United Nations Targeted Sanctions against the Financing of Terrorism and the Proliferation of Weapons of Mass Destruction

Typologies paper

This document was developed by Oman's National Counter Terrorist Committee in cooperation with the Anti-Money Laundering and Counter Terrorism Financing National Committee.

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 14 sanctions regimes which focus on supporting political settlement of conflicts, nuclear non-proliferation, and counter-terrorism.

This document focuses on the following United Nations Security Counsil Resolutions (UNSCRs):

- Those related to terrorism and terrorist financing, i.e.:
  - UNSCR 1267
  - UNSCR 1988
  - UNSCR 1989
- Those related to the proliferation of weapons of mass destruction and its financing, i.e.:
  - UNSCR 1718
  - UNSCR 2231

All information presented in this document is derived from public sources. It includes a compilation of cases and situations, aiming to provide guidance to public and private institutions. The paper highlights trends and methods used by sanctioned persons, groups or entities to circumvent the sanctions imposed by the above-listed UNSCRs. It is the responsibility of each institution to implement adequate measures to prevent being misused to breach the UNSCR and duly report to the competent authorities any (attempted) circumvention.

Terrorist Financing

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 includes providing food, lodging, training, and making means available such as transportation or communication equipment. Such financing can take place with money or in kind, and funds involved can be from legal or illegal sources.

The following are methods and cases that illustrate how terrorist groups have misused economic sectors or activities to fund their activities. 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 Organisation Islamic State in Iraq and the Levant (ISIL)" of 2015 FATF identified that ISIL earns revenue primarily from five sources: (1) illicit proceeds from occupation of territory, such as bank looting, extortion, control of oil fields and refineries, and robbery of economic assets and illicit taxation of goods and cash that transit territory where ISIL operates; (2) kidnapping for ransom; (3) donations including by or through non-profit organisations; (4) material support such as support associated with FTFs and (5) fundraising through modern communication networks[1].

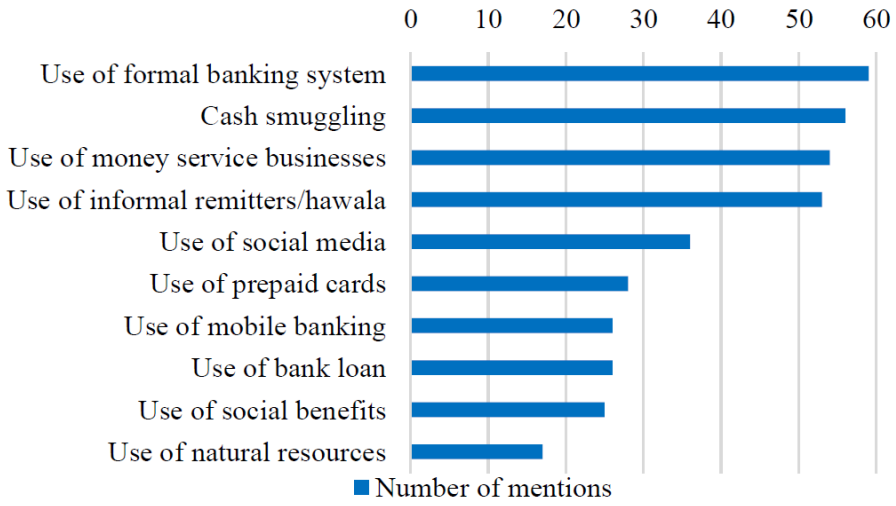
The Joint report of the Counter-Terrorism Committee Executive Directorate and the Analytical Support and Sanctions Monitoring Team pursuant to UNSCRs 1526 (2004) and 2253 (2015) on actions taken by Member States to disrupt terrorist financing, prepared pursuant to paragraph 37 of UNSCR 2462 (2019), of June 3 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 reports on 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 a variety of means, including exploitation of 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 conceal cash, the use of non-profit organizations and trade-based terrorism financing.[4]

Methods most frequently used by terrorist financiers

[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.
[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.



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

Banking services

The formal banking system is vulnerable for terrorist financing because of the difficulty of distinguishing between legitimate and illegitimate low-cost transactions and detecting indirect transactions. Transaction-monitoring programmes are often unable to identify terrorism financing. There is also a risk in the use of bank loans and social benefits payed through banks for terrorist financing.[5]

Continued Access to bank accounts by Foreign Terrorist Fighters

According to sensitive financial information, terrorist financing risks were discovered regarding foreign cash withdrawals via ATMs that were made in areas located near territories where ISIL operates by unknown individuals. These withdrawals were taken from US-based bank accounts using a Debit 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. *Source: United States*.[6]

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 operating without any AML/CFT controls)[7].

