanctions, that state budget may need to be supplemented by a variety of illicit activity.

As a counter-measure to these potential risks, both natural and legal U.S. persons must comply with sanctions and export control regulations issued by the federal government, such as OFAC, the Department of Commerce's BIS, and the Department of State's Bureau of International Security and Nonproliferation.[71] U.S. financial institutions

70 As stated in the 2020 National Illicit Finance Strategy, "While much of [PF] activity takes place in foreign jurisdictions and involves non-U.S. persons, given the importance of the U.S. dollar and financial system to international trade and finance and the difficulty in identifying the underlying illicit connections, U.S. financial institutions often unwittingly process these transactions. On occasion, financial institutions and other businesses and persons willfully engage in sanctions evasion schemes." Department of the Treasury, *National Strategy for Combating Terrorist and Other Illicit Financing*, (Jan. 2020), p. 12, https://home.treasury.gov/system/files/136/National-Strategy-to-Counter-Illicit-Financev2.pdf.

71 OFAC sanctions compliance works on a strict liability standard. The presence of a strong compliance program can, depending on specific circumstances, reduce penalties associated with breaches of U.S. sanctions. Financial institutions are encouraged to consult the OFAC compliance commitments document. Federal Banking Agencies promulgate regulations and conduct examinations of depository institutions to ensure compliance with the BSA and OFAC sanctions requirements and to communicate this and related requirements to relevant covered entities. For a compendium of BSA information by relevant regulators, see Office of the Comptroller of the Currency, "Links to Other Organizations' Bank Secrecy Act (BSA) Information," (n.d.), https://www.occ.treas.gov/topics/supervision-and-examination/bsa/links-to-other-orgs-bsa-info/index-links-to-other-organizations-bsa-info.html. On OFAC compliance, see Department of the Treasury,

and other entities with AML program requirements under the BSA ("covered entities") mitigate these risks through the appropriate, risk-based implementation of their BSA requirements to include customer due diligence, transaction monitoring, and the filing of suspicious activity reports. The revised FATF Standards also require covered private sector entities (financial institutions, designated non-financial businesses and professions, and virtual asset services providers) to assess, understand, and mitigate their PF risk. Often, a great deal of PF activity resembles legitimate commercial trade, and it is very difficult in many instances for even the most sophisticated financial institution or other private sector actor to identify this activity.[72]

Vulnerabilities of the U.S. Financial System and Economy to Illicit Financial Activity

While there may be examples of proliferation networks exploiting several types of vulnerabilities of the U.S. financial system and economy, the most significant PF vulnerabilities stem from the ease with which these relationships can use opaque corporate entities to engage with the U.S. financial system (largely indirectly via correspondent banking networks involving U.S. banks). These networks aim to use opaque corporate entities to conduct seemingly legitimate commercial activity, which is ultimately for the benefit of WMD programs.

These networks generally work across three of the most significant vulnerabilities:

- The misuse of legal entities, as proliferation networks create opaque corporate structures to access needed correspondent banking relationships with globally significant financial institutions. These front or shell companies present themselves as innocuous trading firms, hiding in plain sight amid a larger global ocean of small and medium enterprises;
- The exploitation of the maritime sector to transport goods needed as inputs for proliferation programs and revenue-generating activity (including the trade of important global commodities like oil and coal); and
- The embrace of the digital economy, including malicious cyber activity and misuse of virtual assets, especially as new market entrants may operate in jurisdictions without strong AML/CFT regulation and supervision for virtual assets, may not yet be fully aware of their AML/CFT obligations in their jurisdiction as required by the FATF, or may prioritize growth over compliance with AML/CFT obligations.

In response to private sector feedback to the 2018 NPFRA, this NPFRA provides a wide variety of case studies to demonstrate the breadth of this activity and the specific methodologies PF networks use. As these cases demonstrate, much of the activity identified in the 2018 NPFRA continues, and these actors have further innovated, expanding their networks through new jurisdictions and embracing new financial technology to move funds around the world.

MISUSE OF LEGAL ENTITIES AND CORRESPONDENT BANKING RELATIONSHIPS

Proliferation networks work through the interconnected global financial system, seeking methods for appearing to engage in legitimate commercial activity for revenue generation or the procurement of specific goods for their WMD programs. A key enabler for exploiting this infrastructure is the misuse of legal entities, particularly the ease with which networks can create shell or front companies to obscure who ultimately benefits from the transactions these firms conduct.[73] By design, these front or shell companies appear to be engaged in legitimate commerce. To the

Office of Foreign Assets Control, *A Framework for OFAC Compliance Commitments*, (May 2, 2019), https://home.treasury.gov/system/files/126/framework_ofac_cc.pdf.

72 FATF PF Risk Assessment Guidance, p. 33.

73 This remains a global challenge, as evidenced by the FATF Mutual Evaluation Review process, which collects information on jurisdiction's technical compliance with Recommendation 24. This Recommendation requires timely access to accurate, adequate, and current beneficial ownership information on companies and other legal persons. Many sophisticated

extent that those commercial transactions are cleared in U.S. dollars, they transit the U.S. financial system through the correspondent banking relationships that U.S. financial institutions maintain for banks around the world.

The following case studies highlight that proliferation networks exist in a vast financial and global trade environment with many methods for disguising who they are and the purpose behind their transactions. The ease with which PF networks can create corporate entities whose ownership evades the scrutiny of relevant authorities is a challenge faced by jurisdictions of varying levels of AML/CFT/CPF sophistication. This suggests a global need to improve AML/CFT/CPF compliance, including enhancing appropriate methods for collecting and verifying ultimate beneficial ownership of legal entities to assist law enforcement in investigating sanctions evasion and export control violations.

DPRK

DPRK – Banking and Financial Services – Foreign Trade Bank

The UN- and U.S.-designated Foreign Trade Bank (FTB) of the DPRK is its primary foreign exchange bank. Until its designation by OFAC in March 2013,[74] the state-owned institution was the primary conduit between the global financial system and Pyongyang, as it handled all interbank communications, regulated the use of DPRK currency, and handled the import and export of various commodities on behalf of the government. It was also the "key financial node in North Korea's WMD apparatus."[75] Tracing FTB's linkages to proliferation networks on behalf of Pyongyang remains a U.S. priority.

In May 2020, U.S. authorities unsealed criminal charges against more than 30 individuals who worked in various capacities to allegedly provide services and effect prohibited U.S. dollar transactions for FTB.[76] The indictment outlined specific payments made to U.S. companies ultimately on behalf of the DPRK government. Other payments between FTB front companies and other third-party companies cleared through U.S. correspondent banks.

The individuals listed in the indictment, including previous presidents of FTB, caused correspondent banks to process at least $2.5 billion in illegal payments, via over 250 front companies, that transited through the United States during the period of the conspiracy. These companies were established in China, Austria, Libya, the Marshall Islands, Kuwait, Thailand, and Russia. Many individuals indicted were stationed in these countries, operating covert "branches" of the FTB, with significant activity concentrated in Chinese cities.

The individuals worked with third-party financial facilitators to create front companies that could make payments to purchase commodities and other goods on behalf of the DPRK, including payments related to the trade in refined petroleum and coal. Other payments were made to metals, electronics, and telecommunications companies, including a Chinese firm on the Commerce Department's Entity List.[77] The defendants created new

jurisdictions, including the United States, still struggle to do this effectively.

74 Department of the Treasury, Office of Foreign Assets Control, "Treasury Sanctions Bank and Official Linked to North Korean Weapons of Mass Destruction Programs," (Mar. 11, 2013), https://www.treasury.gov/press-center/press-releases/pages/jl1876.aspx.

75 Ibid.

76 *United States of America v. Ko Chol Man, Kim Song Ui, et al.*, 1:20-cr-00032-RC. Of the 33 named defendants, 7 had already been designated by OFAC prior to the indictment. Of those not designated, many worked for front companies or for the branches of the previously designated FTB.

77 Panda International Information Technology was put on the Entity List in June 2014 for its attempts to procure U.S.-origin times for "activities contrary to the national security and foreign policy interests of the United States," to wit, assisting Chinese telecommunications company Huawei in exporting sophisticated goods to the DPRK. Department of Commerce, Bureau of Industry and Security, "Addition of Certain Persons to the Entity List; and Removal of

front companies once counterparties deemed the old ones suspicious. They used coded payment references in communications between FTB agents so FTB headquarters could direct purchases and keep an accurate appraisal of the flow of funds from their front companies to payees. Finally, when it came to shipping actual goods, the defendants labeled contracts and invoices with false end destinations and end-users.

A civil forfeiture action filed in July 2020 sought more than $2.37 million from four companies that allegedly laundered U.S. dollars on behalf of sanctioned DPRK banks.[78] The four companies allegedly were part of a scheme to launder payments to subsequently sanctioned entities, including multiple covert branches of FTB.

DPRK – Banking and Financial Services – Sinsar Trading PTE

In March 2021, a DPRK national employed by Sinsar Trading PTE, a Singapore-based trading company, was extradited to the United States, where he is accused of laundering money through the U.S. financial system as part of a scheme to provide luxury items to the DPRK. According to the indictment and other court documents, between April 2013 and November 2018, the extradited individual and others conspired to access the U.S. financial system covertly and fraudulently. He is alleged to have defrauded U.S. banks and violated both U.S. and UN sanctions through transactions valued at over $1.5 million.

