ACAMS

SANCTIONS SPACE

WHITE PAPER

NORTH KOREA'S MISSILE TESTS: THE RESPONSIBILITY OF THE GLOBAL FINANCIAL SYSTEM AND THE URGENT NEED FOR CONCRETE ACTION

Background

In September, the Democratic People's Republic of Korea (DPRK) tested a variety of new weapons, including its first hypersonic missile, its first ballistic missile delivery system mounted on a train, and new long-range cruise missiles.[1] In the same weeks, South Korea tested a powerful submarine-launched ballistic missile and announced five different types of new weapons and technologies to counter regional threats.[2]

This is not the first time that tensions have run high in the Korean peninsula; however, the DPRK's regular development of new technologies and weaponry inevitably adds novel layers of complexity in the defense and response systems of South Korea and its allies, especially the US, increasing the likelihood of potential confrontation.[3]

One thing is clear: despite fifteen years of international sanctions aimed at isolating the DPRK economy, the country's regime has continued to develop and foster its nuclear capabilities, while maintaining active nuclear reactors, as recently confirmed by the International Atomic Energy Agency (IAEA) and satellite images.[4] The latest UN Panel of Experts (UNPOE) report on the DPRK, published on October 4, 2021, states clearly that there has been no "appreciable decline" in the DPRK access to global financial institutions.[5]

[1] Foreign Policy (2021), New Cruise Missile Gives North Korea Lethal Capability (foreignpolicy.com); CNN (2021) North Korea says it fired new long-range cruise missiles, according to state media (edition.cnn.com); NK Pro (2021), North Korea's new hypersonic missle and it's likely implications (nknews.org)

[2] NK News (2021) Photos: South Korea's new SLBM, long-range, supersonic and ballistic missiles (nknews.org)

[3] Foreign Affairs (2021), North Korea's Nuclear Family (foreignaffairs.com)

[4] IAEA (2021), IAEA Director General's Introductory Statement to the Board of Governors (iaea.org); 38 North (2021), North Korea's Yongbyon Nuclear Complex: More Evidence the 5 MWe Reactor Appears to Have Restarted (38north.org)

[5] UN (2021), S/2021/777 - E - S/2021/777 (undocs.org)

UNSC resolutions impose wide restrictions on trade with the DPRK.

In the past fifteen years, the global financial system has played (mostly unwittingly) a major role in facilitating the transfer of strategic and other prohibited goods to the DPRK. This paper presents the measures in place to restrain the DPRK economic activities and examines existing gaps in the global financial system which have allowed the country to circumvent international sanctions and expand its nuclear capabilities. Finally, the paper addresses the evolving challenges of countering the DPRK proliferation efforts, including cyber threats and cryptocurrencies.

The International System's Efforts to Contain the DPRK Nuclear Developments

UN Security Council Resolutions

Since 2006, the UN Security Council (UNSC) has adopted nine resolutions imposing increasingly strict trade and financial sanctions on the DPRK, in response to the country's nuclear and missile activities.[6] These resolutions are the most solid and vigorous international measures adopted to curtail the DPRK nuclear weapons development program, and effectively limit the regime's financial resources.

UNSC resolutions impose wide restrictions on trade with the DPRK. They establish that states, and consequently private sector firms, shall prohibit direct and indirect supply, sale, or transfer of aviation fuel, condensed and natural gas liquids, crude oil, luxury goods, helicopters and vessels, refined petroleum products, and other manufacturing goods to the DPRK. UNSC resolutions also prohibit states from purchasing DPRK coal, iron and iron ore, lead and lead ore, precious metals and rare earth minerals, other metals, seafood, and other manufacturing goods. Moreover, countries are prohibited from selling or buying items from the DPRK related to weapons of mass destruction (WMD) and dual use items, all arms, and any item contributing to military capabilities (excluding food or medicine).[7]

In terms of financial and economic sanctions, UNSC resolutions introduced an asset freeze, which covers funds and other resources (including intangible assets) owned or controlled by designated persons or entities. UNSC resolutions also establish that states shall prohibit:[8]