Complicit MVTS Agent

An individual raised funds for Al-Shabaab from within a diaspora in Country A and elsewhere and used a variety of licensed money service businesses (MSBs) with offices in Country A to remit the money to Country B for general support of Al-Shabaab fighters. The co-conspirator, who worked for one of the MSBs involved, helped

[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] Financial Action Task Force, February 2015, p. 23
[7] Financial Action Task Force, October 2015, p.26

the individual avoid leaving a paper trail by structuring transactions into low dollar amounts and by using false identification information. The MSB worker and other conspirators used fictitious names and phone numbers to hide the nature of their transactions.[8]

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 in some cases, the use of businesses that are not regulated financial institutions, the use of net settlement and the commingling of licit and illicit proceeds.[9]

Terrorist Abuse of HOSSPs

A sum of INR 10 000 000 (USD 160 000) was intercepted in Country A which was meant to be delivered to a terrorist gang X. Investigation revealed that a number of earlier consignments had already been delivered to the terrorist gang. It was revealed that development funds of a particular area in Country A was defalcated and then sent to Location X in Country A. From Location X, it was sent to Location Y in Country B with the help of hundi operators operating between Country A and Country B. The hundi operators are told that the money belongs to a very influential person in Country A. The hundi operators do not object conducting the transaction hearing the name of this influential person and deliver the money to Country B to the person authorized by the agent of the terrorist gang. The money is delivered after deducting a commission of 1 per cent from the total money which is transferred. In Country B, the hawala money is then changed from INR to US Dollars in an unregulated exchange market and then transferred to another country, Country C, where arms and ammunition are purchased by the terrorist gang leaders based there. These arms and ammunition are then transferred across the borders and then delivered to the terrorist gang operating in Country A for carrying our terrorist activities. In this case a total of 15 accused were arrested and charge sheeted, and the trial is being held. The arrested members include terrorists, contractors, agents, and government servants.[10]

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.[11]

Fundraising through the Internet

Intelligence information indicates 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 close country from Syria and sell the number of the card with a lower price and take the cash which was afterwards provided to ISIL.[12]

PayPal accounts used for fundraising

A charity set up in 2010, whose chairman is specialised in e-marketing, offers on its website several options to make donations by credit card, PayPal, cash transfers, checks. Over a year and a half, bank accounts of this charity received numerous donations by checks and wire transfers below EUR 500. Of the EUR 2 million

[8] Financial Action Task Force, October 2015, p. 26
[9] Financial Action Task Force, October 2013, p. 41
[10] Financial Action Task Force, October 2013, p. 43
[11] United Nations Office on Drugs and Crime, 2012, p. 7
[12] Financial Action Task Force, February 2015, pp. 24-25

collected, EUR 600 000 came from a few PayPal transactions from another country. Personal PayPal accounts were also used to collects funds, then to be withdrawn by cash, or transferred to other accounts.[1] [3]

Theft through online payment facilities

Online payment facilities can be vulnerable for identity theft, credit card theft, wire fraud, stock fraud, intellectual property crimes and auction fraud.

The Country Z case against Person A: Profits from stolen credit cards were laundered by several means, including transfer through e-gold online payment accounts, which were used to route the funds through several countries before they reached their intended destination. The laundered money was used both to fund the registration by Person A 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.[1] [4]

Donations including by or through non-profit organisations (NPOs)

Individuals and organisations seeking to fundraise for terrorism and extremism support may attempt to disguise their activities by claiming to be engaged in legitimate charitable or humanitarian activities and may establish NPOs for these purposes.[1] [5]

Diversion of Funds by Actors to NPOs

An individual (Mr. A) established a charitable foundation under the pretext of collecting donations for refugees of Country D, people in need of medical and financial aid, and construction of mosques, schools and kindergartens. However, Mr. A was the leader of an organized scheme in which donations were sent to a group of individuals related to Mr. A (Group A) instead of the foundation's account. In most cases, the first stage involved money being sent through money remitters and then transported in cash. The money was then transferred either to credit cards accounts or to e-wallets. The members of Group A placed the relevant information (that funds are being collected for the declared purposes) on the Internet, but, in fact, the funds were sent as an aid for terrorists and their families and meant to be used as a financial support for terrorist activities. This information was discovered through investigations conducted by the FIU based on regular monitoring of entities on their domestic list of designated terrorist entities and related persons or on information provided by law enforcement. Analysis of the collected information allowed the FIU to identify the relation between different cases: common payers and recipients and similar modus operandi in collection and distribution of funds. Further cooperation with law enforcement authorities allowed the FIU to establish the direct link between Mr. A and ISIL's activity. This resulted in several criminal investigations related to Mr. A. In addition, Mr. A was listed on the domestic list of designated terrorist entities, with the relevant freezing procedures performed. Under the court decisions, assets of the Group A members were frozen.[1]

