Typologies on the circumvention of Targeted Sanctions against Terrorism and the Proliferation of Weapons of Mass Destruction

United Arab Emirates

Issued by the Executive Office of the Committee for Goods Subject to Import and Export Control

BurDubai - Umm Hurair
1 - Khalid Bin Al Walid St
Consulates Area in the Ministry of Foreign Affairs and International Cooperation / Dubai Office

https://www.uaeiec.gov.ae/en-us/
Telephone: +971 44 040 040
Fax: +971 43574499
Email: iec@uaeiec.gov.ae

Issued on: 20 Mar 2021
Last amended: 11 May 2021

This document was developed by United Arab Emirates with the technical assistance provided by Financial Transparency Advisors.

Acronyms

DPRK	Democratic People's Republic of Korea
FATF	Financial Action Task Force
ISIL	Islamic State in Iraq and the Levant (Da'esh)
TF	Terrorism Financing
UAE	United Arab Emirates
UN	United Nations
UN Panel of experts	The Panel of Experts pursuant to UNSCR 1874 related to the Nuclear Programme of the Democratic People's Republic of Korea
UNSC	United Nations Security Council
UNSCR	United Nations Security Council Resolution
US	United States of America

Content

Introduction

The United Nations Security Council (UNSC), pursuant to Chapter VII of the United Nations Charter with the aim to maintain peace and security through its Resolutions and Sanctions Committees, mandates the implementation of various sanctions regimes. This document is focused mostly on the UNSC sanctions regimes, particularly, those related to nuclear non-proliferation of weapons of mass destruction, terrorism, and their financing.

The term *targeted financial sanctions* includes both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of individuals, entities, groups, or organization who are sanctioned. In particular, the UNSC has imposed targeted financial sanctions on individual, entities and group considered global terrorists, and to the nuclear programs of Iran and DPRK.

This document presents cases and examples from the UAE and other countries on how these sanctioned activities, persons, groups, or entities have received financing and support, therefore in violation or evading UNSC Resolutions (UNSCR) related to UNSCR 1267 (1999), 1989 (2011), 1988 (2011), 1718 (2006), 2231 (2015) and their successor resolutions. This document also presents cases related to the national UAE terrorist list in accordance with UNSCR 1373.

All information presented in this document derives from public sources. It includes a compilation of cases and situations, aiming to provide trends and methods used by sanctioned persons, groups, or entities to circumvent the UNSCR. Each public and private institution's responsibility is to implement adequate measures to prevent being misused to breach the UNSCR and duly report to the competent authorities any (attempted) circumvention.

Targeted Financial Sanctions against Terrorism

The term terrorist financing includes the provision of funds to commit terrorist activities and the support and maintenance of the person (terrorist) or the terrorist group. This term includes providing food, lodging, training, and making means available such as transportation and communication equipment. Such financing can occur with money or in kind, and funds involved can be from legal or illegal sources. The targeted financial sanctions aim to prevent the financing of terrorists.

The following are methods and cases that illustrate how terrorist groups have misused economic sectors or activities to fund their activities, in breach of sanctions. This document compiles information from documents developed by the UNSC, the United Nations Office on Drugs and Crime (UNODC), and the Financial Action Task Force (FATF).

Terrorist financing methods

In its report "Financing of the Terrorist Organization Islamic State in Iraq and the Levant (ISIL)" of 2015, FATF identified that this terrorist organization earns revenue primarily from five sources: (1) illicit proceeds from the occupation of territories, such as bank looting, extortion, control of oil fields and refineries, and robbery of economic assets and illegal taxation of goods and cash that transit territory where ISIL operates; (2) kidnapping for ransom; (3) donations including by or through non-profit organizations; (4) material support such as support associated with foreign terrorists fighters and (5) fundraising through modern communication networks[1].

The Joint Report of the Counter-Terrorism Committee Executive Directorate and the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015) concerning Islamic State in Iraq and the Levant (ISIL) (Da'esh), Al-Qaida and the Taliban and associated individuals and entities on actions taken by the Member States to disrupt terrorist financing, prepared pursuant to paragraph 37 of UNSCR 2462 (2019), of 3 June of 2020 ("Joint Report") concludes from a questionnaire sent to all United Nations Member States that the most frequently used channels for terrorist financing are (1) the formal banking system; (2) cash smuggling; (3) the money services business; and (4) informal remitters or hawala[2].

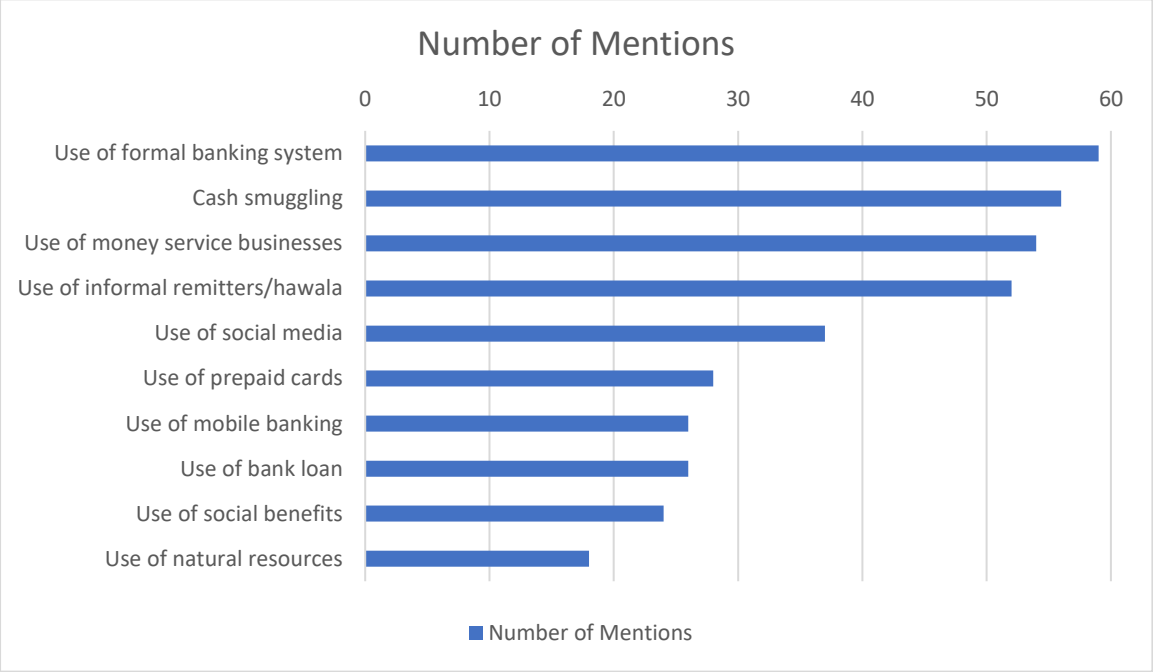
The Joint Report also accounts for the abuse of technology (including social media, prepaid cards, and mobile banking) for terrorist purposes, noting that terrorist financing was facilitated by recent developments in mobile payments and the anonymity of money transfers and illicit donations via crowdfunding platforms.[3]

The UNSC notes that terrorists and terrorist groups raise funds through various means, including exploiting natural resources, kidnapping for ransom, and links to organized crime and drug trafficking. The Joint Report notes the potential for terrorism financing through the construction and real estate sectors, the use of shell companies to

[1] Financial Action Task Force, 2015, p. 12
[2] United Nations Counter-Terrorism Committee Executive Directorate and the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015) , S/2020/493, p. 16.
[3] United Nations Counter-Terrorism Committee Executive Directorate and the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015) , S/2020/493, p. 17.

conceal cash, the use of non-profit organizations, and trade-based terrorism financing.[4]

Figure-1: Methods most frequently used by terrorist financiers



Source: United Nations Counter-Terrorism Committee Executive Directorate and the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015), S/2020/493, p. 16.

Banking services

The formal banking system is vulnerable to the circumvention of sanctions related terrorist financing because all financial product and services, could be misused or vulnerated to finance terrorism, in addition to the difficulty of distinguishing between legitimate and illegitimate low-cost transactions and detecting indirect transactions. Unfortunately, transaction-monitoring programs are often unable to identify terrorism financing.[5]

Continued access to bank accounts by Foreign Terrorist Fighters

Foreign terrorist fighters are individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training, including in connection with armed conflict[6].