- DPRK banks from opening new branches, subsidiaries, or representative offices in their territories
- Their financial institutions from taking ownership interest in DPRK banks, or establishing/maintaining correspondent relationships such as joint ventures with DPRK banks
- The provision of financial services, or the transfer of any assets or resources (including bulk cash) that could contribute to prohibited activities, by freezing assets and enhancing monitoring

[6] Arms Control Association (2018), UN Security Resolutions on North Korea (armscontrol.org)
[7] Carnegie Endowment for International Peace, Making Sense of UN Sanctions on North Korea(carnegieendowment.org)
[8] Subject to exceptions approved by the 1718 Sanctions Committee in advance

- The provision of public and private financial support for trade with the DPRK
- Their financial institutions from operations such as opening new representative offices or subsidiaries, or bank accounts in the DPRK
- The opening, maintenance, and operation of all joint ventures or cooperative entities, new and existing, with DPRK entities or individuals by their nationals or in their territories

States are required to close existing representative offices, subsidiaries, or bank accounts in the DPRK, and repatriate to the DPRK all DPRK nationals earning income as well as all DPRK government safety oversight attachés monitoring DPRK workers abroad.

Financial Action Task Force Recommendations

In 2008, the Financial Action Task Force (FATF) – the global standard-setter on combating financial crime – expanded its mandate to include proliferation financing in addition to money laundering and terrorist financing. In 2012, FATF adopted its "40 Recommendations" – principles which outline how countries can take effective countermeasures against financial crime. FATF recommendations are non-binding, although countries have made a political commitment to observe them.[9]

Recommendation 7 was introduced to ensure the consistent and effective implementation of UNSC targeted financial sanctions by states, de facto reinforcing the international sanctions framework against the DPRK.[10]

In October 2020, FATF took further steps to strengthen states' implementation of UNSC targeted financial sanctions by announcing amendments to its Recommendations 1 and 2, and their respective interpretative notes. Countries and private sector firms are now required to assess their exposure to proliferation financing risk, and take appropriate mitigating measures, including the enhancement of domestic coordination.[11] In June 2021, FATF published its final *Guidance on Proliferation Financing Risk Assessment and Mitigation* to support the efforts of states in complying with proliferation financing rules.

Unilateral/Autonomous Sanctions

In addition to the concerted actions taken by international organizations, the US have introduced unilateral sanctions against DPRK entities and individuals, but also against broader DPRK commercial activities.

The US Treasury and its enforcement arm, the Office of Foreign Assets Control (OFAC), have implemented a variety of far-reaching DPRK sanctions imposable on US firms, US individuals, private firms with a US subsidiary, and all parties involved in US dollar transactions independent of where in the world they are based.[12] Moreover, in 2020 the US Financial Crimes Enforcement Network (FINCEN), part of the US Treasury, published a number of advisories

[9] FATF (2004), The 40 Recommendations (fatf-gafi.org)
[10] FATF (2021), International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation – The FATF Recommendations (fatf-gafi.org)
[11] FATF (2020), Outcomes FATF Plenary (fatf-gafi.org)
[12] U.S. Department of the Treasury, North Korea Sanctions (home.treasury.gov)

At the international level, DPRK sanctions have evolved to target a comprehensive list of entities, individuals, and economic activities.

related to the DPRK proliferation efforts and addressed to the private sector, which essentially require firms to introduce broader compliance efforts to detect DPRK illicit activities.[13]

In April 2020, OFAC introduced a number of amendments to expand DPRK sanctions, including a list of additional activities involving North Korea that may be subject to secondary sanctions, namely sanctions on parties with no US nexus that engage in trade or financial transactions with North Korea. OFAC also introduced new restrictions on the opening or maintenance of US correspondent accounts, for companies that are found to have provided significant financial services to persons subject to the DPRK autonomous sanctions regime.[14]

To be effective, international sanctions need to be coherent and consistently applied by states.

US unilateral sanctions are controversial, and their legality in international law is disputed.[15] However, they do represent a relatively effective tool in limiting DPRK proliferation activities due to their extensive extraterritorial reach, which means that they apply to most companies around the world who deal with the DPRK and have some sort of exposure to either the US, the US dollar (the privileged currency for international trade) or, as per recent amendments, no US exposure at all.