Cash Smuggling

Cash continues to be a prevalent aspect of terrorist operations. While funds may be raised in several ways, often they are converted into cash to be taken to conflict zones. This is assisted by porous national borders, difficulty

[1] Financial Action Task Force, October 2015, p. 38 [3]
[1] United Nations Office on Drugs and Crime, 2012, p. 7 [4]
[1] Financial Action Task Force, October 2015, p. 32 [5]
[1] Financial Action Task Force, February 2015, p. 20 [6]

in detecting cash smuggling (particularly in the small amounts that are sometimes smuggled for TF purposes), and the existence of informal and unregulated economies.[1] [7]

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 Country K. The funds are said to originate from NPO A from Country G as part of humanitarian aid in Burundi, Benin and Zimbabwe. The three couriers are all nationals of Country K and have been living in Country K for a long time. Accounts were held by the three individuals. A coordinating body from Country K of a radical Islamic organisation transferred money to these accounts. Over a period of one year a total amount of nearly EUR 20 000 was withdrawn in cash. Some EUR 10 000 was transferred to Country T.

According to the FIU, NPO A was one of the largest Islamic organisations in Country G. NPO A is said to be linked with NPO B, which had been banned in Country G for allegedly supporting a terrorist organisation. All of NPO B's board members also played a major role in NPO A.

According to information from the intelligence services of Country K, the three individuals referenced above are known to be involved in local branches of a radical Islamic organisation. Given the nature of the transactions and the links between the two NPO referenced above, authorities of Country K suspect that at least part of the funds described above could have been used to support terrorist activities.[1] [8]

[1] Financial Action Task Force, October 2015, p. 23 [7]

[1] Financial Action Task Force, October 2015, p. 23 [8]

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 weapon-related programmes.

Therefore, Proliferation financing is providing financial services to those related programmes 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 programmes, even if those goods are not related to any nuclear, chemical or biological material, for example: oil, coal, steel, 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 nor related to such programmes, for example: diplomats, shipping companies, fisheries, trade in commodities companies.

The following are cases of violations or evasion of the sanctions imposed by the UNSC as presented by the Panel of Experts pursuant to UNSCR 1874, between 2017 and 2020 ("the Panel").

The cases that are explained here involve many sectors worldwide, including the financial, trade and shipping sectors, and evidence the need for countries to increase the awareness in all economic sectors about these sanctions and the importance of their implementation.

With regards to UNSCR 2231 of July 20, 2015, the Joint Comprehensive Plan of Action negotiated between Iran and the P5+1 (the five permanent members of the United Nations Security Council—China, France, Russia, United Kingdom, United States—plus Germany) significantly reduced the sanctions regime under UNSCR 2231. The verification process is currently more focused on the nuclear activity itself and carried out by the International Atomic Energy Agency (IAEA), thus not relevant for this document.

Financial measures

Financial assets

Financial activities of diplomatic and other personnel of the country sanctioned under UNSCR 1718

The Panel investigated diplomatic or official personnel of country sanctioned under UNSCR 1718 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 Panel investigated reports that Jo Kwang Chol, an accredited member of the administrative and technical staff at the Embassy of the country sanctioned under UNSCR 1718 in Country A since 2016, had engaged in sanctions evasion activities on behalf of the designated Foreign Trade Bank. According to information provided by Country A, Mr. Jo had attempted to gain access to Korea Ungum Corporation's frozen accounts at a bank in Country A. Country A's authorities froze the accounts in July 2015 owing to suspected money-laundering activity. At the time, the total balance was approximately $1,895,633[1] . [9]

Cyberactivity targeting financial institutions

There is evidence that the country sanctioned under UNSCR 1718 by the 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 actors from

[1] Report of the Panel of Experts pursuant to UNSCR 1874, S/2020/151, p. 63 [9]

the country sanctioned under UNSCR 1718 attacking financial institutions, cryptocurrency exchanges and mining activity designed to earn foreign currency in multiple countries.[20]

According to the UN Panel of Expert pursuant resolution 1874 report S/2019/691, since 2019 there is a marked increase in the scope and sophistication of such cyberactivities. Some estimates placed the amount illegally acquired by the country sanctioned under UNSCR 1718 at as much as $2 billion[21].