[4] United Nations Counter-Terrorism Committee Executive Directorate and the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015) , S/2020/493, p. 17.
[5] United Nations Counter-Terrorism Committee Executive Directorate and the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015) , S/2020/493, p. 16.
[6] Security Council resolution 2178 (2014) S/RES/2178

According to financial information, terrorist financing risks were discovered regarding foreign cash withdrawals via ATMs made in areas located near territories where ISIL operates by unknown individuals. These withdrawals were taken from US-based bank accounts using a check card. Another terrorist financing risk identified was the existence of large deposits into bank accounts followed by immediate foreign cash withdrawals in areas located near to territories where ISIL operates. This information reveals the terrorism financing risks posed by the continued ability of the individuals who are believed to have travelled to areas occupied by ISIL to reach their bank accounts in their home countries.[7]

Money remitters

Along with the banking sector, the remittance sector has been exploited to move illicit funds and is also vulnerable to Terrorist Financing. In countries where access to banking services is limited, remittance providers may be the primary financial institution through which consumers can engage in cross-border funds transfer activity. Remittance providers are especially vulnerable to abuse for Terrorist Financing where they are unregulated, not subject to appropriate AML/CFT supervision, or where they operate without a license (thus working without any AML/CFT controls)[8].

MVTS for TF

The UAE authorities arrested a person for transferring money to a jihadist group in the Philippines who pledged allegiance to ISIL Terrorist Organization . The suspect received money from persons from different places in the UAE using Exchange Bureaus. The money was sent through multiple payments and in small amounts so that the UAE authorities would not identify them. The investigation determined that the transferred funds' total value accounted for AED 120,000 (one hundred and twenty thousand dirhams).

Hawala and Other Similar Service Providers (HOSSP)

There are several reasons why HOSSPs poses a terrorist financing vulnerability, including a lack of registration and supervision, settlement across multiple jurisdictions through value or cash outside of the banking system, the use of businesses that are not regulated financial institutions, the use of net settlement and the commingling of licit and illicit proceeds[9].

Hawala used for TF

Funds sent to Boko Haram

The UAE authorities arrested seven (7) Nigerian persons involved in fundraising to support Boko Haram Terrorist Movement affiliated with the ISIL Terrorist Organization in West Africa. The suspects used Exchange Houses and Hawala services providers to send and receive money, as well as the method of small payments to avoid raising

[7] Financial Action Task Force, February 2015, p. 23
[8] Financial Action Task Force, October 2015, p.26
[9] Financial Action Task Force, October 2013, p. 41

suspicions and monitoring by the competent authorities in the UAE. In this case, the UAE authorities seized AED 3,000,000 (three million dirhams).

Funds sent to ISIL in Afghanistan

The UAE authorities arrested nine (9) persons who were members of the ISIL Terrorist Organization that received military training on the use of weapons in Khorasan, Afghanistan. The suspects were involved in moving, transferring, and sending funds through a Hawala Service provider using tailor shops. They were also exchanging the currency into US dollars and handing it over to persons with Afghan nationalities for them to send them to Afghanistan. The transferred funds' value reached AED 855,000 (eight hundred and fifty-five thousand dirhams) and USD 14,000 (fourteen thousand US dollars).

Funds sent to ISIL in the Philippines

The UAE authorities arrested a number of persons involved in the transferring of money to the jihadist groups in the Philippines who pledged allegiance to ISIL Terrorist Organization. The suspects obtained cash in the UAE through Hawala service providers which were then sent to the jihadist groups in the form of payments. In the first case, the transferred funds' value reached AED 120,000 (one hundred and twenty thousand dirhams) whereas, in the second case, the UAE authorities determined that the transferred funds' value reached AED 50,000 (fifty thousand dirhams).

Online payment facilities

Online payment facilities offered through dedicated websites or communications platforms make it easy to transfer funds electronically between parties. Funds transfers are often made by electronic wire transfer, credit card, or alternate payment facilities available via services such as PayPal or Skype.[10]

Online payment facilities can be vulnerable to identity theft, credit card theft, wire fraud, stock fraud, intellectual property crimes, and auction fraud. The following cases illustrate how online payment facilities are vulnerable to circumvent sanctions related to terrorism.

Fundraising through the Internet

Information obtained by way of Intelligence indicated that some individuals associated with ISIL have called for donations via Twitter and have asked the donors to contact them through Skype. The donors would be asked to buy an international prepaid card (e.g., a credit for a mobile line or to purchase an application or other program which stores credit) and send the number of the prepaid card via Skype. The fundraiser would then send the number to one of his followers in a close country from Syria and sell the card number at a lower price and take the cash that was afterward provided to ISIL[11].

PayPal accounts used for fundraising .

The United Kingdom case against Younis Tsouli: Profits from stolen credit cards were laundered by several means, including transfer through e-gold online payment

[10] United Nations Office on Drugs and Crime, 2012, p. 7
[11] Financial Action Task Force, February 2015, pp. 24-25

accounts, which were used to route the funds through several countries before reaching their intended destination. The laundered money was used both to fund the registration by Tsouli of 180 websites hosting Al-Qaida propaganda videos and to provide equipment for terrorist activities in several countries. Approximately 1,400 credit cards were used to generate approximately £1.6 million of illicit funds to finance terrorist activity[12].

The use of social media for promoting terrorist activities

The UAE authorities investigated persons who adopted terrorist and extremist ideas. They use information technology to search for a way to organize terrorist organizations and send money to terrorists and ISIL. One of the suspects, of Emirati nationality, adopting the ideology of ISIL, was caught communicating with terrorist persons from abroad using Social Media platforms. He had also exchanged videos and photos endearing and promoting ISIL and transferred these clips to colleagues for promotion. Also, through his communication via social media, he communicated with a person from outside the UAE who requested financial assistance to join the ISIL. The suspect sent an amount of money to help this other person join ISIL through an Exchange house, and he had also provided an amount of money to two (2) of his colleagues to help them prepare for travel so that they could join the ISIL.

The misuse of Facebook

A person of Turkish nationality was arrested in the UAE for aiding Al-Nusra Front and its affiliated factions in Syria, with the aim of providing logistical support to the armed groups in Syria and the factions of the Al-Nusra Front in Syria. The suspect also supported the fighters in the Turkmen Brigade in Syria and provided transportation to the Turkish border. He confessed that he used his account on the social networking site "Facebook" to collect assistance and fundraise to support Al-Nusra Front and the Armed Brigades in Syria. Also, he activated the telegram platform to promote terrorist organizations by publishing videos and pictures endearing and promoting the organizations. The value of the money raised was approximately TRY 850,000 (eight hundred and fifty thousand Turkish liras).

The misuse of WhatsApp.

Based on an investigation carried out by the UAE authorities, it was identified that there are some persons residing in the UAE who support ISIL by using various means. Accordingly, a person of Syrian nationality was arrested for facilitating the transfer of funds in favour of members of the Al-Nusra Front Organization. The suspect used the WhatsApp platform to tell a friend about the location of the money and requested him to send it through an Exchange Bureau to another person who is in Turkey, who is a member of the Al-Nusra Front. The amounts of money that he transferred accounted for SAR 10,000 (ten thousand Saudi riyals).

The misuse of non-profit organizations (NPOs)

Individuals and organizations seeking to fundraise for terrorism and extremism support may attempt to disguise their activities by claiming to be engaged in legitimate

[12] United Nations Office on Drugs and Crime, 2012, p. 7

charitable or humanitarian activities. They may establish NPOs for these purposes[13]. The following cases illustrate how NPOs are vulnerable to be misused to circumvent sanctions related to Terrorism.

Support for recruitment of Foreign Terrorist Fighters

On 4 November 2010, Al Rehmat Trust, an NPO operating in Pakistan, was designated pursuant to US Executive Order (EO) 13224 for being controlled by, acting on behalf of, and providing financial support to designated terrorist organizations, including al Qaida and affiliated organizations.