The Gaps in the System: How Governments and the Global Financial Sector can Make DPRK Sanctions Effective

At the international level, DPRK sanctions have evolved to target a comprehensive list of entities, individuals, and economic activities. At the national level, the US (but also some of its allies, such as the European Union) have imposed strict and wide-ranging unilateral measures against the DPRK, with far-reaching consequences on private sector firms and individuals.[16]

Despite these considerable policy efforts, the DPRK continues to maintain access to the international financial system and trade prohibited goods. This section of the paper explores some of the reasons why Pyongyang has been able to keep its revenues and weapons development program going, notwithstanding a proactive international effort to isolate it from the global economy.

1. Inconsistent Implementation of UNSC Resolutions and FATF Recommendations

To be effective, international sanctions need to be coherent and consistently applied by states. A single leak in the system is sufficient to significantly dilute the achievements of many, and as the UNPOE on North Korea periodically denounces, **there are serious weaknesses in states' actual implementation of the UNSC resolutions on the DPRK.**[17] This is due primarily to a lack of sophisticated understanding of what the UNSC resolutions establish, but also to limited resources, capabilities, and sometimes, political will.

[13] FinCen, Advisories (fincen.gov)
[14] Comply Advantage, North Korea Sanctions Regulations: What Have The US Imposed on North Korea? (complyadvantage.com) ; Dow Jones, What are Secondary Sanctions? (dowjones.com)
[15] Law Explorer (2015), Unilateral Sanctions in International Law: A Quest for Humanity (lawesplores.com)
[16] RAND Corporation (2019), DPRK Sanctions: Countering DPRK Proliferation Activities (rand.org)
[17] UNSC (2021), (undocs.org)

- Countries are required to submit national implementation reports of UNSC resolutions to the UN. However, the latest UNPOE report on the DPRK, published in October 2021, noted that despite an increase in overall reporting, 127 states (66%) have not yet reported on their implementation of the most recent UN resolution on the DPRK, UNSC resolution 2397. This resolution was adopted almost four years ago, on December 22, 2017.[18] Moreover, the report found that the response rate of members states to the UNPOE inquiries is less than 50%, and the numbers are even lower for legal entities and individuals. [19]

- In one of its reports, published in March 2021, the UNPOE found during its investigations that some countries had published implementation reports declaring full compliance with the DPRK UNSC resolutions which later turned out to be inaccurate. In fact, DPRK proliferation networks continue to operate in those jurisdictions.[20]

- The poor implementation of UNSC targeted sanctions can be observed also in the FATF consolidated assessment ratings – namely an overview of the ratings that assessed countries obtained for effectiveness and technical compliance in their mutual evaluation reports.[21] The latest consolidated assessment ratings, published on September 16, 2021, indicate that while 51% of countries are technically compliant or largely compliant with Recommendation 7, only 2% of countries are highly effective in the implementation of Recommendation 7 in practice, while the majority of countries (80%) scored low or moderate in effectiveness.

- This means that private sector firms, including financial institutions operating in countries with low or moderate effectiveness ratings, are very unlikely to have developed sophisticated capabilities in detecting DPRK networks.

Recommendation

Countries need to step-up their efforts to ensure that the UNSC resolutions and FATF recommendations are correctly implemented and effective at the national level.

2. Easy Access to Shell, Front Companies, and Nominee Directors

The common denominator of all the DPRK proliferation networks uncovered to date is the widespread abuse of seemingly legitimate financial corporate structures. DPRK designated government and commercial entities have developed a refined and complex network of shell and front companies, intermediaries, and facilitators in multiple jurisdictions, who effectively allow the regime to evade international sanctions and maintain its business operations intact.[22]

[18] UNSCR (2017), Security Council Resolution 2397 (unscr.com)
[19] UN (2021), S/2021/777 - E - S/2021/777 (undocs.org)
[20] UNSC (2021), (undocs.org)
[21] FATF, Consolidated assessment ratings (fatf-gafi.org)
[22] CNBC (2020), Secret documents show how North Korea launders money through U.S. banks (cnbc.com) ; RUSI, Project Sandstone (rusi.org)

A key challenge for financial institutions is the identification of front and shell companies engaging in sanctions evasion activities, as they often present the same characteristics as legitimate businesses, especially at the on-boarding stage.