The indictment further alleges that he was affiliated with the DPRK's primary intelligence agency, the RGB, which is subject to U.S. and UN sanctions. According to the indictment, the individuals involved in the scheme used a web of front companies and bank accounts registered to false names and removed references to the DPRK from international wire transfer and transactional documents. The defendant used front companies, including a hair and beauty products company, for DPRK banks to process U.S. dollar payments for commodities for DPRK customers. By intentionally concealing that their transactions were for the benefit of DPRK entities, these individuals deceived U.S. correspondent banks into processing U.S. dollar transactions for the benefit of DPRK entities, which the correspondent banks would have otherwise not processed.[79]

According to the indictment, the defendant used Sinsar Trade PTE to procure U.S.-origin technology, agricultural commodities, and luxury goods for DPRK customers. In its September 2017 report, the UN Panel of Experts noted that the DPRK national was a supplier to GLOCOM, a front for Pan Systems Pyongyang, a company operated by the RGB.[80]

The Sinsar-associated front company routed shipments to the DPRK through Chinese ports (including Dalian) and listed false end-destination information on relevant shipping documents, such as bills of lading.[81] Some of the shipping documentation contained generic references to the goods being exchanged as a way to further obscure

---

Person from the Entity List Based on Removal Request," Final Rule, (Jun. 26, 2014), https://www.federalregister.gov/documents/2014/06/26/2014-14935/addition-of-certain-persons-to-the-entity-list-and-removal-of-person-from-the-entity-list-based-on.

78 Department of Justice, "United States Files Complaint to Forfeit More Than $2.37 Million from Companies Accused of Laundering Funds to Benefit Sanctioned North Korean Entities," (Jul. 23, 2020), https://www.justice.gov/opa/pr/united-states-files-complaint-forfeit-more-237-million-companies-accused-laundering-funds.

79 Department of Justice, "First North Korean National Brought to the United States to Stand Trial for Money Laundering Offenses," (Mar. 22, 2021), https://www.justice.gov/opa/pr/first-north-korean-national-brought-united-states-stand-trial-money-laundering-offenses. The complete indictment can be found at https://www.justice.gov/opa/press-release/file/1379211/download.

80 1718 Sanctions Committee (DPRK) Panel of Experts, *Final Report of the Panel of Experts submitted pursuant to resolution 1874 (2009)*, (Sept. 2017), https://www.undocs.org/S/2017/742.

81 According to court documents, communications between the defendant and his Chinese co-conspirators explicitly mentioned switching bills of lading once shipments reached Dalian. See https://www.justice.gov/opa/press-release/file/1379211/download, p. 19.

the trade in banned commodities.[82] Communications among the defendant and his co-conspirators referenced in court documents spoke to their awareness of due diligence measures generally undertaken by international financial institutions to avoid direct dealings with DPRK entities.[83]

The defendant also arranged covert loans to FTB through its office in Shenyang, China, to promote trade with and commercial investment in the DPRK. FTB used a variety of China-based front companies to launder the repayment of the loan, which was also wired through U.S. correspondent banks. In one instance, the defendant arranged, through another company in Singapore, for the purchase of boat engines produced by a U.S. company, which were controlled for export to the DPRK. The defendant also managed the creation of a company, Korea Ferrous Metals Exporting and Importing Corporation, intended to develop commodities business in third countries, including Russia.

Iran

Iran – Export Control Violations and U.S.-Origin Technology – Mehrdad Ansari

In May 2021, a federal jury convicted an Iranian citizen and resident of the UAE and Germany, Mehrdad Ansari, for scheming to obtain military sensitive parts for Iran in violation of the Iranian trade embargo. According to court documents, Ansari and his co-defendants obtained or attempted to obtain from companies worldwide over 105,000 parts valued at approximately $2,630,800 involving more than 1,250 transactions, using Ansari's company, Gulf Gate Sea Cargo, located in Dubai. At no time did the defendants, individually or through any of their companies, ever apply for or receive either a required OFAC license or Department of Commerce export license to ship any item listed in this indictment to Iran. Ansari was sentenced on September 14, 2021 to 63 months in prison followed by three years of supervised release.[84]

According to the indictment,[85] Ansari participated in this scheme in conjunction with Susan Yip and Mehrdad Foomanie. According to a Department of Commerce case summary, Yip acted as a broker and conduit for Foomanie's purchases. She admitted using her companies in Taiwan and Hong Kong to assist Foomanie in unlawfully procuring items from U.S. companies.[86] The individuals operating this network procured goods that did not need an export license if their end-users were in Taiwan or Hong Kong. As documented in the indictment, the defendants understood they were violating U.S. restrictions against Iran by falsifying the end-user locations for their purchases.[87]

82 This includes a November 2018 shipment of "equipment and materials" from Dalian, China, to Nampo, North Korea. Ibid., p. 24.

83 According to the indictment, the communications included explicit instructions to a company in Thailand involved in the export of tobacco to "Please remove North Korea from the invoice" and another transaction where the defendant told an associate who was wiring him money that "The person in charge do not wish to let their counter part to know where is cargo goes to [sic]." Ibid., p. 11.

84 One of Ansari's co-defendants, Susan Yip, was sentenced to two years in federal prison in 2012. The third, Mehrdad Foomanie, remains a fugitive. Department of Justice, "Jury Convicts Iranian National for Illegally Exporting Military Sensitive Items," (May 7, 2021), https://www.justice.gov/opa/pr/jury-convicts-iranian-national-illegally-exporting-military-sensitive-items; Department of Justice, "Iranian National Sentenced for Illegally Exporting Military Sensitive Items," (Sep. 14, 2021), https://www.justice.gov/opa/pr/iranian-national-sentenced-illegally-exporting-military-sensitive-items#:~:text=An%20Iranian%20national%20was%20sentenced,Economic%20Powers%20Act%20(IEEPA).

85 *United States of America v. Susan Yip (a/k/a Susan Yeh), Merhdad Foomanie (a/k/a Frank Foomanie), and Merhdad Ansari*, Case 5:11-cr-00516-XR.

86 Department of Commerce, Bureau of Industry and Security, *Actual Investigations of Export Control and Antiboycott Violations* (Jan. 2017), https://www.bis.doc.gov/index.php/documents/enforcement/2206-dlthty-january-2017/file, pp. 24-25.

87 According to the complaint, this included allegations of repeated false statements to U.S. law enforcement about the components not being exported to any other destination once they had reached Taiwan or Hong Kong.

Iran – Banking and Financial Services - Rosco/Persepolis

In March 2021, the Department of Justice unsealed a criminal complaint charging 10 Iranian nationals with running a nearly 20-year-long scheme to evade U.S. sanctions on the government of Iran. These 10 Iranian nationals allegedly disguised more than $300 million worth of transactions, including the purchase of two $25 million oil tankers, on Iran's behalf through front companies in the San Fernando Valley of California, Canada, Hong Kong, and the UAE. In addition, a forfeiture complaint sought a $157.3 million money laundering penalty. During the scheme, the defendants allegedly created and used more than 70 front companies, money service businesses, and exchange houses, often using the name "Persepolis" or "Rosco." The defendants also allegedly made false representations to financial institutions to disguise more than $300 million worth of transactions on Iran's behalf, using money wired in U.S. dollars and sent through U.S.-based banks. In addition, several defendants allegedly used a Hong Kong-based front company known as Total Excellence Ltd. to secretly buy two $25 million oil tankers on Iran's behalf.[88]

China

China – Export Control Violations and U.S.-Origin Technology – Yi-Chi Shih

In July 2021, a California man, Yi-Chi Shih, was sentenced to 63 months in prison for his role in a scheme to illegally export integrated circuits with military applications to China. As part of his sentence, the judge ordered Shih to pay $362,698 in restitution to the IRS and fined him $300,000.[89] Shih, a former U.S. defense contractor, and his co-defendant, Kiet Ahn Mai, used several front companies they controlled to obtain semiconductor chips from a U.S. company.

Shih and Mai defrauded a U.S. semiconductor fabrication plant (also known as a foundry) that manufactured monolithic microwave integrated circuit (MMIC) technology and is a provider of chips to the U.S. military. According to the Department of Justice press release, MMICs have a variety of potential military uses: missiles, missile guidance systems, fighter jets, electronic warfare, electronic warfare countermeasures, and radar applications. According to the criminal complaint,[90] to facilitate the production of chips according to its customers' specifications, the company maintains an online web portal for uploading design specifications. The company maintains processes for domestic and international end-user and end-use controls to ensure compliance with U.S. export controls. Shih posed as a U.S.-based customer seeking to obtain MMICs for use solely in the United States. Shih used a U.S.-based company he controlled, Pullman Lane, to receive funds from Chinese entities and finance the manufacturing of the MMICS by the victim U.S. company. Shih relied on multiple freight-forwarding companies for delivery to Hong Kong.

China – Export Control Violations and U.S.-Origin Technology – Northwestern Polytechnic University

In April 2021, a Chinese national pleaded guilty in connection with illegally procuring and causing the illegal export of $100,000 worth of U.S.-origin goods to Northwestern Polytechnical University (NWPU), a Chinese military university that is heavily involved in military research and works closely with the People's Liberation Army on the

88 Department of Justice, "Iranian Nationals Charged with Conspiring to Evade U.S. Sanctions on Iran by Disguising $300 Million in Transactions Over Two Decades," (Mar. 19, 2021), https://www.justice.gov/opa/pr/iranian-nationals-charged-conspiring-evade-us-sanctions-iran-disguising-300-million.

89 Department of Justice, "Electrical Engineer Sentenced to More Than Five Years in Prison for Conspiring to Illegally Export to China Semiconductor Chips with Military Uses," (Jul. 22, 2021), https://www.justice.gov/opa/pr/electrical-engineer-sentenced-more-five-years-prison-conspiring-illegally-export-china.