Al Rehmat Trust was found to be serving as a front to facilitate efforts and fundraising for an UN-designated terrorist organization, Jaish-e Mohammed (JEM). After it was banned in Pakistan in 2002, JEM, a UN 1267 designated Pakistan-based terrorist group, began using Al Rehmat Trust as a front for its operations. Al Rehmat Trust has provided support for militant activities in Afghanistan and Pakistan, including financial and logistical support to foreign fighters operating in both countries. In early 2009, several prominent members of Al Rehmat Trust were recruiting students for terrorist activities in Afghanistan. Al Rehmat Trust has also been involved in fundraising for JEM, including for militant training and indoctrination at its mosques and madrassas. As of early 2009, Al Rehmat Trust had initiated a donation program in Pakistan to help support families of militants who had been arrested or killed. In addition, in early 2007, Al Rehmat Trust raised funds on behalf of Khudam-ul Islam, an alias for JEM.

Al Rehmat Trust has also provided financial support and other services to the Taliban, including financial support to Afghanistan's wounded Taliban fighters[14].

NPO Affiliation with a Terrorist Entity

In August 2013, the US Department of the Treasury designated the Jamia Taleem-Ul-Quran-Wal-Hadith Madrassa, also known as the Ganj Madrassa, pursuant to US Executive Order (EO) 13224 for being controlled by, acting on behalf of, and providing financial support to al-Qa'ida and other designated terrorist organizations. The Ganj Madrassa is a school in Peshawar, Pakistan, that was found to be serving as a training center for and facilitating funding for UN and U.S.-designated terrorist organizations, including al-Qa'ida, Lashkar-e Tayyiba, and the Taliban. The activities of the Ganj Madrassa exemplify how terrorist groups, such as al-Qa'ida, Lashkar-e Tayyiba, and the Taliban, subvert seemingly legitimate institutions, such as religious schools, to raise and divert charitable donations meant for education to support terrorist training and violent acts. The action did not target all madrassas, which often play an essential role in improving literacy and providing humanitarian and developmental aid in many areas of the world; it only identified this specific madrassa as supporting terrorism and terrorist financing.

The Ganj Madrassa is controlled by UN-designated al-Qa'ida facilitator Fazeel-A-Tul Shaykh Abu Mohammed Ameen Al-Peshawari, also known as Shaykh Aminullah. Shaykh Aminullah was designated by both the United States pursuant to US Executive Order (EO) 13224 for being controlled by, acting on behalf of, and providing financial

[13] Financial Action Task Force, October 2015, p. 32
[14] Financial Action Task Force, June 2014, p. 46

support to designated terrorist organizations and the United Nations (UN) in 2009 for providing material support to al-Qa'ida and the Taliban.

The Ganj Madrassa serves as a terrorist training center where students have been trained to conduct terrorist and insurgent activities under the guise of religious studies. In some cases, students were trained to become bomb manufacturers and suicide bombers. Shaykh Aminullah has directed donations provided for the school to terrorist groups such as the Taliban, which use the money to fund the ongoing violence in Afghanistan[15].

Cash Smuggling

Cash continues to be a prevalent aspect of terrorist operations. While funds may be raised in several ways, they are often converted into cash to be taken to conflict zones. This is assisted by porous national borders, difficulty in detecting cash smuggling (particularly in the small amounts that are sometimes smuggled for TF purposes), and the existence of informal and unregulated economies[16].

The following cases illustrate how smuggling is used to circumvent sanction on Terrorism.

Cash Smuggling

The UAE authorities arrested a person involved in providing Yemen's Houthi Terrorist Movement with funds and assistance by sending funds estimated at AED 200,000 (two hundred thousand dirhams) with a driver who transported such cash across the land borders.

Smuggling of gold

Based on intelligence gathered by the UAE authorities, the customs authority seized a consignment of sixty (60) kilograms of gold that arrived in the UAE from the Republic of Sudan. During the investigations, it was found that this gold belonged to the Justice and Equality Movement (JEM), a group included in the United Nations Security Council Resolutions on Sudan.

Cash couriers

Over a period of three consecutive days, three individuals declared a total amount of some EUR 90.000 in cash to customs officials at the airport in Brussels. The funds are said to originate from NPO A from Germany as part of humanitarian aid in Burundi, Benin, and Zimbabwe. The three couriers are all Belgian nationals and have been living in Belgium for a long time. A Belgian coordinating body of a radical Islamic organisation transferred money to accounts held by the three individuals. Over a one year period, approximately EUR20k was withdrawn in cash, and EUR10k was transferred to Turkey.

According to the German FIU, NPO A was one of the largest Islamic organizations in Germany. NPO A is said to be linked with NPO B, which had been banned in Germany

[15] Financial Action Task Force, June 2014, p. 117
[16] Financial Action Task Force, October 2015, p. 23

for allegedly supporting a terrorist organization. All of NPO B's board members also played a significant role in NPO A.

According to information from the Belgian intelligence services, the three individuals reverenced above are known to be involved in local branches of a radical Islamic organization. Given the nature of the transactions and the links between the two NPO referenced above, Belgian authorities suspect that at least part of the funds described above could have been used to support terrorist activities.[17]

Circumventing Sanctions through Trade

Trade can be very vulnerable to circumvent sanctions against terrorism. It is challenging to identify when sanctioned persons are involved in any part of the value of chain of trade.

The following cases illustrate how sanctions can be circumvented through trade.

Trade in dual use goods.

The UAE authorities arrested a person for supplying Yemen's Houthi Terrorist Movement with 100 tons of prohibited chemicals, and cash accounted for YER 200,000 (two hundred thousand Yemeni riyals). Also, he shipped communication devices and SIM cards by smuggling them through land border crossings using forged bills of lading through a shipping office in the UAE. To smuggle them into Yemen, the substances' names were changed to be exported as permitted materials. Also, the amount of shipped substances (materials) was reduced to avoid paying taxes.

Trade of communication devises

A Yemeni national supplied Yemen's Houthi Terrorist Movement with funds, means of communication, tools, and chemicals through a shipping company. The suspect has carried out several equipment smuggling operations to Yemen through a company in the UAE with the support of a third suspect, who is Greek and of Yemeni origin. These suspects smuggle a consignment of servers and communication devices belonging to Huawei Company (six (6) wooden boxes containing servers - a large number of small cartons in it containing small black devices) in favor of the Houthis in Yemen for an amount of USD 13,000 (thirteen thousand dollars). To smuggle them, the suspect tore down the papers affixed indicating that these were communication devices and dyed the Huawei logo attached on the wooden boxes with a black dye to cover them up and not allow them to be identified. A third suspect produced and forged bills of lading with different data for the shipped devices. They were recorded in the bill of lading as computers and automobile spare parts. The aim was to facilitate importing and smuggling from one of the land border crossings in the UAE due to the prohibition to export them into Yemen. The first suspect also smuggled communication equipment, SIM cards, generators, and chemicals in favor of the Houthis.

In another similar case, another person was arrested by the UAE authorities for shipping auto spare parts and pipes, as well as wired and wireless devices (walkie-talkies) based on the guidance of the Houthi leaders.

[17] Financial Action Task Force, October 2015, p. 23

Trade of natural resources

The targeted financial sanctions imposed by the United Nations include the freezing and prohibition to provide economic resources, including natural resources to terrorists. The following are cases that show how there was an attempt to circumvent sanctions, but Authorities were able to prevent that these resources reach terrorists.

Trade of oil and derivates.

UAE authorities arrested a person for supplying Yemen's Houthi Terrorist Movement with funds and Iranian diesel. The diesel was smuggled through maritime routes from Djibouti to the Port of Al-Hudaydah in Yemen. The diesel was sold to entities affiliated with Yemen's Houthi Terrorist Movement through three (3) companies owned by the suspect that operate in the oil business. The value of the companies in Yemen is estimated at AED 255,000,000 (two hundred and fifty-five million dirhams).

Trade of Charcoal from Somalia:

Based on UN resolution no (2036) in 2012 regarding the band of charcoal from Somalia due to using charcoal for financing Alshabab terrorist group, FCA, local Customs Departments and the Executive office of Control Importing and Exporting Goods has ban importing charcoal from Somalia and monitor the trade and market for diversion of the goods. The following is the investigation findings:

1. Somalin Charcoal has diverted to several country such as Comoros and Iran
2. Counterfeited Certified of Origin
3. Counterfeited bill of Leading

UAE authorities seized the Charcoal and sold it in auctions.

The misuse of legal entities

Legal entities can be misused to circumvent sanctions by means of the characteristics of the legal type of entity, for example by using a legal entity as a shell company, or complex legal structures to obscure the beneficial owner. Another method is through the misuse of the economic activity developed by the legal entity. Trade and commercial activities are among the highly vulnerable activities for sanctions evasion related to terrorism.