Operation "FASTCash"

The Panel, in its report of August 2019, reported on a cyberattack carried out by cyber actors from the country sanctioned under UNSCR 1718 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 country sanctioned under UNSCR 1718 across more than 20 countries in five hours. That operation required large numbers of people on the ground, which suggests extensive coordination with nationals working abroad from the country sanctioned under UNSCR 1718 and possibly cooperation with organized crime[22].

The operation, known as "FASTCash", was enabled by Lazarus, a group involved in both cybercrime and espionage, with apparent links to the country sanctioned under UNSCR 1718. With this operation it was possible to fraudulently empty ATMs of cash. To make the fraudulent withdrawals, Lazarus first breaches targeted banks' networks and compromises the switch application servers handling ATM transactions.

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

According to a 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.[23]

Cyberattack to cryptocurrency exchange bureaus

In 2019, cyber actors from the country sanctioned under UNSCR 1718 shifted focus to targeting cryptocurrency exchanges. Some cryptocurrency exchanges have been attacked multiple times, in particular those registered in Country S. Bithumb was reportedly attacked by cyber actors from the country sanctioned under UNSCR 1718 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 cyber actors from the country sanctioned under UNSCR 1718. Similarly, Youbit (formerly Yapizon) suffered multiple attacks involving a $4.8 million loss in April 2017 and then 17 per cent of its overall assets in December 2017, forcing the exchange to close.[24]

Designated banks maintain representative offices and agents abroad

The Panel 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 territory of Country C, 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 Country B. DCB Finance shared several officers with DCB.

---

[20] Report of the Panel of Experts pursuant UNSCR 1874, S/2019/691, p. 26

[21] Report of the Panel of Experts pursuant UNSCR 1874, S/2019/691, p. 26

[22] Report of the Panel of Experts pursuant UNSCR 1874, S/2019/691, p. 26

[23] 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.

[24] Report of the Panel of Experts pursuant UNSCR 1874, S/2019/691, p. 28

When the DCB correspondent accounts were closed in 2005, DCB Finance was set up to undertake wire transfers and business transactions on its behalf.[2] [5]

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 and exchanged large quantities of bulk cash transferred to Country C from the country sanctioned under UNSCR 1718 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 X in late 2012, and Y in 2014, the three offices cooperated in managing the activities of foreign exchange, transfer, bulk cash exchange and loans.[2] [6]

Economic resources

Bulk cash and gold

Bulk cash and gold are used by the country sanctioned under UNSCR 1718 to transfer value by circumventing the formal financial sector entirely. The following are some cases reported by the Panel.

On 6 March 2015, Country B seized 26.7 kg of gold bars and jewellery (worth $1.4 million) from the hand luggage of the First Secretary of the embassy of the country sanctioned under UNSCR 1718 in City X. An invoice related to those goods had been issued by AMM Middle East General Trading in Country U, and they were collected from Country S. The First Secretary had flown into and out of Country S from City X on the same day, leaving the airport for three hours. He had undertaken on average one such trip per month over the previous 15 months from both different cities, 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 country sanctioned under UNSCR 1718 on some of the trips.[2] [7]

On 17 March 2016 in Country A, an overseas worker of the country sanctioned under UNSCR 1718 was arrested at the airport in Country A carrying $167,000 in cash, gold jewellery and watches. He was en route from Country O to Country W and made no customs declaration. He was accompanied by five other individuals from the country sanctioned under UNSCR 1718 who were working in Country O for a construction company of the country sanctioned under UNSCR 1718 based in Country U with a post office box address. He produced a list with 311 names of workers of the country sanctioned under UNSCR 1718 whose families he was to pay (with amounts varying from $200 to $1,500, with an average of around $300 per family).[2] [8]

Oil ship-to-ship transfers

Since 2018, the Panel has evidence of an increasing frequency of ship-to-ship transfers and of one unprecedented prohibited petroleum product transfer comprising 57,623.491 barrels alone, worth $5,730,886. The Panel's investigation of this transfer reveals a very sophisticated case of vessel identity fraud with vessels related to the country sanctioned under UNSCR 1718, highlighting new sanction evasion techniques that defeated the due diligence efforts of the region's leading commodity trader, as well as the banks from Country A and B that facilitated the fuel payments and a leading insurer from Country U 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[2] [9] and also the lack of implementation of freezing sanctions.