- While the easiness to do business and the ability to set up companies in a short period of time without excessive bureaucratic hurdles is beneficial for enterprises, **lax due diligence, and overall poor compliance with international regulations from the part of company service providers and other designated non-financial businesses and professions (DNFBPs)** continue to pose a serious challenge to the integrity of the financial system, as demonstrated also by the recent publication of the Pandora Papers.[23]

- Moreover, the **lack of easily accessible and verified beneficial ownership registers** in most countries make it very difficult for private sector firms to meaningfully and independently confirm the veracity of client information.[24] The UNPOE in its latest report found that DPRK sanctions evasion networks have on multiple occasions taken advantage of jurisdictions with opaque corporate registry processes and non-public or unverified beneficial ownership information to conceal their operations;[25] these include major global financial centres, such as London and Hong Kong.[26] In this regard, the recent FATF public consultation for the potential amendments to Recommendation 24 on the transparency of beneficial ownership is a welcomed initiative, relevant also in the fight against proliferation networks.[27]

Another key challenge is the identification of nominee directors and intermediaries.

A key challenge for financial institutions is the **identification of front and shell companies** engaging in sanctions evasion activities, as they often present the same characteristics as legitimate businesses, especially at the on-boarding stage.

- While global banks have increasingly adopted more **sophisticated due diligence procedures and network analysis tools**, small and medium sized financial institutions often have limited technological capabilities to enhance their onboarding process. Moreover, the principle of a risk-based approach to financial crime means that in practice firms will not thoroughly investigate entities which do not exhibit explicit red flags. The establishment of **transparent corporate and beneficial ownership registers** would allow the private sector to have wider and easier access to information relevant for the identification of sanctions evasion networks. Open corporate registers may not eliminate the threat posed by DPRK shell and front companies completely, but they would create an ecosystem where DPRK sanctions evasion networks spend more resources to hide their links to designated entities and individuals.

Another key challenge is the **identification of nominee directors and intermediaries**. DPRK sanctions evasion networks have traditionally benefitted from the support of ideologically affiliated entities and associates, however in the past few years there has also been an increase in opportunistic businessmen and conspirators, who trade or deal with the DPRK for purely commercial profit.

[23] Transparency International UK (2017), Hiding In Plain Sight: How UK Companies Are Used To Launder Corrupt Wealth (transparency.org.uk); Basel Institute on Governance (2021), Basel AML Index 2021: 4 things holding back the global fight against money laundering (baselgovernance.org); ICIJ (2021), Pandora Papers (icij.org)
[24] Transparency International (2021), 404 Beneficial Owner Not Found: Are EU Public Registers In Place & Really Public? (transparency.org)
[25] UN (2021) S/2021/777 - E - S/2021/777 (undocs.org)
[26] NK Pro (2017), London calling: UK shell companies in North Korea's networks (nknews.org) ; Kharon, North Korea Leverages Hong Kong Corporate Law Conducts Cyberattacks, U.N. Panel Finds (brief.kharon.com)
[27] FATF, Revisions to Recommendation 24 - White Paper for Public Consultation (fatf-gafi.org)

DPRK sanctions evasion networks have taken advantage of the increased connectivity to move funds and recruit collaborators across different regions, without the need for face-to-face interaction.

- In September 2021, the US Department of Justice (DOJ) sentenced a US-Canadian individual to 11 years in prison, for collaborating with North Korean hackers who organized cyber-attacks against financial institutions all over the globe. According to the indictment, the culprit, who had no clear affiliation to North Korea, recruited and organized individuals in various jurisdictions to withdraw stolen cash from ATMs, and used bank accounts to launder the funds.[28] The scheme involved, amongst others, a Nigerian Instagram celebrity, whom most private firms would have struggled to associate with DPRK proliferation networks before this case became public.[29]

Recommendations

- Countries need to take strong measures, including enforcement actions against non-compliant private sector firms beyond financial institutions, to prevent the abuse of legitimate corporate structures for sanctions evasion purposes.
- Countries need to seriously consider the adoption of publicly available and verified beneficial ownership registers, given their fundamental role in the identification of illicit sanctions evasion networks.
- Corporate service providers and other DNFBPs need to duly comply with financial crime regulations and adopt stricter compliance measures for the identification of ultimate beneficial owners (UBOs) and controllers.
- Financial institutions need to have effective due diligence and know your customer (KYC) procedures. Financial institutions need to prioritize investment in advanced staff training and professional development, and the acquisition of new technologies, including network analysis tools, to boost their ability to identify proliferation networks at the onboarding stage.

3. A Fragmented Global Financial System

The globalization of the financial system has allowed financial institutions to leverage their network of correspondent banking relationships and process payments more quickly all over the world.[30]

DPRK sanctions evasion networks have taken advantage of the increased connectivity to move funds and recruit collaborators across different regions, without the need for face-to-face interaction.

Increased cooperation and the establishment of private-public partnerships has in part mitigated the financial crime risks posed by new challenges, although most public-private efforts have been dedicated to anti-money laundering and counter-terrorist financing, rather than counter-proliferation financing.[31]

[28] OCCRP (2021), Money Launderer for North Korean Hackers Sentenced to 11 Years (admin.occrp.org)
[29] U.S. Department of Justice (2021), Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe (justice.gov)
[30] BIS (2020), On the global retreat of correspondent banks (bis.org)
[31] Royal United Services Institute (2020), Five years of growth in public-private financial information-sharing partnerships to tackle crime (future-fis.com)

- Moreover, **collaboration between firms on counter-proliferation financing has particularly been lacking**, and the private sector has not been able to keep pace with the rapid growth and diversification of sanctions evasion networks. This is in part due to data privacy regulations and the absence of a clear legal framework for information sharing in the private sector, which largely discourage financial institutions from sharing information with one another or across jurisdictions.[32]
- The current situation has not only led to a massive **replication of efforts within the financial industry** (with multiple financial institutions investigating the same sanctions evasion networks from different angles), but it has also prevented financial institutions from "joining the dots" and identifying DPRK sanctions evasion networks more efficiently and comprehensively. It is important to keep in mind that financial institutions have limited ability to trace payments, as a bank can only see the transactions it processes on behalf of its clients and has no visibility on what happens once the money is sent to the account of an entity or individual in another bank. In this regard, the Monetary Authority of Singapore (MAS) recent initiative to create a digital platform for financial institutions to share information on high-risk clients and transactions represents a very positive attempt to increase private sector cooperation to fight financial crime.[33]

Recommendations

- Public-private partnerships should be extended beyond anti-money laundering and counter-terrorist financing, to also cover the exchange of information on specific counter-proliferation financing threats.
- Countries and international organizations should take practical steps to enhance the information sharing legal and operational framework, to allow private sector firms to exchange information on proliferation networks, typologies, and indicators rapidly and in a safe environment.
- Private sector firms should proactively support further private-private collaboration to enhance the effective detection of sanctions evasion networks and avoid duplication of efforts.

4. Ability to Trade Strategic Goods

DPRK sanctions evasion networks have consistently taken advantage of how relatively easy it is to conceal the trade of strategic and other prohibited goods in the current global trade and financial system. Financial institutions rely heavily on the information provided by the client or associated parties, and therefore have limited access to independent and verified information concerning the underlying goods being traded.[34]

[32] FATF, FATF Guidance – Private Sector Information Sharing (fatf-gafi.org)
[33] MAS (2021), MAS and Financial Industry to Use New Digital Platform to Fight Money Laundering (mas.gov.sg)
[34] U.S. Department of the Treasury (2020), Sanctions Advisory for the Maritime Industry, Energy and Metals Sectors, and Related Communities (home.treasury.gov)

- In open account transactions (wire transfers), the payment method for 80% of global trade, **clients are not required to provide additional documents concerning the trade transaction**, and financial institutions have no information beyond the "description of transaction" field. Clients are not obliged to complete this field, which is often left blank or contains invoice numbers, generic statements such as "payment for goods", or other unintelligible references.[35]

- In trade finance transactions, clients are required to provide additional documents concerning the trade to financial institutions, including the bill of lading, commercial invoices, vessel name and packing lists (certificates of origin, often falsified in DPRK sanctions evasion schemes, are not always required).[36] Upon review, these documents may present inconsistencies and red flags on the legitimacy of the trade transaction. However, **DPRK sanctions evasion networks can be highly sophisticated, and capable of forging credible and coherent trade documents** with the assistance of conspirators (including as shipping companies and freight forwarders) which allow them to hide the strategic nature of the good and the origin/final destination.[37]