The following case illustrate how legal entities can be misuse to circumvent sanctions.

The UAE authorities identified two (2) commercial companies that received funds from a third-party non-profit organization for an amount of AED 51,000,000,000 (fifty-one million dirhams) (EUR 12.4 million). These funds were transferred from the companies accounts to other accounts by way of checks and cash withdrawals. It was also found that the same companies that received money from Company (X) had also received funds from Company (Y) because these transactions were authorized by the same owners or by the same authorized signatories.

The UAE authorities found that the two companies were owned by the same individuals, and the funds were received from high-risk countries. In addition, the banking transactions of the companies that received the funds did not match their

level of revenues. Eventually, a link was found between the foreign non-profit organization and the terrorist organization (Hamas) and a suspicious relationship with the Muslim Brotherhood, an organization that is listed in the UAE's terrorist list.

The UAE authorities froze all the bank accounts of the companies in the UAE (forty-nine (49) accounts in four (4) banks) with a total of frozen funds of AED 29,000,000,000 (twenty-nine million dirhams) (EUR 7,000,000 seven million euros).

The case was referred to the court, which included fifty-nine (59) suspects, of which twenty-eight (28) legal persons and thirty-one (31) natural persons. The court ruled life imprisonment on the first suspect and ten (10) years imprisonment on the other suspects, with a fine of AED 500,000 (five hundred thousand dirhams). Also, a fine of AED 500,000 (five hundred thousand dirhams) as a penalty for incorporated companies, besides the confiscation of seized funds and the closure of the companies.

Indirectly making economic resources available.

An important aspect to prevent sanctions evasion is to have procedures in place to prevent circumventing sanctions indirectly, for example when provided goods to a customer who will then, make them available to terrorists. The following case exemplifies how this situation can happen.

Toyotas reaching ISIL

Toyota Motor Corp. found itself unwanted attention, when the Terror Financing unit of the U.S. Treasury Department had launched an inquiry into how ISIL militants were getting their hands on so many Toyotas.

ISIL propaganda videos show gunmen patrolling Syrian streets in what appear to be older and newer model white Hilux pick-ups bearing the black caliphate seal and crossing Libya in long caravans of gleaming tan Toyota Land Cruisers. When ISIS soldiers paraded through the center of Raqqa, more than two-thirds of the vehicles were the familiar white Toyotas with the black emblems. There were small numbers of other brands including Mitsubishi, Hyundai and Isuzu.

Toyota's own figures show sales of Hilux and Land Cruisers tripling from 6,000 sold in Iraq in 2011 to 18,000 sold in 2013, before sales dropped back to 13,000 in 2014.

Questions about the ISIL use of Toyota vehicles have circulated for years. In 2014, a report noted that the U.S. State Department delivered 43 Toyota trucks to Syrian rebels. A report in an Australian newspaper said that more than 800 of the trucks had been reported missing in Sydney between 2014 and 2015, and quoted terror experts speculating that they may have been exported to ISIS territory.

Attempts to track the path of the trucks into ISIL hands has proven complicated for U.S. and Iraqi officials. ISIL groups may be getting the vehicles in several ways, one theory posits that the vehicles are being stolen from Syrian rebels or other sources

overseas and smuggled into the conflict zone. Another is that ISIL sympathizers are simply buying up the trucks and shipping them to the militants[18].

[18] ABC news. US Officials Ask How ISIS Got So Many Toyota Trucks. 6 October 2015. Available at https://abcnews.go.com/International/us-officials-isis-toyota-trucks/story?id=34266539

Financing the Proliferation of Weapons of Mass Destruction

The term proliferation of weapon of mass destruction (proliferation) does not limit itself to providing or allowing chemical, biological, radiological, or nuclear material or equipment to build weapons, but it also involves the transfer and export of technology, goods, software, services or expertise that could be used in nuclear, chemical or biological weapons-related programs. The targeted financial sanctions aim to prevent the financing of proliferation.

Proliferation financing is providing financial services to those related programs for the transfer and export of nuclear, chemical, or biological weapons, their means of delivery, and related materials. It also involves the financing of trade in sensitive goods needed to support or maintain those programs, even if those goods are not related to any nuclear, chemical, or biological material, such as oil, coal, steel, and military communication equipment. Additionally, proliferation financing includes the financial support to individuals or entities engaged in proliferation, even if they perform other activities that are not related to such programs, such as diplomats, shipping companies, fisheries, and trade-in commodities companies.

The following are cases of violations or evasion of the sanctions imposed by the UNSC related to the Nuclear Programme of the Democratic People's Republic of Korea (DPRK), as presented by the Panel of Experts pursuant to UNSCR 1874, between 2017 and 2020 ("the UN Panel of experts"). This paper also gives examples of cases related to the circumvention of the United States of America's sanctions imposed on Iran and the UN sanctions pursuant to UNSCR 1737, continued by UNSCR 2231 related to Iran's nuclear program.

The cases that are explained here involve many sectors, including the financial, trade, and shipping industries. The aim is to increase the awareness in all economic sectors about these sanctions and the importance of their implementation.

Financial measures

The use of the Banking Sector

Designated banks maintain representative offices and agents abroad

The UN Panel of experts reported in February 2017 that it had obtained information showing that two UNSC sanctioned banks, Daedong Credit Bank (DCB) and Korea Daesong Bank (KDB), are both operating on Chinese territory, through representative offices in Dalian, Dandong, and Shenyang. A director of such offices also served as a director of a designated company, DCB Finance Ltd., registered in the British Virgin Islands. DCB Finance shared several officers with DCB. When the DCB correspondent accounts were closed in 2005, DCB Finance was set up to undertake wire transfers and business transactions on its behalf[19].

The representative in Dalian of DCB and DCB Finance undertook transactions worth millions of United States dollars, including several of $1 million or more. He also facilitated payments and loans between companies linked to DCB. He exchanged

[19] Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 75

large quantities of bulk cash transferred to China from the DPRK into newer and larger denomination United States dollar notes. He also regularly undertook foreign exchange between United States dollars and euros and transferred balances between DCB and its shareholder, Korea Daesong Bank. When DCB established representative offices in Shenyang in late 2012 and Dandong in 2014, the three offices cooperated in managing the activities of foreign exchange, transfer, bulk cash exchange, and loans[20].

In 2019, the UAE expelled representatives of the following DPRK Banks:

- Representative and Deputy representative of Korea Kumgang Group Bank
- A representative of Korea Kumgang Group Bank: Who transported DPRK laborers' money in the Middle East to the DPRK.

Financial activities of diplomatic and other personnel of the DPRK

The UN Panel of experts investigated diplomatic or official personnel of the DPRK who act on behalf of the country's sanctioned financial institutions to establish illicit banking networks and provide the country with access to global banking systems.

The UN Panel of experts investigated reports that Jo Kwang Chol, an accredited member of the administrative and technical staff at the Embassy of the DPRK in Austria since 2016, had engaged in sanctions evasion activities on behalf of the designated Foreign Trade Bank. According to information provided by Austria, Mr. Jo had attempted to gain access to Korea Ungum Corporation's frozen accounts at an Austrian bank. Austrian authorities froze the accounts in July 2015 owing to suspected money-laundering activity. At the time, the total balance was approximately $1,895,633[21].

Transfers through banks

US authorities in 2016 and 2019 indicated the woman, Ma Xiaohong, her company, Dandong Hongxiang Industrial Development Corp., and other executives in the company on charges of money laundering and helping North Korea evade international sanctions.

Before the indictments, Ma and Dandong Hongxiang routed money to North Korea through China, Singapore, Cambodia, the US, and elsewhere, using an array of shell companies to move tens of millions of dollars through US banks in New York. There is an estimate that in 2015 there were transfers of US $85.6 million[22].

Use of cash to circumvent US sanctions

The United States and the United Arab Emirates (UAE) jointly took action to disrupt an extensive currency exchange network in Iran and the UAE that has procured and transferred millions in US dollar-denominated bulk cash to Iran's Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF) to fund its malign activities and regional proxy groups. Specifically, the US Department of the Treasury's Office of Foreign Assets

[20] Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 76
[21] Report of the Panel of Experts pursuant to UNSCR 1874, S/2020/151, p. 63
[22] NCBC News, 2020, available at https://www.nbcnews.com/news/world/secret-documents-show-how-north-korea-launders-money-through-u-n1240329

Control (OFAC) designated nine Iranian individuals and entities. Iran's Central Bank was complicit in the IRGC-QF's scheme and actively supported this network's currency conversion and enabled its access to funds that it held in its foreign bank accounts. This network of exchangers and couriers has converted hundreds of millions of dollars[23].