---

[2] Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 75 [5]
[2] Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 76 [6]
[2] Report of the Panel of Experts pursuant to UNSCR 1874, S/2017/150, p. 79 [7]
[2] Report of the Panel of Experts pursuant to UNSCR 1874, S/2017/150, p. 79 [8]
[2] Report of the Panel of Experts pursuant UNSCR 1874, S/2019/691, p. 8 [9]

The GENCO/KOGEN Group

This is a case, published in the 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 Country A intelligence agency that manages the state's clandestine operations.

The 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 labourers, prohibited cooperative entities and joint ventures of the country sanctioned under UNSCR 1718 and earns significant revenue. According to a country, GENCO/KOGEN "has worked to supply Country A laborers in the Middle East for the purpose of earning hard currency for [the] government of Country A".The Panel's investigations found evidence of KOGEN activity by a joint venture with a company of Country B.[3]

According to corporate registration documents, GENCO is the partial owner of a construction cooperative entity or joint venture company in the Russian Federation, LLC "SAKORENMA", with majority ownership belonging to a national of Country C. This cooperative entity or joint venture maintains an account with a bank of Country C. 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 Country C, that together formally employ 17 foreign nationals.[3] [1]

The presence of GENCO/KOGEN in Africa covers different countries. In one it is registered as "Korea General Company for External Construction GENCO (Nigeria)." In the other, "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 S.L. as its implementing partner for a project funded by Country X. 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 Country X the same year.[3] [2]

Analysis of GENCO/KOGEN bank accounts, in dollars and in local currency, showed regular cash and cheque activity and high account turnover. The accounts demonstrated similar patterns of cheque deposits, followed by incoming transfers, followed by regular cheque withdrawals[3] . [3]

The Glocom group

Glocom is company based in Country A which 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 based companies in Country A acted on its behalf: International Golden Services Sdn Bhd and International Global Systems Sdn Bhd.[3] [4]

Information obtained by the Panel demonstrates that Glocom is a front company of Pan Systems Pyongyang Branch, which comes from the country sanctioned under UNSCR 1718 and is linked to a company in Country B named Pan Systems (S) Pte Ltd.[3] [5]

---

[3] Report of the Panel of Experts pursuant UNSCR 1874, S/2019/171, p. 56 [0]
[3] Report of the Panel of Experts pursuant UNSCR 1874, S/2019/171, p. 56 [1]
[3] Report of the Panel of Experts pursuant UNSCR 1874, S/2019/171, p. 56 [2]
[3] Report of the Panel of Experts pursuant UNSCR 1874, S/2019/171, p. 55 [3]
[3] Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 34 [4]
[3] Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 34 [5]

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 Panel determined that "Wonbang Trading Co." is an alias of Pan Systems Pyongyang. Information shows that Pan Systems Pyongyang also regularly received funds from the Korea Mining Development Trading Corporation (KOMID)[3] .

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 materiel. The global network consisted of individuals, companies and bank accounts from different countries in Asia and the Middle East. In particular, €36,939 was transferred to International Global Systems in 2008 from an account at the branch of a Middle Eastern bank.[3]

Since 1998, Pan Systems Pyongyang and International Global Systems have used accounts in United States dollars and euros at Daedong Credit Bank (a Bank from the country sanctioned under UNSCR 1718) to gain access to the international financial system, including through bank accounts in Country A. These accounts were used to transfer funds to a supply chain of more than 20 companies located primarily in East Asia. 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 foreign and code names working in East Asia and the Middle East.[3]

In terms of incoming transfers, Pan Systems Pyongyang received large remittances from an account at a major bank in Country B, as well as from numerous companies of the country sanctioned under UNSCR 1718 . Transfers were also made from a consulate of the country sanctioned under UNSCR 1718. Pan Systems Pyongyang also regularly used bulk cash transfers. In addition, Pan Systems Pyongyang received funds from two designated entities, KOMID and Hyoksin Trading Corporation. Between 2011 and 2013, Hyoksin made multiple euro denominated transfers to Pan Systems Pyongyang, as did KOMID between 2011 and 2015.[3]

In addition to its four bank accounts with the Daedong Credit Bank, the Glocom network controlled at least 10 accounts in four other countries between 2012 and 2017, including through Country B-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[4] .

[3] Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 36
[3] Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 77
[3] Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 77
[3] Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 78
[4] Report of the Panel of Experts pursuant UNSCR 1874, S/2018/171, p. 64

References

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, 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.

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.

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.

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.