- Illicit actors also heavily rely on the **inexperience and lack of training** of analysts reviewing trade finance transactions and KYC files, especially in financial institutions with less mature compliance programs. In fact, in the past few years DPRK sanctions evasion networks have shifted towards a greater use of national and local financial institutions in Asia, Europe, and the Middle East, to take advantage of their correspondent banking networks and the ability to access the global financial system with minimal oversight from major global banks.[38]

However, challenges are not limited to national and local financial institutions; global banks have also been vocal about their **difficulties in identifying strategic goods based on the various lists published by governments and international organizations.**[39]

- These lists usually include specific information concerning the name, composition, and other technical characteristics of prohibited goods. The ACAMS International Sanctions Compliance Task Force, which includes representatives from major financial institutions, recently reiterated that banks lack the technical expertise to identify the trade of strategic goods.[40]

- Significantly, some financial institutions have started to move away from strategic goods screening, acknowledging that the list-based approach for the identification of trade transactions involving strategic goods has produced very few and no valuable hits over the years.

[35] JDSUPRA (2021), Shift to Open Account Trade Highlights Evolving Risks in the Maritime Sector (jdsupra.com)
[36] MoreThanShipping.com (2013), International Trade and Documents (morethanshipping.com) ; Max Freight Forwarders, Which Countries Need a Certificate of Origin (maxfreights.com)
[37] U.S. Department of Justice (2018), (justice.gov) ; U.S. Department of Justice (justice.gov)
[38] UNSC (2021), (undocs.org) ; David Szerlip (2017), How North Korea is Using the U.S. Financial System to Evade Sanctions (linkedin.com)
[39] The Wassenaar Arrangement, On Export Controls for Conventional Arms and Dual-Use Goods and Technologies (wassenaar.org) ; European Commission (2016), Report on the EU Export Control Policy Review (trade.ec.europa.eu) ; A Resource on Strategic Trade Management and Export Controls, Overview of U.S. Export Control System (2009-2007.state.gov)
[40] ACAMS (2021), ACAMS International Sanctions Compliance Task Force Submission to FATF (acams.org)

Different sectors need to collaborate more closely to improve the identification of strategic goods trade.

Ultimately, it is very unlikely that illicit actors would openly declare the sensitive nature of the goods they trade, and financial institutions need to move towards more sophisticated technological solutions, and closer collaboration with other sectors, to identify high-risk transactions.

Recommendations

- Countries and industry associations need to closely collaborate to introduce innovative payment processing and trade solutions (e.g. blockchain), which would allow greater visibility and record-keeping of transactions.
- Countries and industry associations need to closely collaborate to ensure the private sector's access to relevant external verified databases, to enable them to independently assess the information provided by clients (e.g. certificates of origin, KYC information, past trade transactions with proliferation countries).
- The private sector, especially financial institutions, need to consistently and strategically invest in tailored staff training on proliferation financing typologies and red flags, especially in compliance investigations and trade finance departments.
- Financial institutions need to invest in bespoke technological solutions (e.g. dual-use items screening, maritime vessels screening, network analysis tools) to streamline the review of trade transactions and promptly identify high risk customers and activities.

5. Limited Cross-Sector Collaboration

Different sectors need to collaborate more closely to improve the identification of strategic goods trade. **At present, financial institutions, payment service providers, maritime companies, strategic goods manufacturers, and export control departments often work in silos**, and share very little information with each other about their respective work.[41] DPRK sanctions evasion networks know this, and take advantage of the highly scattered processes, procedures, and requirements across different sectors.

- Tactical and strategic collaboration, between the firms and government departments most vulnerable to DPRK sanctions evasion networks, would be very effective in enhancing the implementation of current counter-proliferation measures and the identification of illicit activities.
- The establishment of regular forums and exchange hubs, to share information within a secure and appropriate legal framework, would strongly increase awareness of existing loopholes in the counter-proliferation compliance system, and lead further concerted action from the public and private sector.

[41] Carnegie Endowment for International Peace (2018), Challenges With Implementing Proliferation Financing Controls: How Export Controls Can Help (carnegieendowment.org)

- Collaboration across different sectors could also be fostered at a higher level, through the exchange of sanitized case studies, red flags, and typologies of sanctions evasion networks, focusing particularly on emerging trends.

DPRK proliferation networks have demonstrated that they are very agile and capable to adapt quickly to changing environments. The private and public sector need to engage on multiple levels, and as proactively as possible within the current legal and regulatory framework, to maintain a dynamic approach to a rapidly evolving risk ecosystem. This is especially true given the DPRK's exponential increase in the use of new technologies and alternative payment methods to circumvent existing sanctions controls.

Recommendations

- Countries and international institutions need to engage with a wider array of private sector firms beyond financial institutions, including payment service providers, maritime companies, strategic goods manufacturers, and export control departments.
- National counter-proliferation agencies should interact more closely with the private sector through forums and exchange hubs, but also through training exercises and simulations aimed at identifying gaps in the counter-proliferation framework and areas for further collaboration.

Countering DPRK Proliferation Networks: Roadmap and Next Steps for the Public and Private Sector

In this paper, ACAMS has put forward the below suggestions for the public and private sector to enhance effective counter-proliferation financing measures and detect DPRK proliferation networks.

Priorities for Countries/Regions and Public-Private Partnerships

- Step-up efforts to ensure that the UNSC resolutions and FATF recommendations are correctly implemented and effective at the national level.
- Take substantial enforcement actions against non-compliant private sector firms beyond financial institutions (e.g. company service providers, DNFBPs), to demonstrate commitment to the implementation of international sanctions against the DPRK.
- Introduce publicly available and verified beneficial ownership registers to support efforts in the identification of illicit sanctions evasion networks.
- Extend public-private partnerships to include the exchange of information on counter-proliferation financing threats, red flags, and typologies.

- Take practical steps to enhance the information sharing legal and operational framework, to allow private sector firms to exchange information on proliferation networks, typologies, and indicators rapidly and in a safe environment.
- Closely collaborate with industry associations to introduce innovative payment processing and trade solutions (e.g. blockchain), which would allow greater visibility and record-keeping of transactions.
- Closely collaborate with industry associations to ensure the private sector's access to relevant external and verified databases to independently assess the information provided by clients (e.g. certificates of origin, KYC information, past trade transactions, and exposure to proliferation countries).
- Engage with a wider array of private sector firms beyond financial institutions, including payment service providers, maritime companies, strategic goods manufacturers, and export control departments.
- National counter-proliferation agencies should interact more closely with the private sector through forums and exchange hubs, but also through training exercises and simulations aimed at identifying gaps in the counter-proliferation framework and areas for further collaboration.

Priorities for the Private Sector

- Update and implement effective due diligence and know your customer (KYC) procedures, to include steps to identify some of the common strategies employed by sanctions evasion networks to avoid detection at the on-boarding stage.
- Prioritize investment for the acquisition of new technologies, including network analysis tools and sophisticated databases, to advance your organization's ability to identify proliferation networks at the onboarding stage.
- Consistently and strategically invest in tailored staff training on proliferation financing typologies and red flags, especially in compliance KYC/enhanced due diligence, transactions review, investigations, and trade finance departments.
- Proactively support and lobby for the establishment of a legal and operational framework to further private-private collaboration, and enhance the effective detection of sanctions evasion networks, while avoiding duplication of efforts across the industry.
- DFNBPs and virtual assets service providers (VASPs) should duly comply with financial crime regulations, and adopt stricter compliance measures for the identification of ultimate beneficial owners (UBOs) and controllers.

The Challenges Ahead

The challenge posed by DPRK sanctions evasion networks has become more severe in the past few years, with the advent of new technologies and alternative payment methods that allow illicit actors to raise funds and process payments outside of the traditional financial system. The private sector is vulnerable to these advancements in many crucial ways.

DPRK sanctions evasion networks have continued to flourish and innovate in the past 15 years, despite increasingly strict international sanctions to isolate the DPRK economy.

- A first vulnerability relates to the DPRK cyber program and its ability to conduct sophisticated attacks to steal funds from private sector firms, particularly financial institutions with less developed cyber security capabilities.[42] Financial institutions may not only become the target of cyber-attacks, but they may also be exploited to process payments related to cyber heists, as criminals attempt to launder the stolen funds. As mentioned in this paper, the DPRK's ability to recruit a wide array of opportunistic cyber criminals, operating all over the world, poses additional challenges for the identification of DPRK sanctions evasion networks, and requires financial institutions to think more holistically about their proliferation financing risks.[43]

- A second vulnerability relates to the DPRK networks' use of cryptocurrencies. Most financial institutions have been cautious to engage with crypto companies, however their approach will inevitably change as financial opportunities and general public use of virtual assets grow.[44] Financial institutions' greater exposure to cryptocurrencies is likely to increase exposure to DPRK sanctions evasion networks, which have long embraced the use of virtual currencies to evade strict compliance controls and launder virtual assets stolen through their cyber activities.[45] Although information on how DPRK networks use cryptocurrencies is still relatively limited, their efforts have been consistent and creative, going as far as trying to launch a start-up, for the purchase of fractional ownership interests in maritime vessels using cryptocurrencies and blockchain technology.[46]

DPRK sanctions evasion networks have continued to flourish and innovate in the past 15 years, despite increasingly strict international sanctions to isolate the DPRK economy. The DPRK recent missile tests and weaponry developments are only the latest reminder that the stakes have never been higher, and both the public and private sector need a concerted effort to be ahead of the proliferation financing curve.

About ACAMS

ACAMS is the largest global membership organization for anti-financial crime professionals, with 82,000+ members in over 175 countries/regions.

ACAMS offers two exclusive programs for sanctions professionals – the internationally recognized **Certified Global Sanctions Specialist** (CGSS) accreditation, and the **Sanctions Compliance Foundations** online certificate (new in 2021).

[42] U.S. Department of Justice (2021), Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe (justice.gov)
[43] Cybersecurity & Infrastructure Security Agency (2020), Alert (AA20-239A) FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks (us-cert.cisa.gov)
[44] Reference.Point (2021), Regulated Financial Institutions & Cryptocurrencies: Strategic, Risk Management & Regulatory Considerations, (referencepoint.com)
[45] Bank Info Security (2019), UN Report: N. Korea Targets Cryptocurrency Exchanges, Banks (bankinfosecurity.com)
[46] Recorded Future (2018), Shifting Patterns in Internet Use Reveal Adaptable and Innovative North Korean Ruling Elite(recordedfuture.com) ; U.S. Department of Justice (2020), (justice.gov)

Also available to sanctions teams and professionals is the **ACAMS Sanctions Space**, led by Dr Justine Walker and our International Sanctions Compliance Task Force. The Sanctions Space is a comprehensive and dynamic resource center, encompassing Masterclasses, Global Monthly Update briefings, authoritative white papers and a podcast series telling the stories behind the sanctions.

Learn more about sanctions at **acams.org/sanctions**

Commitment to Counter-Proliferation Financing

ACAMS is committed to raising awareness and contributing to the debate about the design and implementation of counter-proliferation financing (CPF) measures in the public and private sector. Our mission is to explore and share practical and concrete solutions to improve the effectiveness of national and international financial crime regulations.

In the past year, ACAMS – often in collaboration with our International Sanctions Compliance Task Force, which includes representatives from the private sector and think tanks – has published a number of white papers relevant to CPF, including:

- **Maritime Sanctions Compliance: Enhancing Cross Industry Cooperation and Implementation**
- **Nexus of Cyber, Ransomware and Sanctions Compliance**
- **RUSI-ACAMS Proliferation Finance Survey**
- **ACAMS International Sanctions Compliance Task Force Submission to FATF**

ACAMS has also discussed CPF topics at various occasions as part of our Global Sanctions Monthly Update.

Author: Carolina Prelazzi, Global Subject Matter Expert in Sanctions, Proliferation & AFC, ACAMS

Carolina Prelazzi joined ACAMS in September 2021, after more than four years working in the Global Financial Crime Analysis team at HSBC, focusing on sanctions evasion networks linked to North Korea and Iran.

October 2021