Cyberactivity targeting financial institutions

There is evidence that the DPRK, by means of cyberattacks, is stealing funds from financial institutions and cryptocurrency exchanges in different countries, which allows the country to evade financial sanctions and generate income in ways that are harder to trace and subject to less government oversight and regulation. During 2019, there were investigations of at least 35 reported instances of DPRK actors attacking financial institutions, cryptocurrency exchanges, and mining activity designed to earn foreign currency, including in the following Member States: Bangladesh (2 cases), Chile (2), Costa Rica (1), the Gambia (1), Guatemala (1), India (3), Kuwait (1), Liberia (1), Malaysia (1), Malta (1), Nigeria (1), Poland (1), the Republic of Korea (10), Slovenia (1), South Africa (1), Tunisia (1) and Viet Nam (1)[24].

According to the UN Panel of Expert, since 2019, there is a marked increase in such cyber activities' scope and sophistication. Some estimates placed the amount illegally acquired by the DPRK at as much as $2 billion[25].

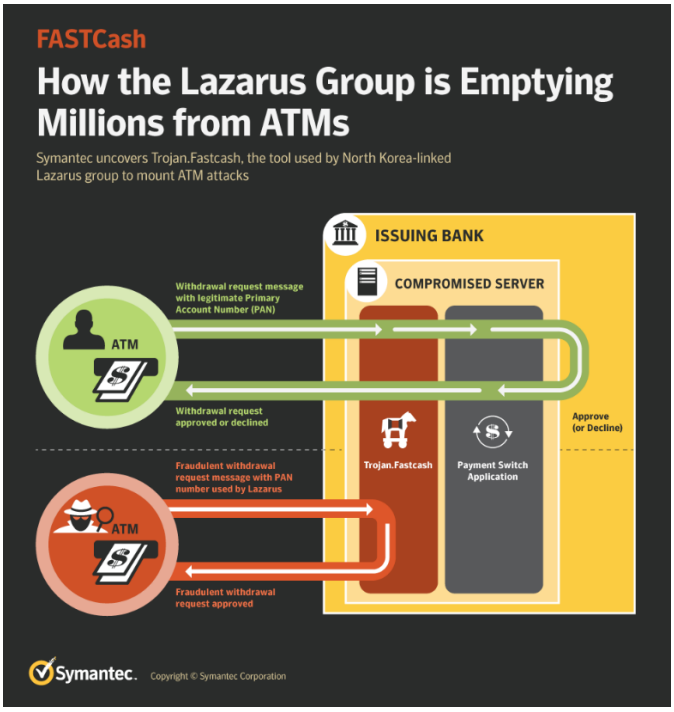
Operation "FASTCash"

In its report of August 2019, the UN Panel of experts reported on a cyberattack carried out by DPRK cyber actors who gained access to the infrastructure managing entire automatic teller machine networks of a country. The purposes were to install malware modifying transaction processing in order to force 10,000 cash distributions to individuals working for or on behalf of the DPRK across more than 20 countries in five hours. That operation required large numbers of people on the ground, which suggests extensive coordination with DPRK nationals working abroad and possibly cooperation with organized crime[26].

The operation, known as "FASTCash," was enabled by Lazarus, a group involved in both cybercrime and espionage, with apparent links to DPRK. With this operation, it was possible to fraudulently empty ATMs of cash. To make fraudulent withdrawals, Lazarus first breaches targeted banks' networks and compromises the switch application servers handling ATM transactions.

[23] U.S. Department of Treasury , 2018, https://home.treasury.gov/news/press-releases/sm0383#:~:text=Washington%20%E2%80%93%20Today%20the%20United%20States,IRGC%2DQF)%20to%20fund%20its, accessed on February 1, 2021.
[24] Report of the Panel of Experts pursuant UNSCR 1874, S/2019/691, p. 26
[25] Report of the Panel of Experts pursuant UNSCR 1874, S/2019/691, p. 26
[26] Report of the Panel of Experts pursuant UNSCR 1874, S/2019/691, p. 26

Figure-2: Diagram showing Lazarus Group schemes used to circumvent UN sanctions



Source: "FASTCash: How the Lazarus Group is emptying millions from ATMs," Symantec, 2 October 2018. Available at www.symantec.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware.

Once these servers are compromised, previously unknown malware (Trojan.Fastcash) was deployed. In turn, this malware intercepts fraudulent Lazarus cash withdrawal requests and sends fake approval responses, allowing the attackers to steal cash from ATMs.

According to a US government alert, one incident in 2017 saw cash withdrawn simultaneously from ATMs in over 30 different countries. In another major incident in 2018, cash was taken from ATMs in 23 separate countries. To date, the Lazarus FASTCash operation is estimated to have stolen tens of millions of dollars[27].

Cyberattack on cryptocurrency exchange bureaus

In 2019, DPRK cyber actors shifted focus to targeting cryptocurrency exchanges. Some cryptocurrency exchanges have been attacked multiple times, in particular those registered in the Republic of Korea. Bithumb was reportedly attacked by DPRK cyber actors at least four times. The first two attacks, in February and July 2017, resulted in losses of approximately $7 million each, with subsequent attacks in June 2018 and March 2019 resulting in the loss of $31 million and $20 million, respectively, showing the increased capacity and determination of DPRK cyber actors. Similarly, Youbit (formerly Yapizon) suffered multiple attacks involving a $4.8 million loss in April 2017 and then 17 percent of its overall assets in December 2017, forcing the exchange to close[28].

[27] FASTCash: How the Lazarus Group is emptying millions from ATMs, Symantec, 2 October 2018. Available at www.symantec.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware.
[28] Report of the Panel of Experts pursuant UNSCR 1874, S/2019/691, p. 28

Economic resources

Bulk cash and gold

The DPRK uses bulk cash and gold to transfer value by circumventing the formal financial sector entirely. The following are some cases reported by the UN Panel of Experts.

On 6 March 2015, Bangladesh seized 26.7 kg of gold bars and jewelry (worth $1.4 million) from the hand luggage of the First Secretary of the embassy of the DPRK in Dhaka. An invoice related to those goods had been issued by AMM Middle East General Trading in Dubai, United Arab Emirates, and they were collected from Singapore. The First Secretary had flown into and out of Singapore from Dhaka on the same day, leaving the airport for three hours. He had undertaken on average one such trip per month to Singapore over the previous 15 months from both Dhaka and Beijing (ranging from a few hours to two days on the ground), suggesting that he was serving as a regular diplomatic courier smuggling gold and other items in evasion of sanctions. He was accompanied by other diplomats of the DPRK on some of the trips[29] .

On 17 March 2016 in Sri Lanka, an overseas worker of the DPRK was arrested at the airport in Colombo carrying $167,000 in cash, gold jewelry, and watches. He was en route from Oman to Beijing and made no customs declaration. He was accompanied by five other individuals from the DPRK who were working in Oman for a construction company of the DPRK based in Dubai with a post office box address. He produced a list with 311 names of workers of the DPRK whose families in Pyongyang he was to pay (with amounts varying from $200 to $1,500, with an average of around $300 per family)[30].

Oil ship-to-ship transfers

Since 2018, the UN Panel of experts evidence of an increasing frequency of ship-to-ship transfers and one unprecedented prohibited petroleum product transfer comprises 57,623.491 barrels alone, worth $5,730,886. The Panel's investigation of this transfer reveals a very sophisticated case of DPRK-related vessel identity fraud, highlighting new sanction evasion techniques that defeated the due diligence efforts of the region's leading commodity trader, as well as the United States and Singaporean banks that facilitated the fuel payments and a leading United Kingdom insurer that provided protection and indemnity cover to one of the vessels involved. The case also underlines, once again, the extremely poor reporting, oversight, monitoring, and control over the vessels exercised by the flag-of-convenience States under whose jurisdiction they apparently sail[31] and also the lack of implementation of freezing sanctions.