90 *United States v. Yi-Chi Shih and Kiet Ahn Mai*, Case 2:18-cr-00050 -JAK.

advancement of its military capabilities.[91] Shuren Qin, 44, a Chinese national residing in Wellesley, Massachusetts, who gained admittance into the United States through the EB-5 Immigrant Investor Visa Program in 2014, pleaded guilty to multiple charges.

According to the indictment,[92] Qin established LinkOcean Technologies, Ltd., which he used to import goods and technology with underwater and marine applications into China from the United States, Canada, and Europe. NWPU has been involved in the development of unmanned aerial vehicles, autonomous underwater vehicles, and missile proliferation projects. Since 2001, the Department of Commerce has had NWPU on its Entity List for national security reasons.[93] Qin communicated with and received taskings from NWPU to obtain items used for anti-submarine warfare. Between approximately July 2015 and December 2016, Qin caused at least 60 hydrophones (devices used to detect and monitor sound underwater) to be exported from the United States to NWPU without obtaining the required export licenses from the Department of Commerce. Qin and his company, LinkOcean, did so by concealing from the U.S. manufacturer of the hydrophones that NWPU was the true end-user and by causing false end-user information to be filed with the U.S. government.

China – Export Controls and U.S.-Origin Technology – Alex Yun Cheong Yue Violations

In March 2021, a California resident, Alex Yun Cheong Yue, was sentenced to time served and three years of supervised release and a prohibition from engaging in import-export transactions for the same period. Alex Yun Cheong Yue pleaded guilty to one count of conspiracy to commit export violations, two counts of unlawful exports and attempted exports of U.S. goods to Hong Kong, and one count of smuggling.[94] He and an at-large co-defendant, Wai Kay Victor Zee of Hong Kong, using Yue's company Premium Tech Systems, conspired to procure and export cesium atomic clocks from the United States to Hong Kong without obtaining the required export licenses.[95]

To obtain the atomic clocks, Yue created a front company, Ecycle Tech International Ltd., representing to the U.S. seller that the clocks would be used solely in the United States. Yue would take possession of the clocks and reship them to Hong Kong with paperwork that falsely described what the clocks were and undervalued their worth.

Russia

Russia – Export Control Violations and U.S.-Origin Technology – Multi Technology Integration Group EOOD

In December 2020, a federal grand jury indictment charged three foreign nationals (a Russian citizen and two Bulgarian citizens) with violating IEEPA, the Export Control Reform Act, and a money laundering statute in a scheme to procure sensitive radiation-hardened circuits from the United States and ship those components to

91 Department of Justice, "Chinese National Pleads Guilty to Illegal Exports to Northwestern Polytechnical University," (Apr. 28, 2021), https://www.justice.gov/usao-ma/pr/chinese-national-pleads-guilty-illegal-exports-northwestern-polytechnical-university.

92 *United States v. Shuren Qin, LinkOcean Technologies, Ltd. and Northwestern Polytechnic University*, Case 1:18-cr-1025-DJC.

93 The Department of Commerce added NWPU to the Entity List in 2001, as the University conducts research on UAVs, autonomous underwater vehicles, and missile proliferation projects. U.S. Department of Commerce, Bureau of Export Administration, "Entity List: Revisions and Additions," Final Rule (May 14, 2001), https://www.federalregister.gov/documents/2001/05/14/01-12188/entity-list-revisions-and-additions.

94 Department of Justice, U.S. Attorney's Office for the District of Massachusetts, "California Man Sentenced for Illegally Exporting Cesium Atomic Clocks to Hong Kong," (Mar. 5, 2021), https://www.justice.gov/usao-ma/pr/california-man-sentenced-illegally-exporting-cesium-atomic-clocks-hong-kong.

95 Cesium atomic clocks are controlled for national security reasons; the clocks have various defense and aerospace applications, including as components in global positioning system solutions, network timing protocols, and encryption programs.

Russia through Bulgaria without the required licenses.[96] The indictment alleged that they used Bulgarian company Multi Technology Integration Group EOOD (MTIG) to receive controlled items from the United States and send them to Russia. In 2014, the defendants met with the supplier of radiation-hardened components in Austin, Texas, and were informed that radiation-hardened circuits could not be shipped to Russia because of U.S. trade restrictions. As a result, they used MTIG in Bulgaria to buy the controlled electronic circuits. The parts were shipped to Bulgaria in 2015 and MTIG soon thereafter shipped them to one of the defendant's companies in Russia.

In conjunction with the indictment, the Department of Commerce added the individuals and the companies they controlled to the Entity List. It also imposed a civil monetary penalty on the Texas-based company totaling $497,000 (with a portion suspended until September 2023) and a suspended denial of export privileges (until September 2023).[97]

Russia – Export Control Violations and U.S.-Origin Technology – Alexander Brazhnikov

In March 2021, the Department of Commerce's BIS imposed a 15-year denial order against a New Jersey resident, Alexander Brazhnikov Jr., capping a multiyear investigation into his efforts to export to Russian entities. He was also sentenced and fined for money laundering and smuggling. The Federal Bureau of Investigation (FBI) concluded that this four-year-long operation effected the illicit export of $65 million worth of electronics to Russia.[98] Brazhnikov's network procured goods on behalf of 14 entities that were part of Russia's military-industrial complex, including the All-Russian Scientific Research Institute of Technical Physics (VNITF), a nuclear weapons center and component of Russia's atomic energy agency Rosatom that has been on the Entity List since 1997.[99]

To defraud U.S. manufacturers, Brazhnikov and his co-conspirators relied on tried-and-true methods for smuggling goods to countries without an export license. Brazhnikov owned and operated four companies in New Jersey that specialized in the export of microelectronics. Brazhnikov would make purchases from U.S.-based manufacturers. When received at his New Jersey-based companies, Brazhnikov and his co-conspirators would repackage them for export, lying about their true value and ultimate end-user to evade detection by U.S. export authorities. They created front companies in third countries to arrange the initial goods orders. Once the goods arrived at their initial destination, individuals would open and subsequently repackage the goods for onward shipment to Russia. Brazhnikov's associates in Moscow would then collect the packages, often from vacant storefronts or apartment buildings for the final end-users, including VNITF.

The initial financing for the scheme originated from Russian defense entities. To avoid arousing suspicion, the Russian entities routed the initial payments through the bank accounts of multiple shell corporations located in the British Virgin Islands, Latvia, the Marshall Islands, Panama, Ireland, England, the UAE, and Belize. Brazhnikov

96 Department of Justice, "International Trio Indicted in Austin for Illegal Exports to Russia," (Dec. 18, 2020), https://www.justice.gov/opa/pr/international-trio-indicted-austin-illegal-exports-russia.

97 Department of Commerce, Bureau of Industry and Security, "BIS Imposes Administrative Penalty of $497,000 to Resolve Allegations of Conspiracy to Divert Radiation-Hardened Silicon Wafers to Russia," (Sep. 28, 2021), https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/2846-2021-09-28-final-clean-vorago-press-release/file.

98 Brazhnikov had previously pleaded guilty and been sentenced to 70 months in prison for his role in this scheme. U.S. Department of Justice, "Union County, New Jersey, Man Sentenced to 70 Months in Prison for Role in Illegal International Procurement Network," (Jun. 30, 2016), https://www.justice.gov/usao-nj/pr/union-county-new-jersey-man-sentenced-70-months-prison-role-illegal-international. U.S. Department of Commerce, Bureau of Industry and Security, "BIS Imposes Denial Order on New Jersey Resident for Exports to Russian Nuclear Weapons Center and Other Prohibited End Users," (Mar. 10, 2021), https://bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/2723-brazhnikov-press-release-3-10-21/file.

99 Department of Commerce, Bureau of Industry and Security, "Revisions to the Export Administration Regulations: Additions to the Entity List," (Jun. 30, 1997), https://nuke.fas.org/control/export/news/bxa063097.htm.

could likewise remit money back to his customers through one of 28 separate bank accounts controlled by him and located in banks in the United States, Russia, Germany, and Cyprus.

Pakistan

Pakistan – Export Control Violations and U.S.-Origin Technology – Business World

In January 2020, the Department of Justice indicted five Pakistani nationals, all associated with the front company Business World, in a scheme to allegedly procure U.S.-origin goods for entities with ties to Pakistan's WMD program, including the Pakistan Atomic Energy Commission (PAEC) and the Advanced Engineering Research Organization (AERO).[100] The latter is on the Entity List for its use of front companies to procure items for use in Pakistan's cruise missile and strategic UAV programs.[101]

The five defendants, located in Canada, the United Kingdom, Hong Kong, and Pakistan, allegedly used a series of linked Business World-branded companies in Rawalpindi, as well as other small firms that either the defendants owned or for which they served as corporate officers, to carry out this scheme. The conspirators' network of front companies acted as the supposed purchasers and end-users of the goods and as the apparent source of payments for the goods, even though the goods were ultimately received in Pakistan and paid for by AERO or PAEC.

According to the indictment, among the goods this web of companies and payments procured were semiconductors, electrical components, aircraft parts, satellite communication equipment, and various pieces of industrial equipment. The fact pattern generally involved PAEC or AERO initiating wire transfers to Business World (Rawalpindi)'s bank account. Those funds would then be forwarded to the accounts controlled by the front companies in the United Kingdom, Hong Kong, and Canada. The shipments of U.S.-origin goods would be routed through Hong Kong to Business World (Rawalpindi).

Key Takeaways

These case studies demonstrate how PF networks rely on corporate secrecy to facilitate their illicit access to global banking services. This activity implicates the U.S. financial system through the misuse of correspondent banking relationships. Front and shell companies serve as an important part of the infrastructure for disguising transactions designed to evade sanctions, procure proliferation-related goods, or both. The misuse of these entities is compounded by many jurisdictions' failing to collect beneficial ownership information for legal entities effectively and on a timely and accurate basis. Lack of access to beneficial ownership information for corporate entities established in the United States or abroad continues to be a significant vulnerability for the United States in the deterrence, disruption, and investigation of a variety of financial crimes, including the financing of WMD proliferation.

100 Department of Justice, "Five Men Indicted for Operating an International Procurement Network to Export U.S.-Origin Goods to Pakistan's Nuclear Program," (Jan. 15, 2020), https://www.justice.gov/opa/pr/five-men-indicted-operating-international-procurement-network-export-us-origin-goods-pakistan. The full indictment can be found at https://www.justice.gov/opa/press-release/file/1234726/download.

101 U.S. Department of Commerce, Bureau of Industry and Security, "Addition and Modification of Certain Persons on the Entity List; and Removal of Certain Persons From the Entity List," Final Rule, (Sep. 18, 2014), https://www.federalregister.gov/documents/2014/09/18/2014-22277/addition-and-modification-of-certain-persons-on-the-entity-list-and-removal-of-certain-persons-from.

EXPLOITATION OF THE MARITIME SECTOR

Proliferation networks exploit the entire global commercial supply chain to evade detection and finance the acquisition of controlled material. Shipping companies and vessels feature prominently in sanctions evasion and export control violation activities,[102] and this use of the maritime sector is abetted by the use of front and shell companies. As documented in the March 2020 global maritime advisory, Iran, Syria, and the DPRK falsify documents, reflag vessels, and switch off automatic identification systems (AIS) to avoid being discovered in the process of illicitly transferring goods.[103]

The COVID-19 pandemic profoundly disrupted global supply chains, and the world saw a global downturn in maritime trade as quarantine protocols suppressed economic demand and had practical effects for shipping, such as reduced port calls. These effects, though a temporary consequence of the pandemic, did have consequences for proliferating states. The DPRK sealed its border with China beginning in January 2020, with a limited reopening in November 2021, and according to UN Panel of Experts reporting, there was a documented reduction in both licit and illicit trade originating from or transiting to the DPRK.[104] However, these economic consequences do not appear to have deterred or slowed its advances in weapons research and development.

As with the legitimate international financial system, proliferation networks exploit the global maritime sector to support their procurement and revenue-generating activity in contravention of international law, U.S. law, or both. DPRK, Iranian, and Syrian entities rely on maritime links to conduct natural resources trade (such as oil, coal, and other globally traded commodities prohibited or restricted by U.S. or UN sanctions, or both) and smuggle goods, including U.S.-origin goods that are required inputs for weapons programs. The transactions implicating the maritime sector are largely cleared in U.S. dollars, directly implicating the U.S. financial system, and are often structured to obscure the interest and involvement of a sanctioned person or hide transactions involving a violation of relevant export controls.

Unlike the U.S. financial system (or the global finance sector writ large), which has attuned itself to the obligations of multilateral and U.S. sanctions (related to nonproliferation generally and the Iran, Syria, and DPRK country programs specifically), the maritime sector (and associated sectors like insurance) is still navigating the unique compliance challenges associated with this complex activity.

DPRK

DPRK – Sanctions Evasion and Illicit Natural Resources Trade – M/T Courageous

In July 2021, the District Court for the Southern District of New York entered a judgment of forfeiture against the M/T *Courageous*, an oil-products tanker used to make illicit deliveries of petroleum products through ship-to-ship transfers with DPRK-flagged vessels.[105] According to the Department of Justice, criminal charges for conspiracy to evade DRPK-related sanctions and money laundering are pending against the alleged owner and operator of the vessel, a Singaporean national.

---

102 This reflects a trend identified in the 2018 NPFRA, which cited several case studies and PF methodologies involving shippers. See, for example, 2018 NPFRA, pp. 14, 22, 25-27.

103 Advisory for the Maritime Industry.

104 According to the September 2021 report, "The continued border closure of the Democratic People's Republic of Korea in response to the COVID-19 pandemic appears to have significantly affected its maritime trade in its import of refined petroleum and its prohibited export of coal and other commodities," p. 13.

105 Cambodian authorities detained the vessel in March 2020 and ultimately seized it for violations of local law. Department of Justice, "United States Seizes Oil Tanker Used to Violate Sanctions Against North Korea," (Jul. 30, 2021), https://www.justice.gov/opa/pr/united-states-seizes-oil-tanker-used-violate-sanctions-against-north-korea.

According to the criminal complaint, this individual and his co-conspirators allegedly used front companies incorporated in Panama, Singapore, and China to obscure any links between M/T *Courageous* and the DPRK. He and his co-conspirators manipulated identifying information to make it appear that M/T *Courageous* was a different vessel. This also included turning off the vessel's AIS,[106] a common method for facilitating covert maritime activities, ship-to-ship transfers, and illegal visits to DPRK ports. Among the vessels M/T *Courageous* provided services for was the *Chong Rim 2* (also known as the *Saebyol*), a vessel sanctioned by the United States and the UN.[107] The defendant and his co-conspirators arranged for a variety of payments denominated in U.S. dollars that were processed through U.S.-based correspondent accounts for the vessel's operations, including fuel and crew salaries.

DPRK – Sanctions Evasion and Vessel Identity Laundering – Billions No. 18

To avoid scrutiny, networks supporting the DPRK's illicit maritime trade actively recycle the identities of vessels to evade UN and U.S. sanctions. Vessel identity laundering may involve the physical altering of a ship's markings to make it appear to be a different vessel (for example, by painting a different name, International Maritime Organization [IMO] number, or both). It may also involve the broadcasting of false AIS information, including IMO numbers of other vessels, to confuse efforts to track a ship's movement or investigate its voyage records.[108]

The operational history of the oil tanker known at various times as *Billions No. 18*, *Kingsway, Apex*, and *Shun Fa* is illustrative of this trend. In August 2021, South Korea detained a vessel that was sailing as the Mongolia-flagged *Apex* (also known as *Shun Fa*). The *Apex* had entered the area of the port of Busan. As documented by the UN Panel of Experts for the DPRK and media reports, South Korean authorities discovered the vessel was, in fact, the UN- and U.S.-sanctioned *Billion No. 18* (also known as *Kingsway*), which had been sanctioned in 2017 for an unreported transfer of petroleum to the DPRK.[109]

Once impounded, investigations discovered the traces of the vessel's real IMO number and noted other similarities between the *Apex* and *Billions No. 18*, such as similar engine models and other equipment discovered onboard. According to the UN Panel's investigations, there was a vessel called *Apex* that had sailed under a Mongolian flag. After its 2017 designation, the *Billions No. 18* effectively stole the *Apex's* identity, with physical alterations to the ship and routine broadcasting of its IMO number by the *Billions No. 18's* AIS transponder.

Further investigation by the UN Panel revealed an additional link between the two vessels: The *Billions No. 18's* holding company, United Ships Maritime Corp, was listed at the same physical address as a company called Better Smart, Ltd., the owner and manager of the *Apex* since its registration with Mongolian authorities.

106 As documented in the 2020 Maritime Guidance, AIS is "an internationally mandated system that transmits a vessel's identification and navigational positional data via high frequency waves." While there may be some legitimate reasons that vessels would disable their AIS, those that engage in illicit activity will often do so intentionally to obscure their activities. Advisory for the Maritime Industry, p. 2.

107 According to the Department of Justice press release, for a four-month period between August and December 2019, *M/T Courageous* illicitly stopped transmitting information regarding its location, during which time satellite imagery showed that *M/T Courageous* engaged in a ship-to-ship transfer of more than $1.5 million worth of oil to a North Korean ship, the *Saebyol.*

108 For additional background on these tactics in the context of the DPRK, see Department of State, Department of the Treasury, and U.S. Coast Guard, "North Korea Sanctions Advisory: Updated Guidance on Addressing North Korea's Illicit Shipping Practices," (Mar. 21, 2019), https://home.treasury.gov/system/files/126/dprk_vessel_advisory_03212019.pdf.

109 UN Panel of Experts, *September 2021 Report*, pp. 16-18; Chad O'Carroll, Joengmin Kim, Won-Gi Jung, "South Korea detaining North Korea-linked ship suspected of sanctions violations," NK News, (Aug. 20, 2021), https://www.nknews.org/2021/08/south-korea-detaining-north-korea-linked-ship-suspected-of-sanctions-violations/.

Iran – Export Control Violations and Transshipment Hubs – Computer Numerical Control Machines

In August 2019, federal authorities arrested a U.S-Iranian dual national, who previously resided in Los Angeles, for his alleged role in a conspiracy to export computer numerical control (CNC) machines to Iran illegally from the United States. According to the indictment, CNC machines allow for the automated processing of raw materials to precise finished products using digital instructions, and the Department of Commerce controls their export for nonproliferation reasons.[110]

The dual national and his co-conspirator, located in the UAE (who remains at large), engaged in a scheme where they would purchase the machines and related equipment (including, according to the indictment, shipping containers) from suppliers based in the United States and Canada for maritime shipment to the UAE. The dual national defendant would use falsified and forged invoices and packing lists and rely on his UAE-based co-conspirator to forward the machines from the UAE to Iran. The use of transshipment hubs and the falsification of trade documentation are both common typologies for proliferation networks that exploit the maritime sector.

Iran/Syria – Sanctions Evasion and Illicit Natural Resources Trade – Grace 1/Adrian Darya 1

In August 2019, the Department of Justice unsealed an arrest warrant and asset forfeiture complaint alleging the vessel known as the *Grace 1*, its cargo (Iranian-origin crude oil), and money held in a U.S. bank associated with a front company, Paradise Global Trading LLC, were subject to forfeiture. The warrant and complaint alleged that the vessel and front company were engaged in violations of IEEPA, bank fraud, and money laundering as well as a separate terrorism statute violation.[111] The warrant and complaint followed a protracted legal dispute after the vessel was seized off the coast of Gibraltar in July 2019. Ultimately, the Supreme Court of Gibraltar ordered the vessel's release from the government's custody. The vessel then sailed to the coast of Syria, where it turned off its AIS transponder. Satellite imagery confirmed that it unloaded its cargo to Iranian-flagged vessels before transiting the Suez Canal (under the name of *Arman 114*).

According to the complaint, the *Grace 1* allegedly participated in a scheme to access the U.S. financial system unlawfully to support illicit shipments to and from Iran by the IRGC. This scheme included the use of multiple parties affiliated with the IRGC to supply Iranian-origin crude oil to the Assad regime in Syria. The IRGC controlled the vessel through a complex ownership structure, where separate companies owned, managed, and crewed the vessel, and these companies appeared to be operating on behalf of other parties. An unnamed Singapore-based company operated as a front for illegal oil sales for Iran, managed the vessel, and made U.S. dollar payments to one unnamed U.S. logistics company that provides petroleum tanker products and another that sells maritime insurance. That Singapore-based company is part of a group of companies based in the UAE with links to designated Iranian entities, including the National Iranian Oil Company.

The complaint further documented the *Grace 1's* track record of AIS manipulation, including shutting off its AIS before calls on Iranian ports or ship-to-ship transfers in the Persian Gulf. It was during at least one of these transfers that the *Grace 1* liaised with another ship known to have engaged in ship-to-ship transfers for Syria. To disguise the interests of Iranian-linked entities, the *Grace 1's* owner-operators falsified shipping documentation

110 U.S. Department of Justice, U.S. Attorney's Office for the Central District of California, "Man Taken into Custody after Being Charged with Illegally Exporting Prohibited Manufacturing Equipment to Iran," (Aug. 20, 2019), https://www.justice.gov/usao-cdca/pr/man-taken-custody-after-being-charged-illegally-exporting-prohibited-manufacturing.

111 Department of Justice, "Unsealed Warrant and Forfeiture Complaint Seek Seizure of Oil Tanker 'Grace 1' for Unlawful Use of U.S. Financial System to Support and Finance IRGC's Sale of Oil Products to Syria," (Aug. 16, 2019), https://www.justice.gov/opa/pr/unsealed-warrant-and-forfeiture-complaint-seek-seizure-oil-tanker-grace-1-unlawful-use-us. For the complaint for forfeiture, see https://www.justice.gov/opa/press-release/file/1196361/download. For the arrest warrant, see https://www.justice.gov/opa/press-release/file/1196366/download.

to represent that they were actually transacting in Iraqi-origin crude oil. According to the complaint, multiple companies engaged in multiple financial transactions related to the *Grace 1*'s shipment of Iranian oil that were processed through the U.S. financial system. These payments included transfers from two companies registered in Saint Kitts and Nevis. One of those companies was registered at the same address as Blue Energy Trade Ltd., which is sanctioned by OFAC for shipping petroleum to Syria.

Multiple Countries – Sanctions Evasion – UniCredit Group Enforcement Action

In April 2019, three UniCredit Group constituent banks, UniCredit Bank AG (Germany), UniCredit Bank Austria AG, and UniCredit S.p.A (Italy), entered into a $1.3 billion settlement with OFAC and U.S. federal and state law enforcement and regulatory authorities to resolve apparent violations of multiple sanctions programs, including Burma, Cuba, Iran, Libya, Sudan, and Syria, and WMD and terrorism sanctions authorities.[112]

For a period between 2007 and 2011, these UniCredit Group banks maintained accounts for the Islamic Republic of Iran Shipping Lines (IRISL) and several companies owned by or otherwise affiliated with IRISL. They managed the accounts of those individuals or entities, causing transactions that did not identify the interest or involvement of IRISL to be sent to or through U.S. intermediaries. The nature of UniCredit Group's apparent violations did not allow U.S. intermediary parties to discern the IRISL interest in the payments and, thus, that the payments violated U.S. law.

Key Takeaways

The maritime sector remains a necessary part of the infrastructure of PF networks. Shipping and related services are necessary for the procurement of proliferation-related goods, and for those countries subject to comprehensive sanctions, the illicit import-export of commodities requires the use of vessels and associated methods (vessel identity laundering, flag-hopping, and AIS manipulation) for obscuring their activities from relevant authorities. Financial institutions, as well as other firms operating in the maritime sector, should be aware of U.S. laws and regulations targeting proliferation-related activity, including the BSA and OFAC sanctions, as well as these and other deceptive measures highlighted in relevant U.S. government and other guidance. As the 2018 NPFRA noted, some of these activities may also attempt to exploit trade finance instruments. Those engaged in trade finance activities should also consult the trade finance section of the FATF PF Risk Assessment Guidance and FATF Guidance on Trade-Based Money Laundering.[113]

112 The law enforcement and regulatory authorities are the Department of Justice, the New York County District Attorney's Office, the Federal Reserve Board of Governors, and the Department of Financial Services of the State of New York. U.S. Department of the Treasury, Office of Foreign Assets Control, "U.S. Treasury Department Announces Settlement with UniCredit Group Banks," (Apr. 15, 2019), https://home.treasury.gov/news/press-releases/sm658. The settlement agreements with all three component banks can be found in this file: https://home.treasury.gov/system/files/126/20190415_uni_webpost.pdf. The fact pattern of this case closely resembles a similar example from Commerzbank in the 2018 NPFRA, p. 22.

113 FATF PF Risk Assessment Guidance, pp. 21, 27.; Financial Action Task Force and Egmont Group, "Trade-Based Money Laundering Trends and Developments," (Dec. 2020), https://www.fatf-gafi.org/media/fatf/content/Trade-Based-Money-Laundering-Trends-and-Developments.pdf, pp. 19, 48.

UNDERMINING THE DIGITAL ECONOMY AND EMBRACING NEW FINANCIAL TECHNOLOGY

There is no evidence that a proliferation network has used a virtual asset to procure a specific proliferation-sensitive good or technology as an input to a WMD or ballistic missile program. However, virtual assets play an essential role in revenue generation and moving assets across borders.[114] States and groups that are involved in exploiting the digital economy for sanctions evasion have used existing virtual assets, like bitcoin, Ether, XRP, and Litecoin, among others, and many have developed or are trying to develop central bank digital currencies (CBDCs),[115] or virtual assets backed by the state (such as Venezuela's petro), to aid in sanctions evasion.

Hackers affiliated with or linked to the DPRK have conducted a broad range of criminal cyber activity to "further the strategic and financial interests of the DPRK government and its leader, Kim Jong-un."[116] In many cases, the activities directly target U.S. individuals and companies (including, but not limited to, financial institutions). In April 2020, the Departments of State, Homeland Security, and the Treasury, along with the FBI, released *Guidance on the North Korean Cyber Threat* to provide a comprehensive resource on how cyber actors linked to the DPRK threaten both "traditional" financial institutions as well as new financial technology companies, especially VASPs.[117]

While this activity poses a threat to U.S.-based VASPs, the risk is perhaps highest for VASPs operating in jurisdictions with weak AML/CFT/CPF controls. One of the key findings of the FATF's *Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers* is that, while there has been progress in applying the FATF Standards to this sector, many jurisdictions do not have operational AML/CFT regimes for VASPs. This is especially true for jurisdictions that are not full FATF members.[118] The FATF review paid particular attention to challenges around the implementation of the travel rule,[119] underscoring how cross-border transfers present an obstacle to preventing illicit financial activity.[120]

---

114 For example, the 2021 Annual Threat Assessment of the U.S. Intelligence Community concluded that "North Korea has conducted cyber theft against financial institutions and cryptocurrency exchanges worldwide, potentially stealing hundreds of millions of dollars, probably to fund government priorities, such as its nuclear and missile programs [emphasis added]." 2021 Annual Threat Assessment, p. 16.

115 As described by the U.S. Federal Reserve, a central bank digital currency (CBDC) is "a generic term for a third version of currency that could use an electronic record or digital token to represent the digital form of a nation's currency. CBDC is issued and managed directly by the central bank and could be used for a variety of purposes by individuals, businesses, and financial institutions." U.S. Federal Reserve, "What is a Central Bank Digital Currency? / Is the Federal Reserve moving toward adopting a digital dollar?" (n.d.), https://www.federalreserve.gov/faqs/what-is-a-central-bank-digital-currency.htm.

116 Department of Justice, "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe," (Feb. 17, 2021), https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and.

117 Department of State, Department of Treasury, Department of Homeland Security, and Federal Bureau of Investigation, CISA Alert (AA20-106A), *Guidance on the North Korean Cyber Threat*, (revised Jun. 23, 2020), https://us-cert.cisa.gov/ncas/alerts/aa20-106a.

118 Financial Action Task Force, *Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers* (Jul. 2021), https://www.fatf-gafi.org/media/fatf/documents/recommendations/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf.

119 FATF Recommendation 16 requires countries to ensure that financial institutions follow certain requirements for wire transfers of at least $1,000 or 1,000 euros, including the name of originator, beneficiary, and account number or unique transaction reference number. This obligation extends to payments made through virtual assets. In the context of the U.S. travel rule, it does not require the name of the beneficiary to be passed on (unless it has been provided to the transmitter's financial institution).

120 The Second 12-Month Review also included a specific update for PF, arising from changes to Recommendation 1 and 15, underlining that VASPs also need to assess PF risk in the context of the targeted financial sanctions imposed pursuant to

Proliferation networks are increasingly embracing certain types of virtual assets that enhance user anonymity. This activity is a significant source of revenue raised in violation of U.S. and UN sanctions.

DPRK

DPRK – Cyber-Enabled Theft and Money Laundering – RGB

In February 2021, the Department of Justice unsealed an indictment against three DPRK computer programmers who were members of units of the RGB and had allegedly engaged in, among other things, cyber-attacks on the entertainment industry, including ransomware and other cyber-enabled extortion, cyber-enabled heists against banks, cyber-enabled ATM cash-out thefts, and spear-phishing campaigns.[121] The DOJ estimated the hackers attempted to steal or extort $1.3 billion from victims. The indictment expanded an ongoing investigation into the RGB's activities dating back to 2018, highlighting the worldwide reach of Pyongyang's hacking units, variously referred to by the U.S. government and private sector as the Lazarus Group and Advanced Persistent Threat 38 (APT 38).

In these schemes, DPRK entities could rely on assistance from criminal actors knowingly engaged in helping RGB to launder funds procured through its cyber capabilities. Simultaneously with the expanded RGB indictment, the DOJ also indicted Canadian citizen Ghaleb Alaumary, who agreed to plead guilty for his role as a money launderer for the conspiracy, among other criminal schemes. Alaumary was sentenced to 140 months in federal prison in September 2021 for this and related criminal activity.[122]

The Departments of the Treasury and Justice also acted against two Chinese nationals who were charged with laundering over $100 million in virtual assets from a hack of a virtual asset exchange. OFAC designated the two Chinese nationals for having provided material support to the Lazarus Group. The two defendants allegedly worked with DPRK cyber actors who have stolen nearly $250 million worth of virtual assets.[123]

DPRK – Information Technology Workers – Munitions Industry Department

While the DPRK has prioritized the exploitation of virtual assets, it is not the only technology in which the country has invested effort to generate revenue. As referenced in the March 2021 UN Panel of Experts report,[124] the DPRK has used freelance information technology (IT) workers, who represent themselves as legitimate service providers, to generate revenue for eventual repatriation to the DPRK.

In contrast to the malicious cyber actors associated with the RGB, the DPRK IT workers often are subordinate to the UN- and U.S.-designated Munitions Industry Department, which is directly responsible for overseeing the

---

UNSCRs.

121 Department of Justice, "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe," (Feb. 17, 2021), https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and. For the text of the indictment see https://www.justice.gov/opa/press-release/file/1367701/download.

122 Department of Justice, "International Money Launderer Sentenced to over 11 Years in Federal Prison for Laundering Millions from Cyber Crime Schemes," (Sep. 8, 2021), https://www.justice.gov/usao-cdca/pr/international-money-launderer-sentenced-over-11-years-federal-prison-laundering.

123 Department of the Treasury, "Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group," (Mar. 2, 2020), https://home.treasury.gov/news/press-releases/sm924; Department of Justice, "Two Chinese Nationals Charged with Laundering Over $100 Million in Cryptocurrency From Exchange Hack," (Mar. 2, 2020), https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack; Yinyin-Jiadong indictment: https://www.justice.gov/opa/press-release/file/1253486/download; Yinyin complaint: https://www.justice.gov/opa/press-release/file/1253491/download.

124 1718 Committee, *Final Report* (Mar. 4, 2021), https://undocs.org/S/2021/211, p. 57.

country's WMD and ballistic missile programs. According to UN Panel of Experts reporting, DPRK IT workers are primarily dispatched to China and Russia, in addition to several other countries, sometimes relying on tourist or student visas to obfuscate the fact they are in these countries to generate revenue for the regime, thereby evading sanctions. UN Security Council Resolution (UNSCR) provisions require all DPRK workers abroad, regardless of their visa status, including these IT workers abusing their visas, to be repatriated to the DPRK. However, China and Russia have not pursued active enforcement along those lines.

Some DPRK IT workers advertise their services on freelance platforms, where they use a variety of methods to obscure their nationality or connection to DPRK state entities, modeled on the methods the Kim regime uses to access the formal financial system. These methods include false identification (including the repeated use of fraudulent credentials by multiple workers across multiple platforms) and the use of front companies in third countries to provide their services. DPRK IT workers will often deliberately seek to work through platforms with weak due diligence and sanctions compliance protocols.

Multiple Countries – Exploitation of Digital Payment Platforms – BitGo and Payoneer Enforcement Actions

U.S. enforcement authorities have focused on compliance deficiencies in the virtual asset space, particularly where the activity takes place in comprehensively sanctioned jurisdictions.[125] In December 2020, OFAC entered into a settlement agreement with California-based company BitGo, Inc. for apparent violations of multiple sanctions programs.[126] The apparent violations arose from virtual asset transactions taking place on its non-custodial, secure digital wallet management service,[127] which allowed customers in comprehensively sanctioned jurisdictions (the Crimea region of Ukraine, Cuba, Iran, Sudan, and Syria) to make transactions that were not permitted under U.S. law.

At the time of the apparent violations, BitGo knew that, based on internet protocol (IP) addresses, its users were located in such jurisdictions but did not incorporate this information into its sanctions compliance procedures to block those transactions. Consequently, BitGo allowed transactions to jurisdictions where there was a high risk of assets being made available to individuals and entities engaged in WMD activities. In its announcement, OFAC pointed out that, like all financial service providers, those operating virtual asset businesses should understand the sanctions risks that arise from their business operations and implement controls commensurate with those risks.

In July 2021, OFAC reached a settlement agreement with online money transmitter Payoneer, which processes transactions for corporate and financial institution customers. The company's compliance program failed to stop over 2,000 transactions that violated multiple sanctions programs, including the Ukraine, Syria, Iran, and WMD nonproliferation sanctions regulations.[128] The apparent violations were caused by deficiencies in its sanctions filters that allowed "close matches" to individuals and entities on the Specially Designated Nationals and Blocked

125 Most recently, OFAC released a brochure for the virtual assets industry to help it navigate and comply with sanctions. Department of the Treasury, Office of Foreign Assets Control, "Publication of Sanctions Compliance Guidance for the Virtual Currency Industry and Updated Frequently Asked Questions," (Oct. 15, 2021), https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20211015.

126 Department of the Treasury, Office of Foreign Assets Control, "Settlement Agreement between the Department of the Treasury's Office of Foreign Assets Control and BitGo, Inc.," (Dec. 30, 2020), https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20201230_33.

127 Non-custodial wallet service providers allow users to retain control over the private keys that allow them unfettered access to their virtual asset holdings. These are also referred to as "unhosted wallets."

128 Department of the Treasury, Office of Foreign Assets Control, "OFAC Enters Into $1,400,301.40 Settlement with Payoneer, Inc. for Apparent Violations of Multiple Sanctions Programs," (Jul. 23, 2021), https://home.treasury.gov/system/files/126/20210723_payoneer_inc.pdf.

Persons List to not be flagged appropriately. Like BitGo, Payoneer also failed to screen IP addresses for customers residing in comprehensively sanctioned jurisdictions.

Key Takeaways

While the principal risk arising from proliferation networks remains in the traditional infrastructure of global banking, particular threats, especially the DPRK, find digital platforms increasingly attractive for generating, storing, and moving value. Many of these threats also find malicious cyber activity against global banking to be highly lucrative and will seek to exploit weak security protocols in the financial sector. Instilling a culture of compliance and building a robust cybersecurity regulatory perimeter in both the traditional financial sector as well as the virtual assets sector will continue to be a U.S. government priority, as it would aid in the prevention and detection of a variety of illicit financial activity that directly supports WMD proliferation.[129]

129 President's Working Group on Financial Markets, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency, *Report on Stablecoincs* (Nov. 2021), https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf.

SECTION III.: TRENDS AFFECTING THE U.S. CPF REGIME

The United States maintains a strong legislative and regulatory framework to counter PF, which is in direct response to the complexity and pervasiveness of the proliferation risks cited in this assessment. Given the open nature of the U.S. financial system and its centrality in global trade and investment and the continued manufacturing by U.S.-based businesses of components useful to PF networks, the United States will remain vulnerable to exploitation.

Since the 2018 assessment, the United States has moved to strengthen discrete aspects of its AML/CFT/CPF regime to address outstanding vulnerabilities. While the United States prioritizes the implementation of a variety of regulations, it must also be prepared to innovate constantly to meet new challenges, and this will be addressed in the 2022 National Illicit Finance Strategy. The following trends are not an exhaustive list but are indicative of the trends that will mark the evolution of the U.S. CPF regime.

The Future of Correspondent Banking: Increased Financial Intermediation

As stated in the introduction to the NPFRA and reinforced throughout the Vulnerabilities and Risk section, the U.S. dollar is central to many aspects of the modern global economy and commerce and remains the most frequently used currency for global reserve holdings and cross-border transactions. Illicit actors need to buy and sell commodities priced and transacted in dollars, meaning many proliferation networks need touchpoints with the U.S. financial system. For example, the maritime sector is fully integrated into a global dollar-based system, and trade finance transactions and commodities contracts are frequently priced in dollars. While this system serves as source for exploitation, it also provides insight into activity using U.S. dollars and increases the reach of compliance practices at U.S. dollar-clearing institutions, which has benefits for global AML/CFT compliance programs and the enforcement of U.S. sanctions.

However, concerns about delays, frictions, or political issues in the international payment system have led to increased interest in alternatives for international transactions. To the extent these alternatives materialize and accumulate critical market share in the future, the United States could see a corresponding reduction in its ability to use its AML/CFT/CPF tools and authorities that leverage dollarization to protect the U.S. and international financial system and U.S. national security, depending on the nature and origin of the alternatives used. The U.S. government is aware that China and Russia are exploring ways to provide alternatives to U.S. dollar clearing, including alternatives to the SWIFT payment messaging system. China is a first mover in creating a digital version of its currency (the eCNY), which it hopes will see wider adoption and integration with existing payment mechanisms, pending a successful domestic pilot program.[130] If adopted at scale and used for cross-border payments in lieu of the U.S. dollar, the eCNY could pose a risk of reducing transparency in payments using the eCNY. This could hinder the ability of law enforcement to identify proliferation networks, some of which originate in China. China's growing economy in general as well as the specific impacts of the Belt and Road Initiative are also increasing the international reach of Chinese state-owned enterprises and financial institutions. Such trends are not likely to affect the ability of the U.S. AML/CFT/CPF regime to mitigate these threats in the intermediate term; rather, these are developments to monitor.

130 "China will advance development of eCNY, c. bank gov says," *Reuters*, (Nov. 9, 2021), https://www.reuters.com/world/china/china-will-advance-cbank-digital-currency-improve-its-design-governor-says-2021-11-09/.

Implementing Corporate Transparency

As the NPFRA demonstrates, proliferation networks often take advantage of jurisdictions with more lax business formation and beneficial ownership transparency requirements to advance their WMD programs. In particular, proliferation networks seek jurisdictions that do not collect beneficial ownership information at the time of incorporation or foreign-entity registration, or when ownership changes, to carry out illicit schemes anonymously through ostensibly legitimate legal entities. The anonymity afforded to these legal entities inhibits law enforcement investigations into illicit activities and underscores the need for competent authorities to have timely access to adequate, accurate, and up-to-date beneficial ownership information.

As part of the Anti-Money Laundering Act of 2020, the U.S. is working to implement regulations to require the collection of beneficial ownership information when certain corporate entities are formed (or for non-U.S. companies, when they register with a state to do business in the United States) and when their ownership changes. FinCEN, as of the publication of the NPFRA, is engaged in the rulemaking process for implementing the requirements of the Corporate Transparency Act, including the publication of the Proposed Rule in December 2021 beneficial ownership reporting.[131]

Globally, the United States also supports the efforts of the FATF and the FATF-style regional bodies to strengthen standards on beneficial ownership transparency, including compliance with and effective implementation of Recommendation 24 and Immediate Outcome 5.[132] In its Public Statement on the Pandora Papers, the FATF commented on how global implementation of Recommendation 24 remains poor and, in its 2020-2021 Annual Report, concluded that hundreds of billions of dollars laundered through fake companies demonstrates "the current beneficial ownership rules are not working."[133]

In October 2021, the FATF announced a public consultation on proposed revisions to strengthen Recommendation 24.[134] Cross-border information-sharing challenges, including those related to data privacy, protection, and localization, will likely continue to figure prominently in the inability of national authorities to discover the threats behind front and shell companies.

---

131 Congress, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Public Law No. 116-283, https://www.congress.gov/bill/116th-congress/house-bill/6395/text/enr; Department of the Treasury, Financial Crimes Enforcement Network, "FinCEN Launches Regulatory Process for New Beneficial Ownership Reporting Requirement," (Apr. 1, 2021), https://www.fincen.gov/news/news-releases/fincen-launches-regulatory-process-new-beneficial-ownership-reporting. Department of the Treasury, Financial Crimes Enforcement Network, "FinCEN Issues Proposed Rule for Beneficial Ownership Reporting to Counter Illicit Finance and Increase Transparency," (Dec. 7, 2021), https://www.fincen.gov/news/news-releases/fincen-issues-proposed-rule-beneficial-ownership-reporting-counter-illicit.

132 Recommendation 24 requires competent authorities to be able to "obtain, or have access in a timely fashion to adequate, accurate and current information on the beneficial ownership and control of companies and other legal persons" created in that country. https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf. Immediate Outcome 5 is an effectiveness measurement designed to gauge whether countries can prevent legal persons and arrangements from being misused for money laundering or terrorist financing purposes and whether competent authorities can avail themselves of beneficial ownership information "without impediments." https://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf. The FATF provides consolidated assessment ratings for all countries who have undergone a mutual evaluation. Financial Action Task Force, *Consolidated Assessment Ratings* (Updated Aug. 11, 2021), https://www.fatf-gafi.org/publications/mutualevaluations/documents/assessment-ratings.html.

133 Financial Action Task Force, "Public Statement on Pandora Papers: Statement by the FATF President," (Oct. 21, 2021), https://www.fatf-gafi.org/publications/fatfgeneral/documents/pandora-papers.html; Financial Action Task Force, *Annual Report 2020-2021,* https://www.fatf-gafi.org/media/fatf/documents/brochuresannualreports/Annual-Report-2020-2021.pdf, p. 5.

134 Financial Action Task Force, "Revisions to Recommendation 24 and its Interpretive Note - Public Consultation," (Oct. 21, 2021), http://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-consultation-r24.html.

Sanctions Evasion and State Complicity

Much of the sanctions evasion activity that PF networks engage in is enabled, either wittingly or unwittingly, by countries ignoring their responsibilities under relevant UNSCRs. States engage in this activity for a variety of reasons, which touch upon strategic, diplomatic, political, and economic priorities. State complicity, whether the witting evasion of sanctions or a "looking-the-other way" approach, is a key enabler of PF—without this complicity and permissive environment, it would be significantly more difficult for PF networks to operate. State actors including Iran and DPRK succeed largely through the neglect or active support of others. Proliferation networks seek permissive, geographically proximate jurisdictions to aid in the diversion of goods and obfuscation of transaction chains.

State complicity has been pronounced in many areas related to sanctions evasion. For example, in the context of DPRK, both Russia and China have documented track records of ignoring UNSCRs that oblige member states to repatriate DPRK nationals earning income in their jurisdictions, subject to limited exceptions. In many cases, both countries allow these laborers under different visa categories (such as student visas) to justify their presence, despite the UNSCR repatriation obligation that applies regardless of visa category. According to the State Department's 2021 Trafficking in Persons Report, there are approximately 20,000 - 80,000 North Koreans working in China. For Russia, the figures show nearly 3,000 tourist and study visas for North Koreans issued in 2020, with plans for the DPRK to send as many as 10,000 workers to Russia.[135] Importantly, as referenced in UN Panel of Expert reports, the vast majority of earnings made by North Korean laborers abroad are kept by the state-owned enterprises that employ them, giving the regime an important source of revenue.[136]

Moreover, the DPRK also forms joint ventures, which are prohibited under the DPRK UNSCRs, and conducts illicit natural resources trade with companies based in China and Russia, much of which is prohibited or otherwise restricted under those same resolutions.[137] For example, in China, individuals have used joint ventures to transfer ownership of vessels to DPRK-based individuals.[138] Joint ventures between Chinese and North Korean companies can also be found in a variety of revenue-generating activities, including hog farming, sand and gravel extraction, and IT workers.[139]

The Chinese government has also stood in the way of Chinese financial institutions providing information to U.S. authorities investigating sanctions evasion cases, which reflects a general trend to not cooperate with U.S. investigations that may touch upon Chinese state security. This trend was seen recently in the challenges faced by the Department of Justice in obtaining a response from Chinese banks to subpoenas related to an investigation into transactions they processed through U.S. correspondent bank accounts.[140]

Compliance, Trade Finance, and the Maritime Sector

While the CPF regime has prioritized encouraging best-in-class compliance practices from financial institutions, this risk assessment has demonstrated that PF networks work across multiple nodes in global supply chains. Many

135 United States Department of State, Office to Monitor and Combat Trafficking in Persons, *2021 Trafficking in Persons Report: North Korea*, https://www.state.gov/reports/2021-trafficking-in-persons-report/north-korea/.

136 1718 Committee Panel of Experts, March 2021 Report, p. 396

137 1718 Committee Panel of Experts, March 2021 Report, p. 27.

138 In response to inquiries by the Panel, the Chinese government responded that it had no evidence to suggest the vessel had been transferred. 1718 Committee Panel of Experts, March 2021 Report, p. 36.

139 1718 Committee Panel of Experts, March 2021 Report, pp. 32, 55, 57.

140 United States District Court for the District of Columbia, Memorandum Opinion, *In re* Grand Jury Investigation of Possible Violations of 18 U.S.C. § 1956 and 50 U.S.C. § 1705, (Mar. 18, 2019), https://www.dcd.uscourts.gov/sites/dcd/files/FINAL_18mc175_176_177_Mar_18_2019_Mem_Op_redacted.pdf.

nonfinancial firms may not know the extent to which they are implicated in the activities of PF networks or, if they do, what course of action to take once they discover it.[141] Building a strong culture of compliance takes time, and it requires reinforcement through guidance and, as needed, enforcement actions to punish bad behavior (and deter others from committing similar mistakes).[142] One example is an August 2019 OFAC designation of a ship-to-ship transfer network involving Taiwanese individuals and entities.[143] In response to this and U.S. official conversations with their counterparts, Taiwanese authorities have worked to address some of the compliance deficiencies in their maritime sector.[144]

The United States, as well as its partners like the United Kingdom and Japan, have tried to encourage a stronger compliance posture from actors in the maritime industry, including shippers, brokers, insurers, providers of oil and gas services, and port authorities.[145]

Beginning in 2020, for example, the Department of State encouraged countries with flag registries to join the Registry Information Sharing Compact (RISC), an information-sharing arrangement established by the flag registries of several states to encourage better information-sharing about suspicious vessels.[146] OFAC, the Department of State, and the U.S. Coast Guard highlighted the RISC in their global maritime guidance.[147] The UN Panel of Experts for the DPRK and the research community continue to highlight the ways in which proliferation networks try to evade such scrutiny and the need for such coordinated efforts to grow substantially.

Emerging Technologies

The United States understands that civilian and military technology advancements can have profound implications for CPF. U.S. adversaries are tracking and driving developments in emerging technologies across the nuclear, chemical, and biological space and are seeking any opportunity to expand their capabilities. Emerging technologies in a variety of realms have several potential military applications. This includes novel life sciences research that may produce new biological agents or chemical agents with a potentially offensive capability. The COVID-19 pandemic has generated increased attention in the biological space, particularly on applications of life sciences research to biological warfare capabilities.

141 This is separate, of course, from the firms who knowingly engage in these activities because the vast profit is worth engaging in criminal activity (including violation of international law).

142 A recent example of an enforcement action against a shipping company is: Department of the Treasury, Office of Foreign Assets Control, "Settlement Agreement between the Department of the Treasury's Office of Foreign Assets Control and Eagle Shipping International (USA) LLC," (Jan. 27, 2020), https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20200127.

143 Department of the Treasury, "Treasury Designates Shipping Network Engaged in Ship-to-Ship Transfers with North Korean Vessels," (Aug. 30, 2019), https://home.treasury.gov/news/press-releases/sm762.

144 "Taiwan tells U.S. it is complying with North Korea sanctions," *Reuters*, (May 19, 2020), https://www.reuters.com/article/us-northkorea-missiles-taiwan-usa/taiwan-tells-u-s-it-is-complying-with-north-korea-sanctions-idUSKBN22V0F6; and "Taiwan inspects port, tells shippers to follow North Korea sanctions," *Reuters*, (Oct. 8, 2020), https://www.reuters.com/article/northkorea-taiwan/taiwan-inspects-port-tells-shippers-to-follow-north-korea-sanctions-idINKBN26T14M.

145 United Kingdom, HM Treasury, Office of Financial Sanctions Implementation, *Maritime Guidance: Financial sanctions guidance for entities and individuals operating within the maritime shipping sector*, (December 2020), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/948299/OFSI_Guidance_-_Maritime_.pdf.

146 Led, as of May 2020, by Liberia, Panama, and the Marshall Islands.

147 Maritime Advisory, p. 12.

Future Proliferation Trends

The U.S. CPF regime has focused on the threat actors identified in the 2022 and 2018 NPFRA because their pursuit of WMD capabilities has direct consequences for U.S. national security (as well as U.S. allies and partners). It should not be assumed that, going forward, this assessment of the threat would remain static. The eroding norms around the proliferation and use of some of these weapons, marked by Syria's and Russia's repeated use of chemical weapons and the DPRK's use of a chemical weapon at the Kuala Lumpur airport in Malaysia, may translate into the fact that some countries that were previously not interested in pursuing their own capabilities may choose to do so in the future as a preemptive or defensive measure. Many of these countries will not be U.S. adversaries per se, and in fact, many of them potentially could be close U.S. partners or allies. If they feel these capabilities are required, they may pursue them on a clandestine basis, using many of the same methodologies cited in the NPFRA. These actions will have implications for the U.S. CPF regime, which has prioritized the activities of the countries highlighted in this risk assessment.

CONCLUSION

As this assessment has demonstrated, the threat actors who try to exploit the U.S. financial system and other sectors to raise and move revenue or to acquire specific proliferation-related goods and technology continue to adapt their methods for evading the scrutiny of existing AML/CFT/CPF programs. These networks operate their own illicit global supply and financing chains throughout the global financial system. The United States sits at the center of that system and consequently faces a sophisticated PF threat through global financial institutions and the broad use of the dollar.

Since the publication of the 2018 NPFRA, the threat actors have remained largely consistent, but the geographic breadth of their activities has expanded, as they continue to create front and shell companies in multiple jurisdictions. They also continue to exploit the maritime sector, hiding illicit activity in the larger arena of global commerce. Many of these threat actors, particularly the DPRK, continue to develop their significant cyber capabilities to evade sanctions for the purposes of furthering the development of their nuclear weapons and ballistic missile capabilities. These techniques include exploitation of the expanding virtual asset sector. Those with mature WMD programs, such as China and Russia, are attempting to augment their existing capabilities by illicitly acquiring U.S.-origin technology.

The financing of proliferation will remain a key national security threat to the United States, as well as to international peace and security more broadly. In response to the nature of these threats, the United States maintains a strong regulatory framework that prioritizes countering PF, and its private sector demonstrates a strong awareness of PF as part of existing AML/CFT or sanctions compliance programs. Law enforcement is committed to robust information sharing with the private sector (particularly financial institutions) to aid investigations and prosecutions.

However, the centrality of the United States to the global financial system and trade transactions, as well as its advanced manufacturing base, continue to make it vulnerable to PF risk. As this assessment has discussed, this vulnerability is acute in the correspondent banking relationships that U.S. financial institutions maintain with banks around the world, among other things. While PF networks are advanced, this residual risk remains manageable if the United States maintains a mature and robust framework for assessing and mitigating PF and enhances key aspects of that regime, including the transparency of beneficial ownership information.

LIST OF ACRONYMS

ACH	Automated Clearing House
AEC	Anonymity-Enhanced Cryptocurrencies
AERO	Advanced Engineering Research Organization
AIS	Automatic Identification System
AML	Anti-Money Laundering
AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism
BSA	Bank Secrecy Act
BSA/AML	Bank Secrecy Act / Anti-Money Laundering
CBDC	Central Bank-Issued Digital Currencies
CBP	U.S. Customs and Border Protection (Department of Homeland Security)
CBW Act	Chemical and Biological Weapons Control and Warfare Elimination Act of 1991
CDD	Customer Due Diligence
CFTC	Commodity Futures Trading Commission
CIP	Customer Identification Program
CMP	Civil Monetary Penalty
CNC	Computer Numerical Control
CPF	Countering Proliferation Financing
CTR	Currency Transaction Report
CVCs	Convertible Virtual Currencies
CWC	Chemical Weapons Convention
DeFi	Decentralized Finance
DHS	Department of Homeland Security
DOJ	Department of Justice
DPRK	Democratic People's Republic of Korea
eCNY	Digital Yuan
EDD	Enhanced Due Diligence
EU	European Union
FATF	Financial Action Task Force
FBAs	Federal Banking Agencies
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FinCEN	Financial Crimes Enforcement Network (U.S. Department of the Treasury)

FRB	Board of Governors of the Federal Reserve System (or "Federal Reserve Board")
FTB	Foreign Trade Bank (of DPRK)
GTO	Geographic Targeting Order
IBK	Industrial Bank of Korea
IBKNY	Industrial Bank of Korea New York Branch
IC	Intelligence Community
HSI	U.S. Immigration and Customs Enforcement Homeland Security Investigations (U.S. Department of Homeland Security)
IEEPA	International Emergency Economic Powers Act
IMO	International Maritime Organization
IP	Internet Protocol
IRGC	Islamic Revolutionary Guard Corps
IRISL	Islamic Republic of Iran Shipping Lines
IRS-CI	Internal Revenue Service-Criminal Investigation
IT	Information Technology
ML/TF	Money Laundering/Terrorist Financing
MMIC	Monolithic Microwave Integrated Circuit
MSB	Money Services Business
M/T	Motor Tanker
MTIG	Multi Technology Integration Group EOOD
NCUA	National Credit Union Administration
NPT	Treaty on the Non-Proliferation of Nuclear Weapons
NWPU	Northwestern Polytechnical University
OCC	Office of the Comptroller of the Currency
OFAC	Office of Foreign Assets Control (U.S. Department of the Treasury)
OIA	Office of Intelligence and Analysis (U.S. Department of the Treasury)
OPCW	Organisation for the Prohibition of Chemical Weapons
PAEC	Pakistan Atomic Energy Commission
PF	Proliferation Financing
PII	Personal Identifiable Information
P2P	Peer-To-Peer
RGB	Reconnaissance General Bureau
RISC	Registry Information Sharing Compact
SAR	Suspicious Activity Report
SCB	Standard Chartered Bank

SEC	Securities and Exchange Commission
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TFI	Terrorism and Financial Intelligence (U.S. Department of the Treasury)
TFFC	Terrorist Financing and Financial Crimes (U.S. Department of the Treasury)
UAE	United Arab Emirates
UAVs	Unmanned Aerial Vehicles
UNSCR	UN Security Council Resolution
VASP	Virtual Asset Service Provider
VNITF	All-Russian Scientific Research Institute of Technical Physics
WMD	Weapons of Mass Destruction


THE DEPARTMENT OF THE TREASURY
1789