[29] Report of the Panel of Experts pursuant to UNSCR 1874, S/2017/150, p. 79
[30] Report of the Panel of Experts pursuant to UNSCR 1874, S/2017/150, p. 79
[31] Report of the Panel of Experts pursuant UNSCR 1874, S/2019/691, p. 8

Trading in Oil

The UAE authorities arrested a person (of Egyptian nationality) residing in the State and using shipping companies established in the UAE with the intention of evading the sanctions against Iran. The suspect made shipping bills for those companies in the name of the companies he owns in cooperation with persons affiliated with Iran's Revolutionary Guard Corps (IRGC). To achieve this, he forged bills of lading of Iranian oil and imported it to UAE, saying that it was Iraqi oil, and by taking advantage of the licenses that he had obtained. An amount of AED 10,000,000 (ten million dirhams) was seized, and an amount of AED 30,000,000 (thirty million dirhams) in accounts of the companies was frozen.

Nickel wire

The UAE authorities have identified a person with Emirati nationality who has a relationship with members of Iran's Revolutionary Guard Corps (IRGC) and who has carried out several commercial activities with Iranian merchants affiliated with the IRGC through financing projects and real estate. One of these merchants proposed to him to provide a substance called "nickel wire" that is used in the military industries in favor of Iran's Defense Ministry. The substance significance is to prolong the life of the military weapons and their devices. The suspect made a partnership with him to buy this substance from China and selling it to Iran's Defense Ministry at a higher price. Together with his partners, the suspect purchased a sample of nickel wire from China and shipped it to the UAE, and then shipped it to Iran. When the Iranian counterparts agreed with the business, the suspect's partners contacted a person in London to provide the substance from China and to export it to Hong Kong in the name of another person with the intention to ship it to Iran.

In a similar case, the UAE authorities investigated a suspect who was making money transfers to members of Iran's Revolutionary Guard Corps (IRGC). He was also requested to make a partnership with members of this same group in order to import (nickel wire) material from outside the UAE to re-ship it through the companies owned by the suspect in the State to Iran in favor of Iran's Defense Ministry, aiming to evade the UN Security Council sanctions against Iran government. The transaction's value amounted to USD 800,000,000 (eight hundred million dollars), and a payment of USD 8,000,000 (eight million dollars) was transferred in favor of the company that owned the goods. The UAE authorities have the accounts of the suspect and companies frozen.

Carbon fiber

In collaboration with the UAE, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) designated 11 entities and individuals involved in procurement on behalf of Iran's ballistic missile program. OFAC sanctioned Mabrooka Trading Co LLC (Mabrooka Trading) – based in the United Arab Emirates (UAE) – and a UAE-based network involved in procuring goods for Iran's ballistic missile program. This network obscured the end user of sensitive goods for missile proliferation by using front companies in third countries to deceive foreign suppliers. It has also designated five Iranian individuals who have worked to procure ballistic missile components for Iran.

Hossein Pournaghshband and his company, Mabrooka Trading, were providing or attempting to provide financial, material, technological, or other support to Navid Composite Material Company (Navid Composite), an entity also sanctioned by the US in connection with Iran's ballistic missile program. At the time of its designation, Navid Composite was contracting with Asia-based entities to procure a carbon fiber production line in order to produce carbon fiber probably suitable for use in ballistic missile components. Since at least early 2015, Pournaghshband used his company, Mabrooka Trading, to procure materials and other equipment for Navid Composite's carbon fiber production plan. Pournaghshband is also designated for having provided or attempting to provide financial, material, technological, or other support to Mabrooka Trading[32].

Trade-in other goods

Generator

The UAE authorities arrested a man suspected of importing a generator through the company he owned, which operated in the oil and gas business. He imported the generator from Britain, and originally the bill of landing said it was going to be re-exported to Myanmar. But after the device entered the UAE, he forged a bill of lading. He changed the final beneficiary's name from Myanmar to Port of Asalouyeh in Iran, aiming to send the device to Iran's Nuclear Program. The suspect also made financial transfers of the generator's value through his accounts in local banks that were made in batches through the use of a third State, and then transfer the money to a company in Britain. The generator was seized, and the suspect was sentenced to ten (10) years imprisonment, deportation, and the confiscation of the device.

Vibration Analysing devises

The UAE authorities received communication about bills of lading submitted by a company containing three (3) Portable Vibration Analyser, with the final destination Iran and the seller being a company in the UAE. However, the company provided bills of lading containing consignment information of three (3) Vibration Measurement Devices with a value of EUR 22,000 (twenty-two thousand euros), as well as a document that the company claimed to have submitted to the authority by mistake, showing a bill of sale and purchase of the same equipment, of the same value, but with the end-user being different, the buyer was a company in Iran, and the seller was a company in Turkey that sells nuts. On-field inspection, it turned out that this consignment was imported from a company in Hong Kong to a company in the UAE. The company provided forged documents regarding the company's branches in Britain to evade the sanctions against Iran.

Misuse of legal entities or arrangements

DGS Marine

Until July 2012, DGS Marine was a Liechtenstein-registered offshore business company located at a fiduciary's office in Vaduz. Following June 2012 media reports that DGS's

[32] U.S. Department of Treasury , 2017, https://www.treasury.gov/press-center/press-releases/pages/jl0322.aspx accessed on February 1, 2021.

director, David Skinner, had issued insurance certificates for Iranian-owned oil tankers transporting oil from Syria allegedly in contravention of European Union sanctions, the Liechtenstein Financial Authority issued a July 2012 warning notice stating that DGS Marine was not licensed to issue insurance in Liechtenstein. Following the Liechtenstein warning notice, Mr. Skinner registered DGS Marine as a BVI business company in August 2012. The UN Panel of experts was able to confirm that DGS Marine was not licensed or authorized to issue insurance in the BVI either.

In addition, the 2009 DGS Marine annual report contained false information regarding the identity of an individual described as DGS Marine's "independent auditor," calling into question the certification of DGS Marine's annual financial statements. DGS Marine did not respond to the Panel's inquiries, and during the course of the Panel's investigation, the death of Mr. Skinner was announced, and shortly afterward, the DGS website was shut down. Media reporting subsequently indicated that DGS Marine was an elaborate insurance scam that, while maintaining offices in the United Kingdom, Cyprus, Denmark, Vietnam, India, China, and the United Arab Emirates, did not possess the millions of pounds in securities alleged in its annual reports.[33]

The GENCO/KOGEN Group

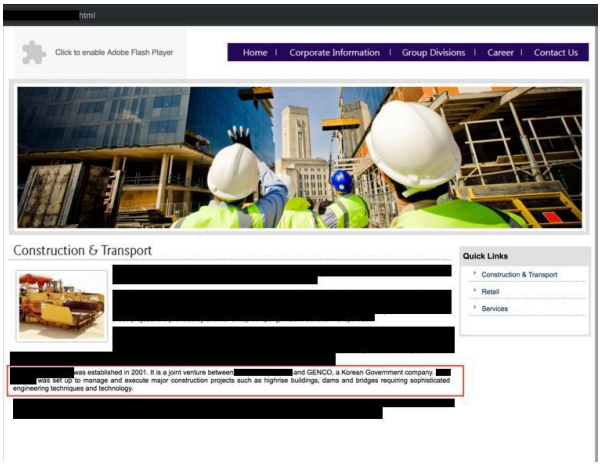
This is a case, published in the UN Panel of experts report pursuant to resolution UNSCR 1874 in March 2019 and August 2019, involving the Korea General Corporation for External Construction (a.k.a. GENCO, a.k.a. KOGEN) group, a network of legal companies and arrangements registered in different countries linked with the Reconnaissance General Bureau, a North Korean intelligence agency that manages the State's clandestine operations.

The UN Panel of experts reported on the ongoing investigation into GENCO/KOGEN that showed that the company has a large reach and extensive network in several countries in the Middle East, Africa, and Eurasia, where it utilizes laborers, prohibited cooperative entities, and joint ventures of the DPRK and earns significant revenue. According to a country, GENCO/KOGEN "has worked to supply North Korean laborers in the Middle East for the purpose of earning hard currency for [the] North Korea[n government]."The Panel's investigations found evidence of KOGEN activity by a joint venture with a company of the United Arab Emirates[34].

According to corporate registration documents, GENCO is the partial owner of a cooperative construction entity or joint venture company in the Russian Federation, LLC "SAKORENMA," with majority ownership belonging to a Russian national. This cooperative entity or joint venture maintains an account with a Russian bank. Furthermore, the company shares addresses, contact information, and shareholders with three other companies, all of which engage in construction-related activities. In addition, corporate registry documents show that GENCO operates two official representative offices in the Russian Federation, one in Vladivostok and one in Khasan, that together formally employ 17 foreign nationals.[35]

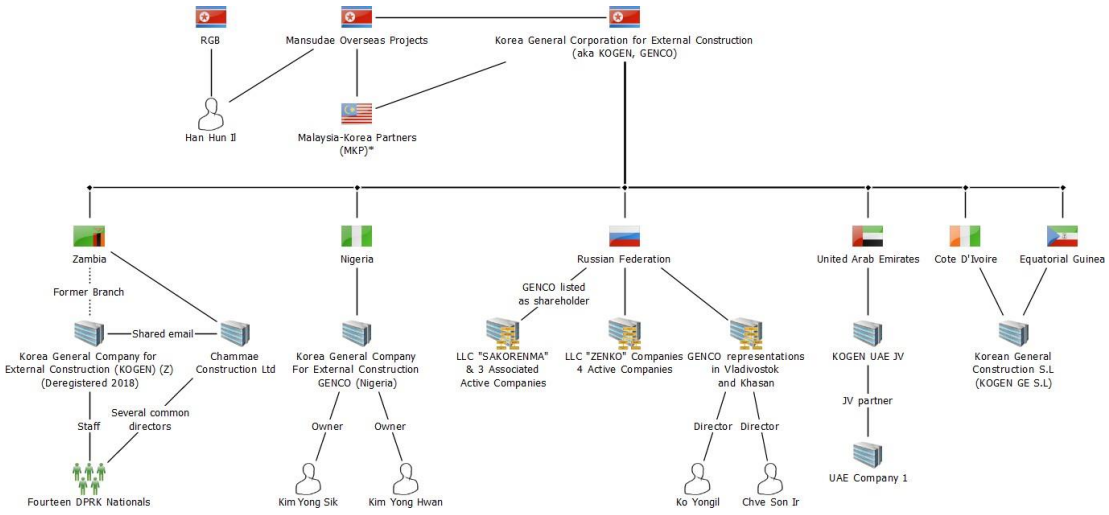
[33] Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 206
[34] Report of the Panel of Experts pursuant UNSCR 1874, S/2019/171, p. 56
[35] Report of the Panel of Experts pursuant UNSCR 1874, S/2019/171, p. 56

Figure-3: Website of KOGEN entity in the United Arab Emirates



The presence of GENCO/KOGEN in Africa covers Nigeria, Côte d'Ivoire, and Equatorial Guinea. In Nigeria, it is registered as "Korea General Company for External Construction GENCO (Nigeria)." In Côte d'Ivoire, "Korea General Construction SL (KOGEN GE SL)" was registered in 2012. The website of the African Union Inter-African Bureau for Animal Resources lists KOGEN GE SL as its implementing partner for a project funded by Equatorial Guinea. KOGEN was separately reported as a contractor for the Rebola Municipal Stadium, completed in 2016, which documents suggest earned KOGEN approximately $30.5 million. Local news claims that KOGEN opened a new, large national headquarters in Equatorial Guinea the same year[36].

Figure-4: I2 chart showing GENCO/KOGEN network



GENCO network

Source: The Report of the UN Panel of experts pursuant UNSCR 1874, S/2019/171, p. 57.

Analysis of GENCO/KOGEN bank accounts in Zambia, in dollars and in the local currency, showed regular cash and cheque activity and high account turnover. The

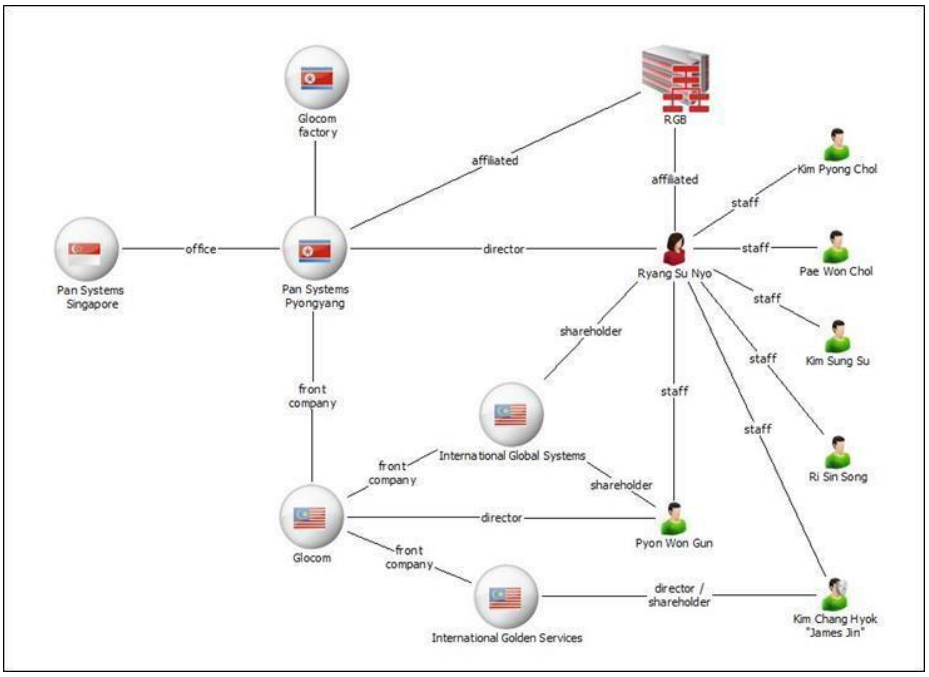
[36] Report of the Panel of Experts pursuant UNSCR 1874, S/2019/171, p. 56

accounts demonstrated similar patterns of cheque deposits, followed by incoming transfers, followed by regular cheque withdrawals[37].

The Glocom group

Glocom is a Malaysia based company that advertises radio communications equipment for military and paramilitary organizations. Glocom claims a presence in more than 10 countries and a prominent international reputation gained through participating, according to its website, in three biennial "Defense Service Asia" arms exhibitions since 2006. However, Glocom is not officially registered and has no presence at its listed physical address. Two other Malaysia based companies acting on its behalf: International Golden Services Sdn Bhd and International Global Systems Sdn Bhd[38].

Figure-5: Pan Systems Pyongyang network



Source: Report of the UN Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 36.

Information obtained by the UN Panel of experts demonstrates that Glocom is a front company of the DPRK company Pan Systems Pyongyang Branch (Pan Systems Pyongyang), which is linked to a Singaporean company named Pan Systems (S) Pte Ltd (Pan Systems Singapore)[39].

According to information obtained by the Panel, Pan Systems Pyongyang is operated by the Reconnaissance General Bureau, the country's premier intelligence agency, designated under UNSCR 2270 (2016). This shows how the Bureau enables its key agents to generate revenues for its operations through such networks. Additionally, the UN Panel of experts determined that "Wonbang Trading Co." is an alias of Pan

[37] Report of the Panel of Experts pursuant UNSCR 1874, S/2019/171, p. 55
[38] Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 34
[39] Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 34

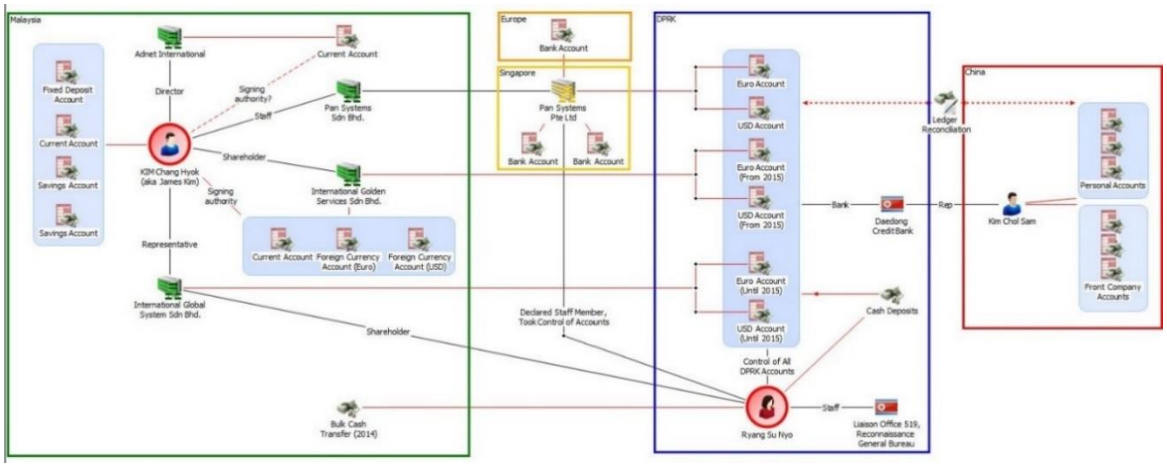
Systems Pyongyang. The information shows that Pan Systems Pyongyang also regularly received funds from the Korea Mining Development Trading Corporation (KOMID)[40].

Financial operations of Glocom/Pan Systems Pyongyang

In its banking operations, Pan Systems Pyongyang and its front companies used an extensive network of individuals, companies, and offshore bank accounts to procure and market arms and related material. The global network consisted of individuals, companies, and bank accounts in China, Indonesia, Malaysia, Singapore, and the Middle East. In particular, €36,939 was transferred to International Global Systems in 2008 from an account at the Damascus branch of a Middle Eastern bank[41].

Since 1998, Pan Systems Pyongyang and International Global Systems have used accounts in United States dollars and euros at Daedong Credit Bank (a DPRK Bank) to gain access to the international financial system, including through bank accounts in China. These accounts were used to transfer funds to a supply chain of more than 20 companies located primarily on the Chinese mainland, in Hong Kong, China, and Singapore. In recent years, procurement shifted almost entirely to companies in China and Hong Kong, China. Most of these companies supplied electronic products, radio components, and casings consistent with Glocom's advertised military communications equipment, while others were transport companies. The network also made regular transfers to various facilitators with Chinese, Korean, foreign, and code names working in China, Indonesia, Malaysia, and the Middle East[42].

Figure-6: Accounts controlled by Glocom



Source: Report of the UN Panel of Experts pursuant UNSCR 1874, S/2018/171, p. 64

In terms of incoming transfers, Pan Systems Pyongyang received large remittances from an account at a major bank in Malaysia, as well as from numerous companies of the DPRK. Transfers were also made from the Shenyang consulate of the DPRK. Pan Systems Pyongyang also regularly used bulk cash transfers. In addition, Pan Systems Pyongyang received funds from two designated entities, KOMID and Hyoksin Trading

[40] Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 36
[41] Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 77
[42] Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 77

Corporation. Between 2011 and 2013, Hyoksin made multiple euro-denominated transfers to Pan Systems Pyongyang, as did KOMID between 2011 and 2015[43].

In addition to its four bank accounts with the Daedong Credit Bank in Pyongyang, the Glocom network controlled at least 10 accounts in four other countries between 2012 and 2017, including through Malaysia-based front companies. Records show that these multiple overseas accounts allowed Glocom to continuously move funds between accounts it controlled in different banks and countries in the course of its illicit trade[44].

[43] Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 78
[44] Report of the Panel of Experts pursuant UNSCR 1874, S/2018/171, p. 64

Red Flags

Considering the above typologies, the following are some red flags or situations that could be looked at more closely or monitored by financial institutions and designated non-financial businesses or professions to identify potential sanctions circumventions of your clients, their business, or their transactions.

- Dealings in sectors vulnerable for terrorist financing and/or proliferation of weapons of mass destructions, for example
    - Financial sector
    - Hawalas or other money transfer services providers
    - Oil and gas sector
    - Non-profit organizations
    - International trade

- Dealings, directly or through a client of your client, with high-risk countries for terrorism financing.

- Dealings, directly or through a client of your client, with sanctioned countries or territories where sanctioned persons are known to operate.

- The use of shell companies through which funds can be moved locally and internationally by misappropriating the commercial sector in the UAE.

- Dealings with sanctioned goods or under embargo. For example:
    - Weapons
    - Oil or other commodities
    - Luxury goods (for DPRK sanctions)

- Dealings with dual-used goods.

- Dealings with controlled substances.

- Identifying documents that seemed to be forged or counterfeited.

- Identifying tampered or modified documents with no apparent explanation, especially those related to international trade.

- Use of intermediaries.

- When the flows of funds exceed those of normal business (revenues or turnover).

- The activity developed or financed does not relate to the original or intended purpose of the company o entity. For example:

    - For companies, they are importing high-end technology devices, but they are registered as a company that commercializes nuts.
    - For a non-profit organization, they are exporting communication devices, but they are an entity aimed to provide health services.

- Very complex commercial or business deals that seem to be aiming to hide the final destiny of the transaction or the good.

- Complex legal entities or arrangements that seem to be aiming to hide the beneficial owner.

- Carrying out of multiple ATM cash withdrawals in short succession (potentially below the daily cash reporting threshold) across various locations in territories where sanctioned people have influence or in the border of sanctioned countries.

- Irregularities during the CDD process which could include, but is not limited to:

    - Inaccurate information about the source of funds and/or the relationship with the counterparty.
    - Refusal to honor requests to provide additional KYC documentation or to provide clarity on the final beneficiary of the funds or goods.
    - Suspicion of forged identity documents

Virtual Assets / Cryptocurrency

- The use of virtual assets to send funds to a few select wallets at unregulated virtual assets exchanges (or exchanges in territories where sanctioned people have influence or sanctioned jurisdictions).

- Financial institutions should pay particular attention to the transfer of funds to a virtual assets exchange's operational banking account (to fund a virtual asset wallet) followed by the crypto-to-fiat conversion (either more or less) from the same exchange within a relatively short period of time.

References

ABC news, 2015. *US officials Ask HOw ISIS Got So Many Toyota Trucks..* [Online]
Available at: https://abcnews.go.com/International/us-officials-isis-toyota-trucks/story?id=34266539
[Accessed 13 Apil 2021].

Financial Action Task Force, February 2015. *Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL),* Paris: FATF.

Financial Action Task Force, June 2014. *Risk of Terrorist Abuse in Non-Profit Organizations,* Paris: s.n.

Financial Action Task Force, October 2013. *The Role of Hawala and Oter Similar Service Providers in Money Laundering and Terrorist Financing,* Paris: FATF.

Financial Action Task Force, October 2015. *Emerging Terrorist Financing Risks,* Paris: FATF.

NCBC News, 2020. *NCBCNews.com.* [Online]
Available at: https://www.nbcnews.com/news/world/secret-documents-show-how-north-korea-launders-money-through-u-n1240329
[Accessed 21 September 2020].

Panel of Experts pursuant to UNSCR 1874, S/2020/151. *Report of the Panel of Experts established pursuant to UNSCR 1874,* New York: United Nations Security Council.

Panel of Experts pursuant UNSCR 1874, S/2017/150. *Report of the Panel of Experts established pursuant to resolution 1874,* New York: United Nations Security Council.

Panel of Experts pursuant UNSCR 1874, S/2018/171. *Report of the Panel of Experts pursuant UNSCR 1874,* New York: United Nations Security Council.

Panel of Experts pursuant UNSCR 1874, S/2019/171. *Panel of Experts Report Pursuant UNSCR 1874 S/2019/171,* New York: United Nations Security Council.

Panel of Experts pursuant UNSCR 1874, S/2019/691. *Report of the Panel of Experts established pursuant to resolution 1874 (2009),* New York: United Nations Security Council.

U.S. Department of the Treasury, 2016. *Press Center.* [Online]
Available at: https://www.treasury.gov/press-center/press-releases/pages/jl0322.aspx
[Accessed 1 February 2021].

U.S. Department of Treasury , 2018. *Press Releases.* [Online]
Available at: https://home.treasury.gov/news/press-releases/sm0383#:~:text=Washington%20%E2%80%93%20Today%20the%20United%20States,IRGC%2DQF)%20to%20fund%20its
[Accessed 1 January 2021].

United Nations Counter-Terrorism Committee Executive Directorate and the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015), S/2020/493. *The joint report of the Counter-Terrorism*

Committee Executive Directorate and the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015), New York: United Nations Security Council.

United Nations Office on Drugs and Crime, 2012. *The Use of the Internet for Terrorist Purposes,* New York: UNODC.

United Nations Security Council, 2014. *Resolution 2178 ,* s.l.: s.n.

www.symantec.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware, 2018. *FASTCash: How the Lazarus Group is emptying millions from ATMs..* [Online] Available at: www.symantec.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware.