Neoficiāls tulkojums no angļu valodas latviešu valodā

FATF

FATF ziņojums

Sarežģītas proliferācijas finansēšanas un sankciju apiešanas shēmas

2025. gada jūnijs

Finanšu darījumu darba grupa (FATF, *Financial Action Task Force*) ir neatkarīga starpvaldību organizācija, kas izstrādā un veicina politiskās nostādnes pasaules finanšu sistēmas aizsardzībai pret noziedzīgi iegūtu līdzekļu legalizāciju, terorisma finansēšanu un masu iznīcināšanas ieroču izplatīšanas (turpmāk tekstā — proliferācija) finansēšanu. FATF rekomendācijas uzskata par pasaules standartu noziedzīgi iegūtu līdzekļu legalizācijas novēršanas (AML) un terorisma finansēšanas novēršanas (CFT) jomā.

Papildu informācija par FATF pieejama tīmekļa vietnē: **www.fatf-gafi.org**

Šis dokuments un/vai jebkura šeit ietvertā karte neskar teritoriju statusu vai suverenitāti, to starptautiskās robežas un teritoriju, pilsētu vai apgabalu nosaukumus.

Atsauce citējot:

FATF (2025), *Sarežģītas proliferācijas finansēšanas un sankciju apiešanas shēmas [Complex Proliferation Financing and Sanctions Evasion Schemes]*, FATF, Parīze, https://www.fatf-gafi.org/content/fatf-gafi/en/publications/complex-proliferation-financing-sanctions-evasion-schemes.html

Saīsinājumi un akronīmi

AML/CFT Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas novēršana (Noziedzīgi iegūtu līdzekļu legalizācijas novēršana / terorisma finansēšanas apkarošana)

AEC Anonimitāti paaugstinošas kriptovalūtas

AIS Automātiskās identificēšanas sistēma

APT38 Paaugstināts pastāvīgs apdraudējums 38

UBOI Informācija par galīgo patiesā labuma guvēju

CBDC Centrālās bankas digitālā valūta

CDD Klienta uzticamības pārbaude

CPF Proliferācijas finansēšanas apkarošana

CVC Konvertējama virtuāla valūta

DeFi Decentralizētas finanses

DNFBP Noteiktas nefinanšu darbības un profesijas

KTDR Korejas Tautas Demokrātiskā Republika

EDD Padziļināta uzticamības pārbaude

FI Finanšu iestāde

FTB Foreign Trade Bank

FTZ Brīvās tirdzniecības zona

GECC Globālā eksporta kontroles koalīcija

SJO Starptautiskā Jūrniecības organizācija

INR Skaidrojoša piezīme par ieteikumu

IRGC Islāma revolucionārās gvardes korpuss

ML/TF Noziedzīgi iegūtu līdzekļu legalizācija/terorisma finansēšana

MVTS Naudas vai vērtību pārvedumu pakalpojums

NRA Nacionālais riska novērtējums

OTC Ārpusbiržas

PF Proliferācijas finansēšana

PoE Ekspertu grupa

P2P Vienādranga

PPP Valsts un privātā partnerība

RGB Izlūkošanas ģenerālbirojs

SAR/STR Ziņojums par aizdomīgām darbībām/darījumiem

SRB Pašregulējoša organizācija

TCSP Trastu un uzņēmumu pakalpojumu sniedzējs

TFS Mērķētas finanšu sankcijas

ANO Apvienoto Nāciju Organizācija

Commented [LŽ1]: https://fid.gov.lv/uploads/files/2021/virtu%C4%81l%C4%81s%20val%C5%ABtas/FID_VV%20risku%20nov%C4%93rt%C4%93jums.pdf

ANO DP Apvienoto Nāciju Organizācijas Drošības padome

UNSCR Apvienoto Nāciju Organizācijas Drošības padomes rezolūcija (mainīt uz ANO DP rezolūcija?)

VASP Virtuālo aktīvu pakalpojumu sniedzējs

WMD Masu iznīcināšanas ieroči

Commented [LŽ2]: https://fid.gov.lv/uploads/files/2024/Terorisma%20un%20prolifer%C4%81cijas%20finans%C4%93%C5%A1anas%20nov%C4%93r%C5%A1anas%20vadl%C4%ABnijas_2024_FID_VDD.pdf

1. Kopsavilkums

Masu iznīcināšanas ieroču (WMD) proliferācija un ar to saistīta finansēšana rada nopietnus draudus globālajai drošībai un starptautiskās finanšu sistēmas integritātei. Ja valsts un privātais sektors neveicinās tehnisko atbilstību un efektivitāti, pieredzējuši valsts un nevalstiskie dalībnieki turpinās izmantot proliferācijas finansēšanas apkarošanas (CPF) kontroles nepilnības. Ņemot vērā WMD potenciāli katastrofālo ietekmi, ir ļoti svarīgi novērst un apkarot šo nelikumīgo darbību finansēšanu.

Sarežģītas proliferācijas finansēšanas (PF) un sankciju apiešanas shēmas ir galvenie draudi starptautiskajai finanšu sistēmai. Atbilstoši FATF pilnvarām, šajā ziņojumā ir uzsvērtas attiecīgās metodes un tendences, kā arī sniegts atbalsts valsts, reģionāla un globāla mēroga draudu un risku novērtējumiem. Pētījumā sīki izklāstīti paņēmieni, kādus izmanto personas, kuras izvairās no 7. ieteikumā sīki aprakstītajām mērķtiecīgajām finanšu sankcijām (TFS) saistībā ar PF, kas ir noteiktas FATF standartos, kā arī paņēmieni, lai izvairītos no citiem sankciju režīmiem (piemēram, valsts un pārvalstiskām sankcijām), uz kuriem neattiecas FATF standartu 7. ieteikums.

Šīs visaptverošās pieejas mērķis ir nodrošināt jaunāko izpratni par apdraudējumiem un ievainojamībām, tostarp attiecīgo tipoloģiju kopīgām problēmām. Pētījuma mērķis ir arī identificēt vērā ņemamas izpildes problēmas un labo praksi, kas palīdz valstīm īstenot PF riska novērtējumus un riska mazināšanas procesus. Plašāks sankciju apiešanas formulējums nav paredzēts, lai no jauna definētu 7. ieteikuma prasības, un tas neiekļauj un/vai neveicina valsts vai pārvalstisku sankciju režīmu apstiprināšanu.[1]

FATF uzskata, ka ar PF un sankciju apiešanu saistītā **apdraudējuma un ievainojamību** attīstība rada milzīgas grūtības valsts un privātajam sektoram. Pašreizējo riska vidi raksturo tas, ka valsts un nevalstiskie dalībnieki iegādājas un/vai iegūst divējāda lietojuma preces, tehnoloģijas un zināšanas, izmantojot iepirkumu tīklus. Pamatojoties uz pašreizējiem globālajiem PF draudiem, FATF Globālais tīkls par visnozīmīgāko dalībnieku atzina Korejas Tautas Demokrātisko Republiku (KTDR). Uz KTDR attiecas ANO sankcijas un FATF standarti.

Lai gan nav vispārpieņemtas aplēses par kopējiem līdzekļiem, kas iegūti vai pārvietoti PF atbalstam, KTDR pēdējos gados ir dažādojusi savus centienus piekļūt finanšu sistēmai un gūt ieņēmumus savai WMD programmai. Tādējādi KTDR ģenerē miljardus dolāru, veicot kiberuzbrukumus ar virtuālo aktīvu uzņēmumiem, piemēram, 2025. gada februārī no uzņēmuma ByBit tika nozagti 1,5 miljardi ASV dolāru. Turklāt KTDR gūst ienākumus, izmantojot IT darbiniekus, dažādas citas nozares un nelikumīgas darbības, lai veicinātu savu WMD programmu.

Daudzas valstis norādīja arī attiecīgus piemērus par sankciju apiešanas shēmām, kurās iesaistīta Irāna un Krievijas Federācija, uz kurām neattiecas ANO sankcijas saistībā ar proliferāciju vai kuras nav iekļautas FATF PF riska definīcijā. Ņemot vērā atšķirīgo riska izpratnes līmeni, apdraudējuma dalībnieki veiksmīgi izmanto valsts un nozaru līmeņa ievainojamības, lai izvairītos no sankcijām, kas attiecas uz PF (skatīt I sadaļu).

[1] Plašāks sankciju apiešanas formulējums nerada nekādus jaunus pienākumus saistībā ar 1. ieteikumu vai kādu citu FATF standartu daļu. Tā vietā FATF tipoloģiju ziņojumu mērķis ir palīdzēt valsts un privātajam sektoram novērtēt un mazināt risku, pamatojoties uz savu unikālo kontekstu.

Neatļautu darbību dalībnieki izmanto sarežģītas shēmas, lai izvairītos no sankcijām un apietu eksporta kontroli saistībā ar PF. Pamatojoties uz FATF Globālā tīkla iesniegto informāciju, šajā ziņojumā ir izceltas **četras galvenās tipoloģijas**: starpnieku piesaistīšana, lai izvairītos no sankcijām; labuma guvēja informācijas (BOI) slēpšana, lai piekļūtu finanšu sistēmai; virtuālo aktīvu un citu tehnoloģiju izmantošana; un jūras un kuģniecības nozaru izmantošana (skatīt II sadaļu). Lai risinātu sarežģītas PF un sankciju apiešanas shēmas, ziņojumā aprakstītas **problēmas un labā prakse** attiecībā uz PF un sankciju apiešanas atklāšanu; izmeklēšana un kriminālvajāšana; iekšzemes koordinēšana un sadarbība; un starptautiskā sadarbība (skatīt III sadaļu).

Šis pētījums veicina FATF Globālā tīkla izpratni par sarežģītām PF un sankciju apiešanas shēmām, tostarp izmantojot attiecīgus **riska rādītājus** kompetentajām iestādēm un privātajam sektoram (skatīt A pielikumu: Riska rādītāji). Tomēr šis pētījums liecina arī par nepieciešamību turpināt uzlabot FATF Globālā tīkla kolektīvo izpratni par riskiem, kas saistīti ar PF un izvairīšanos no sankcijām. Turpmākajos gados apdraudējuma dalībnieki turpinās meklēt CPF kontroles nepilnības, piemēram, kā atšķiras jurisdikciju pieeja PF un sankciju apiešanai, tāpat tie izmantos jaunās tehnoloģijas un ģeopolitiskās situācijas izmaiņas.

Lai novērstu un apkarotu sarežģītas PF un sankciju apiešanas shēmas, FATF Globālajam tīklam būtu jāapsver (skatīt Ieteikumu sadaļu) šādas darbības:

1) **Periodiski atjaunināt izpratni par apdraudējumiem, ievainojamību un tipoloģiju**, jo valstij un privātajam sektoram ir atšķirīga risku izpratne;

2) **Veicināt būtiskāku informācijas apmaiņu, lai stiprinātu valsts un privātā sektora spēju atklāt PF un/vai izvairīšanos no sankcijām**, ņemot vērā, ka attiecīgo izmeklēšanu uzsākšanai tiek izmantoti SAR/STR;

3) Piecu gadu laikā FATF vispārīgajā glosārijā **iekļaut oficiālu WMD PF definīciju**, lai novērstu jurisdikcijas atšķirības, kas kavē starptautisko sadarbību; un

4) Trīs gadu laikā **veikt FATF Globālā tīkla PF riska novērtējumu horizontālu pārskatīšanu**, lai palīdzētu noteikt labo praksi pēc tam, kad valstīm būs bijis vairāk laika PF riska novērtēšanai.

2. Pamatinformācija

Pārskats par FATF standartiem un darbu pie PF

1. 2020. gada oktobrī FATF pieņēma grozījumus 1. un 2. ieteikumā (R.1 un R.2) un to skaidrojošajās piezīmēs (INR.1 un INR.2), lai pieprasītu valstīm, finanšu iestādēm, izraudzītiem nefinanšu uzņēmumiem un profesijām (DNFBP) un virtuālo aktīvu pakalpojumu sniedzējiem (VASP) identificēt, novērtēt un izprast savus proliferācijas finansēšanas riskus, t. i., R.7. detalizēti aprakstīto mērķtiecīgo finanšu sankciju (TFS) iespējamo pārkāpumu, neizpildes vai apiešanas risku un veikt efektīvus riska mazināšanas pasākumus, kas ir samērīgi ar identificētajiem riskiem. Pārskatītajos ieteikumos valstīm arī uzdots uzlabot sadarbību un koordināciju valstu līmenī, kā arī informācijas apmaiņas mehānismus saistībā ar PF riskiem.

2. Lai palīdzētu valsts un privātā sektora ieinteresētajām personām efektīvi īstenot pārskatītajos ieteikumos noteiktos pienākumus, FATF 2021. gadā[2] publicēja Vadlīnijas par proliferācijas finansēšanas riska novērtēšanu un mazināšanu, kurās sniegti norādījumi:

1) kā valsts un privātajam sektoram jāveic riska novērtējumi, lai identificētu, novērtētu un izprastu PF riskus;
2) kā īstenot FATF prasības, lai mazinātu identificētos PF riskus;
3) kā uzraudzības vai pašregulējuma struktūrām būtu jāuzrauga un jāpārrauga FI, DNFBP un VASP, lai nodrošinātu, ka tie pienācīgi novērtē un mazina PF riskus.

3. 2021. gada Vadlīnijas papildina 2018. gada Vadlīnijas par cīņu pret proliferācijas finansēšanu,[3] kuru galvenais mērķis ir atvieglot gan valsts, gan privātā sektora ieinteresētajām personām izprast un īstenot R.7 noteiktos pienākumus saskaņā ar UNSCR, kā arī novērst sankciju apiešanu. Pirms tam ir izdotas 2013. gada Vadlīnijas par UNSCR finanšu noteikumu īstenošanu, lai apkarotu masu iznīcināšanas ieroču proliferāciju[4].

4. Pirms šo vadlīniju dokumentu izstrādes FATF identificēja un analizēja esošos PF riskus un CPF pasākumus un publicēja secinājumus 2008. gada ziņojumā par PF tipoloģiju,[5] lai veicinātu globālo izpratni par šīm norisēm. 2010. gada konference "Proliferācijas finansēšanas apkarošana: Politikas izstrādes un konsultāciju ziņojums par stāvokli"[6] papildina 2008. gada ziņojumu, izklāstot apsveramās politikas iespējas, īstenojot CPF pasākumus saskaņā ar UNSCR, jo īpaši attiecībā uz i) tiesību sistēmām, ii) informācijas apmaiņu un izpratnes veicināšanu starp valsts un privāto sektoru, iii) preventīviem pasākumiem un iv) izmeklēšanu un kriminālvajāšanu.

Commented [LŽ3]: https://termini.gov.lv/kolekcijas/17/skirklis/114553

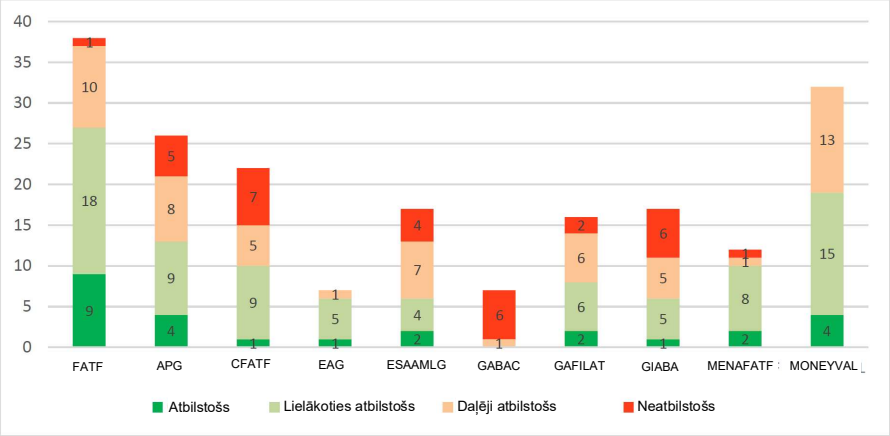
Pašreizējais FATF standartu ieviešanas statuss

5. Savstarpējā novērtējuma (ME) 4. kārtas novērtējuma rezultāti liecina, ka valstis joprojām saskaras ar grūtībām saistībā ar R.7 un TFS īstenošanu un ieviešanu saskaņā ar UNSCR par proliferāciju. 2025. gada aprīlī[7] no 194 FATF un FSRB locekļiem, kas tika novērtēti ME 4. kārtā, tikai 13 % (26 valstis) atbilst R.7, un gandrīz puse (46 %; 89 valstis) tam atbilst daļēji vai neatbilst.

---

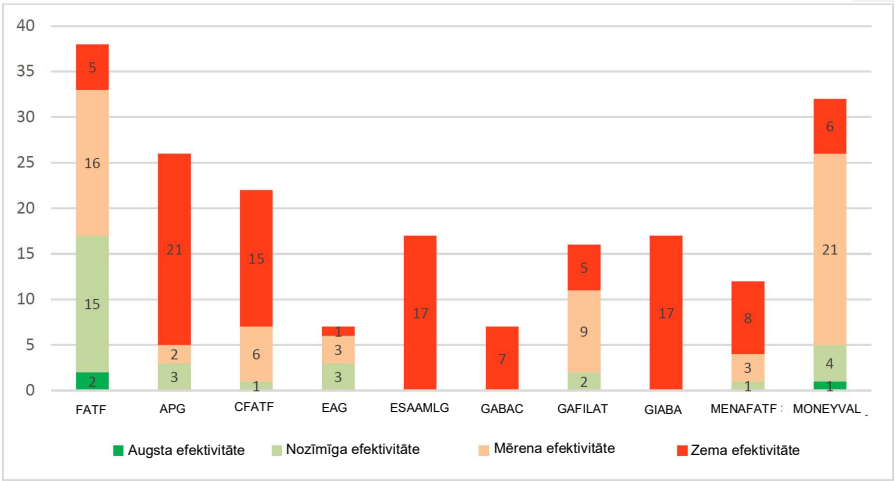
2 FATF (2021) Vadlīnijas par proliferācijas finansēšanas riska novērtēšanu un mazināšanu.
3 FATF (2018) Vadlīnijas par proliferācijas finansēšanas apkarošanu.
4 FATF (2013) Vadlīnijas par UNSCR finanšu noteikumu īstenošanu, lai apkarotu masu iznīcināšanas ieroču proliferāciju.
5 FATF (2008) Proliferācijas finansēšanas tipoloģijas ziņojums.
6 FATF (2010) Proliferācijas finansēšanas apkarošana: Politikas izstrādes un konsultāciju ziņojums par stāvokli.
7 FATF (2024) Konsolidēto vērtējumu reitings.

1. attēls. Novērtēšanas rezultāti: Tehniskā atbilstība R.7 (uz 2025. gada aprīli)



6. Līdzīgi kopējā efektivitāte joprojām ir zema, un tikai 16 % novērtēto valstu ir pierādījušas augstu/būtisku efektivitāti IO.11 (TFS saskaņā ar UNSCR par proliferāciju). FATF un FSRB locekļu efektivitātes rādītāji ievērojami atšķiras (45 % no 38 FATF locekļiem un 10 % no 156 novērtētajiem FSRB locekļiem ir ieguvuši augstu/būtiski efektīvu novērtējumu).

2. attēls. Novērtēšanas rezultāti: 11. tūlītējais rezultāts – efektivitāte (no 2025. gada aprīļa)



Ievads

Pārskats par mērķi

7. Šā ziņojuma mērķis ir balstīties uz diviem esošajiem vadlīniju ziņojumiem un atjaunināt tos: 1) 2018. gada FATF Vadlīnijas par proliferācijas finansēšanas apkarošanu – 1718. UNSCR finanšu noteikumu īstenošana, lai cīnītos pret PFWMD, un 2) 2021. gada Vadlīnijas par proliferācijas finansēšanas riska novērtējumu un mazināšanu. Pētījums sniedz lasītājiem vispusīgu izpratni par pašreizējām sarežģīto sankciju apiešanas shēmu tipoloģijām, kas attiecas uz PF, un tajā ir identificētas izpildes problēmas un labākā prakse, kas palīdz valstīm veikt PF riska novērtējumu un riska mazināšanu. Ziņojumā izmantoti šādi galvenie termini:

1. ierāmējums. Galveno terminu definīcijas

Ziņojumā izmantotas plašas darba definīcijas, kas parādās 2021. gada PF vadlīnijās, kuras balstās uz 2010. gada ziņojumu par stāvokli:

Masu iznīcināšanas ieroču (WMD) proliferācija

Kodolieroču, ķīmisko vai bioloģisko ieroču, to piegādes līdzekļu un saistīto materiālu (tostarp divējāda lietojuma tehnoloģiju un divējāda lietojuma preču, ko izmanto neleģitīmiem mērķiem) ražošana, iegāde, glabāšana, izstrāde, eksports, pārkraušana, starpniecība, pārvadāšana, transportēšana, pārsūtīšana, uzkrāšana vai izmantošana (tostarp gan divējāda lietojuma tehnoloģiju, gan divējāda lietojuma preču, kas paredzētas neleģitīmiem mērķiem, izplatīšanai).

Proliferācijas finansēšana (PF)

Līdzekļu, citu aktīvu vai citu saimniecisko resursu vai finansējuma piesaiste, pārvietošana vai darīšana pilnībā vai daļēji pieejamu personām vai organizācijām WMD izplatīšanas nolūkā, tostarp to nogādes līdzekļu un saistīto materiālu izplatīšanas nolūkā (tostarp gan divējāda lietojuma tehnoloģiju, gan divējāda lietojuma preču, kas paredzētas neleģitīmiem mērķiem, izplatīšanai).[8]

Ziņojumā atkārtoti uzsvērts, ka attiecīgajos starptautiskajos režīmos un forumos nav vienotas universālas WMD proliferācijas vai PF definīcijas, un attiecīgajās sadaļās atzīmēta iespējamā ietekme un vajadzība pēc standarta definīcijas.

PF riski

Izņemot gadījumus, kad norādīts citādi, saskaņā ar pārskatīto 1. ieteikumu un tā skaidrojošo piezīmi (R.1 un INR.1) ziņojumā PF risks ir minēts tikai un vienīgi kā 7. ieteikumā minēto TFS pienākumu iespējamais pārkāpums, neizpilde vai izvairīšanās no tiem.

8. Pamatojoties uz dažādu valstu un starptautisko institūciju plašo darbu, ziņojums ir izstrādāts tā, lai to varētu izmantot FATF Globālā tīkla dalībnieki, kompetentās iestādes, FI, DNFBP, VASP, nevalstiskās organizācijas un citas personas un struktūras, lai risinātu ar PF saistīto sankciju apiešanas problēmu.

---

[8] Šī PF darba definīcija balstās uz FATF 2010. gada ziņojumā par stāvokli sniegto definīciju, kas joprojām ir būtiska šim pētījumam, jo īpaši valstīm, kuras izmanto plašāku pieeju ar PF un sankciju apiešanu saistīto risku mazināšanai. 2010. gada ziņojumā PF ir definēts kā "darbība, kas izpaužas kā tādu līdzekļu vai finanšu pakalpojumu sniegšana, kuri pilnībā vai daļēji tiek izmantoti kodolieroču, ķīmisko vai bioloģisko ieroču un to nogādes līdzekļu un ar tiem saistīto materiālu (tostarp gan tehnoloģiju, gan divējāda lietojuma preču, ko izmanto neleģitīmiem mērķiem) ražošanai, iegādei, glabāšanai, izstrādei, eksportam, pārkraušanai, starpniecībai, transportēšanai, pārsūtīšanai, uzkrāšanai vai izmantošanai, pārkāpjot valsts tiesību aktus vai attiecīgā gadījumā starptautiskās saistības."

Mērķi un struktūra

9. Šā ziņojuma mērķis ir sniegt globālu pārskatu par sankciju apiešanas tendencēm un metodēm saistībā ar PF, lai palīdzētu valstīm mazināt PF riskus. Ziņojumā ir sniegti sarežģītu sankciju apiešanas shēmu rādītāji, apdraudējums un ievainojamības, kā arī apzināta labā prakse un problēmas, kas saistītas ar sankciju apiešanas gadījumu atklāšanu, izmeklēšanu un saukšanu pie atbildības lietās, kas attiecas uz PF. Šie mērķi tiek īstenoti, ziņojumu strukturējot četrās būtiskās daļās:

- **Pirmā sadaļa**: izklāsta projekta tvērumu saskaņā ar īstenošanas plānu. Tajā arī sniegts pārskats par pašreizējo situāciju un, pamatojoties uz gadījumu izpēti un literatūras analīzi, identificēti draudi un ievainojamības jomas, kas saistītas ar izvairīšanos no sankcijām un PF.

- **Otrā sadaļa**: sniedz pārskatu par sarežģītu sankciju apiešanas shēmu tipoloģiju, kas attiecas uz PF.

- **Trešā sadaļa**: apzina problēmas un labo praksi ar PF saistītu noziegumu atklāšanā, ziņošanā, izmeklēšanā un kriminālvajāšanā. Tajā arī izklāstīti dažādi iekšzemes koordinācijas un sadarbības mehānismi, kā arī ar šo tematu saistītā starptautiskā sadarbība.

- **Secinājumi un prioritārās jomas:** apkopo vispārīgo PF un sankciju apiešanas situāciju un norāda jomas, kurās nepieciešams turpmāks darbs.

- **Riska rādītāji**: šis pielikums ir izstrādāts, lai uzlabotu valsts un privātā sektora struktūru spēju identificēt aizdomīgus darījumus un/vai darbības, kas saistītas ar attiecīgajām PF un sankciju apiešanas shēmām.

Metodoloģija

10. Metodoloģija ietvēra esošo pieejamo materiālu par PF un PF riskiem pārskatīšanu un pilnveidošanu, tostarp:

- Literatūras apskats, lai apzinātu ar PF saistīto sankciju apiešanas veida un apmēra attīstības tendences, tostarp no nesenajiem 1718. UNSCR ekspertu grupas (POE) ziņojumiem. Šajā pārskatā galvenā uzmanība tika pievērsta apdraudējumiem, ievainojamībām, kā arī jaunām tendencēm un metodēm.

- Lūgums FATF Globālā tīkla dalībniekiem sniegt informāciju par izvairīšanos no sankcijām saistībā ar PF. Tas ietvēra a) materiālus par stratēģiskās izlūkošanas produktiem vai gadījumu izpēti, kas sniedza informāciju par sankciju apiešanas tipoloģiju un gadījumiem saistībā ar PF, b) draudus un ievainojamības, kas identificētas riska novērtējumos un riska mazināšanas pasākumos, c) atklāšanas, izmeklēšanas un informācijas apmaiņas mehānismus un d) labo praksi un problēmas.

- Papildus FATF Globālā tīkla dalībnieku iesniegtajiem riska rādītājiem tika izskatīti arī šādi papildinoši ziņojumi: i) citu organizāciju un iestāžu PF riska novērtēšanas vadlīnijas, ii) pētījumi par PF tipoloģiju un iii) valstu publicētās TFS vadlīnijas.

- Privātais sektors, pilsoniskā sabiedrība un akadēmiskās aprindas tika aicinātas atbildēt uz vairākiem jautājumiem publiskās apspriešanas laikā, lai piedalītos ziņojuma sagatavošanā, jo īpaši saistībā ar grūtībām un labo praksi iekšzemes koordinācijas un sadarbības jomā.

3. 1. sadaļa. Ar PF saistīto sankciju apiešana – pašreizējā situācija, draudi un ievainojamības

Darbības joma

Ziņojuma ietvars

11. Riska novērtēšanas procesā valstis apsver nelikumīgi iegūtu līdzekļu legalizēšanas (ML), terorisma finansēšanas (TF) un PF riskus, kas rodas, kad attiecīgais drauds veiksmīgi izmanto ievainojamību, lai radītu sekas.[9] Saskaņā ar FATF Globālā tīkla datiem visnopietnākos PF draudus starptautiskajai finanšu sistēmai rada valsts sponsorēti vai ar to saistīti dalībnieki, ieskaitot, bet neaprobežojoties ar tiem, kas saistīti ar sankciju apiešanu un PF darbībām, kas attiecas uz KTDR, vienīgo valsti, kurai ANO ir noteikusi sankcijas.

12. Saskaņā ar pārskatīto FATF 1. ieteikumu PF risks attiecas tikai un vienīgi uz 7. ieteikumā minēto TFS pienākumu iespējamu pārkāpumu, neizpildi vai izvairīšanos no to izpildes, kas attiecas tikai uz šo ANO sankcijām pakļauto valsti – KTDR. Pamatojoties uz šo FATF standartos iekļauto PF riska šauro definīciju, jurisdikcijas identificēja, ka galvenie apdraudējuma dalībnieki ir KTDR un valsts dalībnieki, personas un organizācijas, kas atbalsta KTDR vai sadarbojas ar to, lai apietu ANO sankcijas.

13. Kā aprakstīts FATF 2021. gada PF vadlīnijās,[10] izpratne par plašāku WMD proliferācijas risku un tā pamatā esošo finansējumu var palīdzēt saprast risku, kas saistīts ar FATF PF-TFS pienākumiem. Labāka izpratne par PF risku var arī palīdzēt īstenot uz risku balstītus pasākumus un TFS. Daudzi FATF locekļi izmanto plašāku PF definīciju, lai mazinātu risku plašāk nekā pašreizējie FATF standarti. Līdz ar to jurisdikciju iesniegto dokumentu apjoms atspoguļoja to izpratni par pašreizējiem globālajiem PF draudiem, tostarp KTDR (uz kuru attiecas ANO sankcijas un FATF standarti), kā arī citiem valsts sektora dalībniekiem. Daudzas valstis Irānu un Krievijas Federāciju identificēja kā aktuālu PF apdraudējumu, lai gan uz tām neattiecas ANO sankcijas saistībā ar proliferāciju vai FATF PF riska definīcija.

14. Šā ziņojuma mērķis ir sniegt aktuālu pārskatu par sarežģītajām sankciju apiešanas shēmām, ko izmanto proliferācijas finansētāji, un attiecīgā gadījumā tajā aplūkotas arī sankciju apiešanas shēmas, kas saistītas ar TF un PF plašākā nozīmē neatkarīgi no sankciju režīma, lai nodrošinātu iegūto tipoloģiju ilgtspēju un derīgumu laika gaitā, un risinātu kopējās problēmas. Tāpēc šajā ziņojumā ir aplūkoti visi dalībnieki, kurus jurisdikcijas visbiežāk minējušas, lai palīdzētu FATF Globālajam tīklam identificēt un mazināt PF risku.[11]

FATF Globālā tīkla pieredze PF riska novērtēšanā

15. Efektīvs veids, kā novērtēt attiecīgās ievainojamības, ir PF riska novērtēšana. Lai gan vairums FATF Globālā tīkla valstu ziņoja, ka tās ir novērtējušas vai pašlaik vērtē PF riskus nacionālā riska novērtēšanas procesa ietvaros, ir pazīmes, kas liecina, ka novērtējuma apjoms un/vai izpratne par PF ievainojamību ir agrīnā stadijā.

---

9 FATF (2024) Noziedzīgi iegūtu līdzekļu legalizācijas novēršanas nacionālā riska novērtējuma vadlīnijas.

10 FATF (2021) Vadlīnijas par proliferācijas finansēšanas riska novērtēšanu un mazināšanu.

11 Kā norādīts kopsavilkumā un citviet dokumentā, šajā ziņojumā ir iekļauta informācija par izmantotajām metodēm, kā apiet valstu un pārvalstiskos sankciju režīmus, lai sniegtu aktuālu izpratni par draudiem un ievainojamību, tostarp par kopīgām problēmām starp attiecīgajām tipoloģijām, uz kurām neattiecas FATF standartu 7. ieteikums. Plašāks sankciju apiešanas formulējums nav paredzēts, lai no jauna definētu 7. ieteikuma prasības.

Piemēram, gandrīz puse valstu, kas atbildēja uz anketas jautājumiem, lai sagatavotu šo ziņojumu, neapstiprināja, vai tām ir PF ievainojamība, bet vēl sešas valstis secināja, ka tām nav PF ievainojamības.

16. Atsevišķos gadījumos valstis norādīja uz zemu PF un sankciju apiešanas ievainojamības līmeni vairāku iemeslu dēļ, tostarp ģeogrāfiskā attāluma dēļ no sankcijām pakļautajām valstīm; nav diplomātisko vai tirdzniecības attiecību ar sankcijām pakļautajām valstīm; nepietiekami attīstīts finanšu sektors ar ierobežotu integrāciju pasaules finanšu tirgū; spēcīgs valsts mehānisms ar PF saistīto TFS īstenošanai; un jurisdikcijā nav identificētu PF gadījumu.

17. Daudzi no šiem faktoriem ir leģitīmi, lai mazinātu iespēju, ka PF apdraudējuma dalībnieki var izmantot valsts vai nozares ievainojamību. Tomēr ir svarīgi ņemt vērā, ka pēdējos gados globālais konteksts ir ievērojami mainījies, jo ir parādījušās jaunas tehnoloģijas, tostarp jaunas maksājumu sistēmas, un pieaugusi ģeopolitiskā spriedze. Turklāt iepriekšminētajos faktoros nav ņemti vērā plašāki AML/CFT/CPF kontroles trūkumi valsts un privātajā sektorā vai PF un sankciju apiešanas draudu izplatība, dalībniekiem izmantojot dažādus starpniekus trešajās valstīs, lai apietu sankcijas un eksporta kontroli (skatīt 1. tipoloģiju). Tā kā PF apdraudējuma dalībnieki labprāt izmanto potenciālās "aklās zonas" starptautiskajā finanšu sistēmā, var būt nepieciešams lielāks atbalsts un pasākumi, lai identificētu un mazinātu PF ievainojamību un stiprinātu kolektīvos centienus šo ievainojamību mazināšanai.

Pašreizējā situācija

18. Neraugoties uz visaptverošiem starptautiskiem, pārnacionāliem un valstu sankciju režīmiem un eksporta kontroli, kas vērsta pret WMD programmām, valsts sponsorēti vai ar to saistīti dalībnieki veiksmīgi īsteno sarežģītas iepirkumu un ieņēmumu gūšanas shēmas, lai atbalstītu PF dalībniekus un/vai darbības. Galvenie apdraudējuma dalībnieki jo īpaši izmanto starpniekus trešajās valstīs, slēpj BOI, izmanto jaunās tehnoloģijas un ekspluatē jūrniecības un kuģniecības nozari, lai apietu sankcijas, iegūtu līdzekļus un divējāda lietojuma preces (skatīt 2. sadaļu).

19. FATF pašreizējos draudus un ievainojamības vērtē šādi:

Pašreizējā situācija – KTDR

20. Kopš 2006. gadā KTDR veica savu pirmo kodolizmēģinājumu, tai ir piemērotas ievērojamas starptautiskas sankcijas. 1718. UNSCR, kas tika pieņemta 2006. gadā, pieprasīja, lai KTDR pārtrauktu kodolizmēģinājumus, un ar to cita starpā tika ieviesti TFS pret KTDR kopumā, kā arī konkrēti pret personām un vienībām, kas saistītas ar KTDR WMD programmu.

21. Neskatoties uz to, ka jau gandrīz 20 gadus ir pakļauta ANO sankcijām, KTDR, izmēģinot starpkontinentālas ballistiskās raķetes, turpina attīstīt savas spējas izveidot kodolierīces. Piemēram, 2024. gada 31. oktobrī KTDR palaida ICBM ar nosaukumu Hwasong-19, kas sasniedza aptuveni 7000 km augstumu, bet kopējais attālums bija aptuveni 1000 km. Šis pēdējais izmēģinājums ir 11. IKBM palaišana, ko KTDR veica kopš 2021. gada, kad paziņoja par jaunu piecu gadu militāro paplašināšanās plānu.[12]

[12] KTDR Korejas jaunākais raķetes palaišanas gadījums ir "nopietns drauds" reģiona stabilitātei | UN News.

22. Lai gan KTDR ir turpinājusi šādas darbības, starptautiskās sabiedrības darbības nav sekojušas KTDR radīto draudu tempam vai trajektorijai. ANO sankciju saraksts pret KTDR nav papildināts gandrīz desmit gadu laikā. Turklāt 2024. gadā tika likvidēta 1718. UNSCR komiteju ekspertu grupa (POE). 1718. UNSCR POE darbības izbeigšana ir liels izaicinājums attiecībā uz KTDR piemērojamo sankciju pārkāpumu uzraudzību.[13] Daudzas valstis paļāvās uz 1718. UNSCR POE divgadu ziņojumiem, kas tās informēja par PF valsts riska novērtējumiem. Kā 2024. gada jūnijā norādīja FATF plenārsēde, "spēju iegūt uzticamu un ticamu informāciju, lai pamatotu ar KTDR saistīto PF risku novērtējumu, apgrūtina nesenā 1718. komitejas ekspertu grupas pilnvaru termiņa izbeigšanās."[14]

23. Veicot šo pētījumu, FATF delegācijas norādīja uz diviem galvenajiem pastiprinošiem faktoriem, kas veicina KTDR WMD programmas finansēšanu: pieaugošā KTDR finansiālā savienojamība un KTDR ieņēmumu dažādība.

KTDR finanšu savienojamības palielināšanās

24. Lai gan FATF kopš 2011. gada ir nepārtraukti atkārtojusi, ka visām valstīm ir stingri jāīsteno TFS saskaņā ar UNSCR un jāpiemēro pretpasākumi, lai aizsargātu savu finanšu sistēmu pret nelikumīgu finansējumu, kas nāk no KTDR, jurisdikcija pēdējā laikā ir palielinājusi savienojamību ar starptautisko finanšu sistēmu, kas palielina PF riskus, kā FATF arī norādīja 2024. gada jūnijā.[15]

25. KTDR un Krievijas Visaptverošajā stratēģiskās partnerības līgumā,[16] kas stājās spēkā 2024. gada beigās, abas valstis apņemas stiprināt sadarbību, tostarp radot labvēlīgus apstākļus ekonomiskajai sadarbībai muitas finanšu un banku jomā; kopīgi strādājot, lai radītu labvēlīgus apstākļus tiešu saišu izveidei starp KTDR un Krievijas Federāciju; un veicinot savstarpēju izpratni par reģionu ekonomisko un investīciju potenciālu. Ekonomisko saišu stiprināšana, jo īpaši atjaunojot banku sakarus ar KTDR finanšu iestādēm vai uzņēmumiem, kas ir bijuši saistīti ar PF, varētu radīt jaunas ievainojamības pasaules finanšu sistēmā, jo vairākas KTDR finanšu iestādes un to ārvalstu pārstāvji ir iekļauti 1718. UNSCR sarakstā.[17]

26. Kopš 2016. gada to valstu skaits, kurās uzturas KTDR baņķieri, ir samazinājies no 14 līdz četrām, jo uzņemošās valstis ir piemērojušas sankcijas un KTDR personāls ir atkāpies, pēdējo reizi no Indonēzijas un Lībijas 2023. gada beigās. Tomēr no 2023. gada līdz vismaz 2024. gada vidus KTDR baņķieri kaimiņvalstī un Krievijā veicināja darījumus simtiem miljonu dolāru vērtībā, lai atbalstītu KTDR tirdzniecību un ieņēmumu gūšanu. No 2024. gada vidus vairāk nekā 50 KTDR banku pārstāvju darbojās ārpus valsts, lai gan 2321. UNSRC pieprasīja uzņemošajām valstīm viņus izraidīt.[18]

---

13 Drošības padome nepagarina pilnvaru termiņu ekspertu grupai, kas palīdz Sankciju komitejai pret Korejas Tautas Demokrātisko Republiku | Sēžu atspoguļojums un paziņojumi presei.

14 Augsta riska valstis, uz kurām attiecas aicinājums rīkoties – 2024. gada jūnijs.

15 Augsta riska valstis, uz kurām attiecas aicinājums rīkoties – 2024. gada jūnijs.

16 http://en.kremlin.ru/acts/news/75534

17 Attiecīgās ANO sarakstā iekļautās struktūras ir Tanchon Commercial Bank (KPe.003), Bank of East Land (KPe.013), Amroggang Development Banking Corporation (KPe.009).

18 2321. UNSCR pieprasa uzņemošajām valstīm veikt aktīvus pasākumus, piemēram, izraidīt KTDR banku pārstāvjus un aizliegt valsts un privāto finansiālo atbalstu tirdzniecībai ar KTDR no to teritorijām vai to jurisdikcijā esošām personām vai uzņēmumiem.

Turklāt 2270. UNSCR pieprasa uzņemošajām valstīm slēgt esošās pārstāvniecības un aizliedz KTDR atvērt vai vadīt jaunas filiāles, meitasuzņēmumus vai pārstāvniecības ANO dalībvalstu teritorijās.[19] Viena delegācija norādīja, ka 2024. gada janvārī kāds Krievijā bāzēts baņķieris ļāva noslēgt darījumu par KTDR celtnieku nosūtīšanu uz Krieviju, kur viņi nopelna ārvalstu valūtu un ļauj KTDR turpināt apiet ANO sankcijas.

KTDR ieņēmumu gūšanas darbību daudzveidība dod labumu tās WMD programmai

27. Daudzas valstis ziņoja, ka noziedzīgās darbības, kas visvairāk skar PF un sankciju apiešanas shēmas, ir saistītas ar viltošanu, krāpšanu, (kiber)zādzībām un ieroču, narkotiku, savvaļas dzīvnieku, kontrabandas un citu priekšmetu tirdzniecību. Ar KTDR saistītas personas un uzņēmumi veic šāda veida nelikumīgas darbības un izmanto likumīgus uzņēmumus, lai gūtu ieņēmumus WMD programmai, jo īpaši vēršoties pret valstīm vai nozarēm, kurās ir vāja AML/CFT/CPF kontrole vai tās nav vispār, piemēram, jaunajām tehnoloģijām un jūrniecības un kuģniecības nozarēm (skatīt 3. un 4. tipoloģiju). Papildus tam, ka pēdējos gados KTDR koncentrējas uz ieņēmumu gūšanu, izmantojot IT darbiniekus, tā ir arī pazīstama ar to, ka ieņēmumu gūšanai pievēršas dažādām nozarēm vai nelikumīgām darbībām, tostarp:

- **Parūku un mākslīgo skropstu nozare**: dažas valstis uzrauga, kā KTDR izmanto rentablo parūku un mākslīgo skropstu eksportu, lai uzlabotu savu finansiālo stāvokli un mazinātu starptautisko sankciju ietekmi, kuru mērķis ir ierobežot tās stratēģisko ieroču programmu. Līdz 2024. gada pirmajai pusei šie produkti veidoja gandrīz 60 % no visa KTDR eksporta uz kādu kaimiņvalsti. Šo produktu ražošanai KTDR importē izejvielas no tās pašas kaimiņvalsts, lai izgatavotu pusfabrikātus, kurus pēc tam KTDR nosūta atpakaļ uzņēmumiem galīgai apstrādei un eksportam uz trešajām valstīm. KTDR tirdzniecības uzņēmumi, kas ražo parūkas, ir pakļauti struktūrām, kas iekļautas 1718. UNSCR sarakstā, un tas liecina, ka ieņēmumi no parūkām var atbalstīt KTDR stratēģisko ieroču programmu. Lai gan ANO sankcijas neaizliedz uzņēmumiem pirkt KTDR izcelsmes parūkas un mākslīgās skropstas, galaproduktu ražošanā un iegādē iesaistītie uzņēmumi, iespējams, nezina par saikni ar ANO sankciju subjektiem.

- **Nelegāla savvaļas dzīvnieku un augu tirdzniecība:** lielākā daļa KTDR veiktās nelikumīgās savvaļas dzīvnieku un augu tirdzniecības avotu nāk no Subsahāras Āfrikas valstīs, ņemot vērā daudzu šo valstu vēsturiskās saiknes ar KTDR. Nelegāla tirdzniecība ar savvaļas dzīvniekiem un augiem ir zema riska un augstas atdeves veids, kā KTDR var iegūt līdzekļus. Tā kā KTDR diplomātiskā klātbūtne Subsahāras Āfrikā pēdējos gados samazinās, šo kanālu var būt grūtāk izmantot ar diplomātiskā personāla starpniecību. Turklāt dažas valstis piekrīt RUSI novērtējumam, ka KTDR pilsoņiem, kas darbojas slēpti kā trešo valstu valstspiederīgie, turpmākajos gados var būt lielāka loma šo preču sagādē un pārvadāšanā (piemēram, maskējoties par personām no zināmām savvaļas dzīvnieku un augu tirdzniecības tranzīta un galamērķa valstīm).[20]

[19] Kā aprakstīts FATF 2024. gada jūnija paziņojumā par augsta riska jurisdikcijām, "FATF kopš 2011. gada ir nepārtraukti atkārtojusi, ka visām valstīm ir stingri jāīsteno mērķtiecīgās finanšu sankcijas saskaņā ar ANO DP rezolūcijām un jāpiemēro šādi pretpasākumi, lai aizsargātu savas finanšu sistēmas no nelikumīgi iegūtu līdzekļu legalizēšanas, terorisma finansēšanas un proliferācijas finansēšanas draudiem, kas nāk no KTDR: Pārtraukt korespondentattiecības ar KTDR bankām; slēgt visus KTDR banku meitasuzņēmumus vai filiāles savās valstīs; un ierobežot darījumu attiecības un finanšu darījumus ar KTDR personām. Neraugoties uz šiem aicinājumiem, KTDR ir palielinājusi savienojamību ar starptautisko finanšu sistēmu, kas palielina proliferācijas finansēšanas (PF) riskus, kā 2024. gada februārī norādīja FATF. Tādēļ ir vajadzīga lielāka modrība un šo pretpasākumu pret KTDR atkārtota īstenošana un pastiprināta izpilde. Kā noteikts 2270. UNSCR, KTDR bieži izmanto fiktīvus uzņēmumus, čaulas uzņēmumus, kopuzņēmumus un sarežģītas, neskaidras īpašumtiesību struktūras, lai pārkāptu sankcijas. Tādēļ FATF mudina savus locekļus un visas valstis piemērot padziļinātu uzticamības pārbaudi attiecībā uz KTDR un tās spēju veicināt darījumus KTDR vārdā."

[20] ANO izmeklē apgalvojumus par Ziemeļkorejas savvaļas dzīvnieku un augu tirdzniecību Āfrikā | NK News.

Pašreizējā situācija – Irāna

28. ANO sākotnēji Irānai piemēroja sankcijas saskaņā ar 1737. UNSCR pēc tam, kad šī valsts atteicās ievērot 1696. UNSCR, kurā bija prasīts, lai Irāna pārtrauc urāna bagātināšanas programmu. Šī UNSCR bija pirmā no vairākām rezolūcijām, ar kuru Irānas personām un uzņēmumiem, kas saistīti ar tās kodolprogrammu, tika piemēroti TFS.

29. Ar 2231. UNSCR ANO Drošības padome apstiprināja Kopīgo visaptverošo rīcības plānu, kurā Irāna piekrita ierobežot savu kodolprogrammu apmaiņā pret sankciju atvieglojumiem un citiem noteikumiem. Saskaņā ar 2231. UNSCR 2023. gada oktobrī tika izbeigta ar Irānas kodolprogrammu saistītām personām un uzņēmumiem piemēroto TFS darbība, un tās vairs neattiecas uz FATF 7. ieteikumu. Tomēr vairākas valstis izmanto valsts sankciju programmas, lai īstenotu TFS pret Irānu, ņemot vērā Irānas un ar to saistīto personu un uzņēmumu radītos draudus.

30. Lai mazinātu ekonomisko sankciju ietekmi, Irāna ir paļāvusies uz militarizētiem starpniekiem Tuvajos Austrumos, kā arī uz virkni starptautisku kriminālu organizāciju (SKO), kas atrodas Irānā un ārvalstīs. Irānas naftas kontrabandas centienos ir piedalījušies ārvalstu uzņēmēji ar plašiem sakariem, savukārt bankas, zelta tirgotāji un valūtas maiņas nami var kalpot kā svarīgi noziedzīgi iegūtu līdzekļu legalizēšanas un sarežģītu sankciju apiešanas kanāli. Kā aprakstīts dažādos gadījumu pētījumos, Irāna, apejot sankcijas un eksporta kontroli, var atbalstīt raķešu, ieroču, militārā gaisa aprīkojuma un WMD programmas izstrādi.

31. Irānas starpnieki ir guvuši labumu no piekļuves noziedzīgiem tirgiem, jo īpaši ārvalstu valūtas maiņas namiem, kas iepriekš kalpoja kā ISIS un Al-Qaida finansēšanas kanāli. Hezbollah šajā ziņā ir bijusi īpaši svarīga loma, jo tai ir plašas kontrabandas operācijas, globāls legālas un nelegālas uzņēmējdarbības tīkls un dominējoša loma globālajā noziedzīgi iegūtu līdzekļu legalizēšanā, izmantojot valūtas maiņas namus. Hezbollah ir saistīta ar naftas, ieroču un dažādu sankcijām pakļautu preču kontrabandu.[21]

32. Turklāt Hezbollah ir iefiltrējusies finanšu iestādēs daudzās pasaules valstīs un ir īstenojusi noziedzīgi iegūtu līdzekļu legalizēšanas shēmas, kas aptver vairākus kontinentus un tirdzniecības nozares. Hezbollah darbinieki ir pat meklējuši piekļuvi ieročiem un aprīkojumam, pārkāpjot sankcijas Irānas vārdā, kas ir ļoti riskanta darbība. Šīs sakarības liecina, ka noziedzīgie tirgi, kas ir Irānas ārvalstu operāciju pamatā, kalpo kā dažādu draudu katalizatori.

Pašreizējā situācija – Krievija

33. Starptautisko sankciju spiediena rezultātā, kas tika vērsts pret Krievijas ekonomiku sakarā ar militāro iebrukumu Ukrainā, Krievijas Federācijai nācās veikt pasākumus, lai saglabātu savu ekonomiku un militāro stāvokli. Kā aprakstīts iepriekš šajā sadaļā, viens no šādiem soļiem ir visaptveroša stratēģiskās partnerības līguma parakstīšana ar KTDR.[22]

---

[21] Kā norādīts kopsavilkumā un citviet dokumentā, šajā ziņojumā ir iekļauta informācija par izmantotajām metodēm, kā apiet valstu un pārvalstiskos sankciju režīmus, lai sniegtu aktuālu izpratni par draudiem un ievainojamību, tostarp par kopīgām problēmām starp attiecīgajām tipoloģijām, uz kurām neattiecas FATF standartu 7. ieteikums. Plašāks sankciju apiešanas formulējums nav paredzēts, lai no jauna definētu 7. ieteikuma prasības.

[22] http://kcna.kp/en/article/q/6a4ae9a744af8ecdfa6678c5f1eda29c.kcmsf

Ar šo līgumu tiek veidotas ekonomiskās un militārās saiknes starp abām valstīm, tostarp noteikumi par stratēģiskās un taktiskās sadarbības uzlabošanu, militārās palīdzības sniegšanu un kopīgiem pasākumiem aizsardzības spēju stiprināšanai (informāciju par ekonomisko koordināciju skatīt 26. punktā).

34. KTDR 2025. gada aprīlī apstiprināja Ziemeļkorejas karavīru izvietošanu Krievijas un Ukrainas konfliktā saskaņā ar divpusējo līgumu, savukārt Krievijas amatpersonas apstiprināja KTDR karavīru aktivitātes Kurskas reģionā.[23, 24] Iepriekš 2024. gada marta ANO 1718. POE ziņojumā tika minēti ANO centieni izmeklēt KTDR izcelsmes munīcijas klātbūtni Ukrainā.[25] Tā kā starp Krieviju un KTDR, kam ANO kā galvenajam PF draudu dalībniekam jau divas desmitgades piemēro sankcijas, pastāv ekonomiska un militāra saikne, daudzas valstis uzskata Krieviju par PF draudu paplašinājumu.

Citi draudi

35. Turklāt daudzas valstis joprojām ir nobažījušās par nevalstisko dalībnieku, piemēram, teroristu grupējumu un kriminālo organizāciju, centieniem nopirkt un/vai iegūt ar WMD saistītas preces, zināšanas un tehnoloģijas, tostarp bioloģiskās, ķīmiskās un kodolieroču iespējas. ANO Drošības padome 2022. gada novembrī atjaunoja 1540. UNSCR mandātu, koncentrējoties uz WMD, zināšanu vai prekursoru materiālu izplatīšanas novēršanu nevalstiskiem dalībniekiem.[26] Kā norādīts FATF 2021. gada PF vadlīnijās, 1540. UNSCR pienākumi pastāv atsevišķi un neatkarīgi no 7. ieteikumā un tā skaidrojošajā piezīmē noteiktajiem pienākumiem.[27] Lai gan ir maz piemēru, kad nevalstiski dalībnieki izmanto finanšu sistēmu, lai atbalstītu PF dalībniekus vai darbības, daudzas valstis uzskata, ka šīs darbības potenciālā ietekme aktualizē nepieciešamību to pastāvīgi uzraudzīt. Turklāt iespējams, ka no šīm darbībām izriet tipoloģijas, kas ir būtiskas, lai izprastu un mazinātu vispārējos PF un sankciju apiešanas riskus. Tāpēc šajā ziņojumā ir iekļauti daži nevalstisko dalībnieku gadījumu pētījumi.

Ievainojamības

36. Kā aprakstīts FATF 2021. gada PF vadlīnijās, ievainojamība attiecas uz faktoriem, kurus var izmantot attiecīgais apdraudējums vai apdraudējuma dalībnieki, kas var atbalstīt vai veicināt PF-TFS pārkāpšanu, neizpildi vai apiešanu. Saskaņā ar spēkā esošajiem FATF standartiem tas attiecas uz apdraudējumu, ko rada KTDR un ar to saistītie dalībnieki, kas atbalsta KTDR, lai izvairītos no ANO sankcijām. Tām valstīm, kuras PF risku aplūko plašākā kontekstā, tas attiektos uz ievainojamībām, ko izmanto visi PF dalībnieki, kuri cenšas izmantot valsts un privātā sektora vājās vietas.

37. Valstīm jāapsver ievainojamības valsts (tostarp strukturālā) un nozaru līmenī. Valsts vai strukturālā ievainojamība var ietvert nepilnības AML/CFT/CPF tiesiskajā regulējumā. Citas valsts līmeņa ievainojamības var ietvert jurisdikcijai raksturīgus faktorus, piemēram, ekonomikas lielumu un sarežģītību, skaidras naudas un neformālās ekonomikas izplatību, vai juridisko personu un struktūru daudzveidību. [28] Daudzas valstis norādīja, ka īpaši attiecībā uz ar PF saistīto ievainojamību ir svarīga to ģeogrāfiskā atrašanās vieta.

---

23 http://www.rodong.rep.kp/en/index.php7MTJAMiAyNS0wNC0y0S0wMDFAMTVAMUBAMEAxQ A==
24 http://en.kremlin.ru/events/president/news/76805
25 https://docs.un.org/en/S/2024/215
26 Drošības padome pagarina Kodolieroču, bioloģisko un ķīmisko ieroču uzraudzības komitejas pilnvaras uz 10 gadiem, vienbalsīgi pieņemot 2663. rezolūciju (2022) | Sēžu atspoguļojums un paziņojumi presei
27 Vadlīnijas par proliferācijas finansēšanas riska novērtēšanu un mazināšanu.
28 Money-Laundering-National-Risk-Assessment-Guidance-2024.pdf.coredownload.inline.pdf

Šis konteksta faktors ir atzīts par nozīmīgu saistībā ar iespējamo saistību ar KTDR sankciju apiešanas shēmām.

38. Nozaru ievainojamība attiecas uz nozarei raksturīgām iezīmēm, ko kāda persona vai organizācija var ļaunprātīgi izmantot, lai īstenotu sarežģītas proliferācijas finansēšanas un sankciju apiešanas shēmas. Piemēram, finanšu plūsmu vai aktīvu kustības izsekojamību var kavēt piegādes kanāla kontekstuālās iezīmes kādā nozarē, piemēram, starpnieku un aģentu izplatība.

Valsts līmeņa ievainojamības pret PF un izvairīšanos no sankcijām

39. Dažas no visbiežāk sastopamajām valsts līmeņa vājajām vietām, kas veicina sarežģītas proliferācijas finansēšanas un sankciju apiešanas shēmas, kuras ir identificējis FATF Globālais tīkls, ir šādas:

Ekonomiskie un tirdzniecības faktori

40. Daudzas valstis norādīja, ka PF un sankciju apiešanas draudi ir vērsti uz valstīm, kas darbojas kā starptautiski finanšu centri, ņemot vērā to nozīmi pasaules finanšu plūsmās un transportā (skatīt 1. tipoloģiju). PF ievainojamību rada plašais produktu un pakalpojumu klāsts, ko piedāvā starptautiskie finanšu centri, apkalpojot plašu un daudzveidīgu klientu loku. Turklāt šo izveidoto finanšu sistēmu un ekonomiku atvērtība (tostarp īpašo ekonomisko zonu esamība) un sarežģītība, kas veicina pārrobežu darījumus, padara tās īpaši neaizsargātas pret ļaunprātīgu izmantošanu nelikumīgas proliferācijas tīklu vajadzībām. Tāpat valstis, kurās ir stratēģiskas ostas, kas aprīkotas ar kuģniecības un loģistikas infrastruktūru, var tikt ļaunprātīgi izmantotas, lai apietu sankcijas un eksporta kontroli saistībā ar divējāda lietojuma precēm.

41. Daudzas valstis minēja arī ievainojamības, kas saistītas ar ekonomisko un tirdzniecības attiecību uzturēšanu ar valstīm,[29] uz kurām attiecas sankcijas, kas palielina saskarsmi ar potenciālām PF un sankciju apiešanas shēmām. Ģeopolitiskā saskaņotība, atkarības vai vēsturiskās saiknes var radīt iespējas PF apdraudējuma dalībniekiem vērsties pret šīm valstīm bez valsts ziņas, lai apietu sankcijas un piekļūtu finanšu sistēmām un resursiem.

42. Lielākā daļa valstu uzsvēra muitas aģentūru nozīmi, lai novērstu un atklātu sarežģītas sankciju apiešanas shēmas saistībā ar PF. Muitas aģentūrām ir būtiska loma informācijas vākšanā un apmaiņā iekšzemes, reģionālā un starptautiskā mērogā (skatīt 3. sadaļu).

Regulējuma faktori

43. Lai gan valstis ir guvušas panākumus AML/CFT regulējuma ieviešanā, ar CPF saistīto pasākumu īstenošana pasaulē joprojām atpaliek (skatīt 1. un 2. attēlu). Tā kā trūkst stingra normatīvā, tiesiskā un operatīvā regulējuma, dažas valstis nespēj izpildīt nepieciešamās sankciju saistības un eksporta kontroli, lai novērstu un apkarotu proliferācijas tīklus.

---

[29] Praksē daudzas valstis cenšas novērst ievainojamības, kas saistītas ar izvairīšanos no ANO, valsts un pārvalstisku sankciju režīmu piemērošanas. Tomēr FATF 7. ieteikums attiecas tikai uz KTDR, kas ir vienīgā ANO sankcijām pakļautā valsts. Kā norādīts kopsavilkumā un citviet dokumentā, šajā ziņojumā ir iekļauta informācija par izmantotajām metodēm, kā apiet valstu un pārvalstiskos sankciju režīmus, lai sniegtu aktuālu izpratni par draudiem un ievainojamību, tostarp par kopīgām problēmām starp attiecīgajām tipoloģijām, uz kurām neattiecas FATF standartu 7. ieteikums. Plašāks sankciju apiešanas formulējums nav paredzēts, lai no jauna definētu 7. ieteikuma prasības.

Turklāt sarežģītās PF un sankciju apiešanas shēmās tiek izmantotas dažādas maskēšanas metodes, kuras ir vēl grūtāk atklāt neregulētās nozarēs vai nozarēs ar nepietiekamu uzraudzību, piemēram, VASP. Kā arī PF ievainojamība palielinās valstīs, kurās ir nepilnīgi valsts tiesību akti par juridisko personu patieso labuma guvēju pārredzamību. Grūtības piekļūt patiesā labuma guvēja (BO) informācijai apgrūtina pārrobežu izmeklēšanu, ko veic iestādes, kuras cenšas identificēt un izsekot PF ceļu, jo īpaši, ja ir iesaistītas vairākas valstis ar nesaderīgu tiesisko regulējumu.

Ģeogrāfiskie un demogrāfiskie faktori

44. Dažas valstis ziņoja par ievainojamībām, kas saistītas ar to ģeogrāfisko tuvumu valstīm, uz kurām attiecas ANO, valstu un pārvalstiski sankciju režīmi, kas var radīt iespējas nelikumīgiem tīkliem pārvietot aktīvus un resursus pāri robežām. Stratēģiski izvietotās valstis piedāvā būtiskus kuģošanas ceļus un tirdzniecības ceļus, kas palielina kaimiņvalstu ievainojamību. Piemēram, uz tirdzniecību balstītas sankciju apiešanas shēmas, kas saistītas ar nelegālu preču kontrabandu, ir biežāk sastopamas starp valstīm, kas atrodas sankcijām pakļautu jurisdikcijas tuvumā (skatīt 4. tipoloģiju). Kā liecina gadījumu izpēte, Austrumāzijas valstis var būt pakļautas riskam, ka KTDR veicina apļveida finanšu darījumus un sūtījumus, savukārt Tuvo Austrumu valstis var radīt nelikumīgus finanšu ceļus Irānas WMD programmai. Dažas valstis ziņoja arī par ievainojamībām, kas saistītas ar ANO sankciju režīmam pakļautu jurisdikciju diplomātiskā personāla un citu attiecīgo dalībnieku klātbūtni.

Citi valsts līmeņa faktori

45. Vēl viena ievainojamība ir pasaules finanšu sistēmā plaši izmantoto ārvalstu valūtu, piemēram, ASV dolāru, lielais apjoms. Valstīm būtu jāņem vērā pārrobežu darījumi, kas tiek izpildīti šajās ārvalstu valūtās, ņemot vērā šo valūtu vai šajās valūtās denominētu kontu izmantošanas neaizsargātību pret nelikumīgiem iepirkumiem vai sankciju apiešanu.

46. Turklāt proliferācijas tīkli cenšas izmantot rūpnieciskos un tehnoloģiskos faktorus, lai nelikumīgi iegūtu preces. Tādējādi valstis, kas ražo ar proliferāciju saistītas tehnoloģijas un preces, ir pēc būtības neaizsargātas pret PF un divējāda lietojuma preču ierobežojumu pārkāpumiem. Valstīm ar lielu aizsardzības nozari ir nepieciešams ievērojams skaits organizāciju, kas nodrošina materiālus, produktus un pakalpojumus. Tas PF tīkliem rada iespējas ļaunprātīgi izmantot sarežģītās piegādes ķēdes.

47. Visbeidzot, 1718. UNSCR POE ziņojumos tika uzsvērta KTDR paļaušanās uz organizētiem vai starptautiskiem noziedzības tīkliem, izmantojot to transporta koridorus un starpniekus, lai atbalstītu proliferācijas darbības.

Nozaru līmeņa ievainojamības attiecībā uz PF un izvairīšanos no sankcijām

48. Pamatojoties uz FATF Globālā tīkla iesniegumiem un sabiedriskās apspriešanas rezultātiem, nozares, kuras ir visneaizsargātākās pret sarežģītām PF un sankciju apiešanas shēmām, ir šādas:

Banku un citas finanšu nozares

49. Daudzas valstis norādīja, ka banku un citas finanšu nozares, piemēram, apdrošināšana, ir neaizsargātas pret PF un sankciju apiešanas apdraudējuma dalībniekiem. Kad finanšu darījumi ir izpildīti valstu iekšienē un pāri robežām, no likumīgām vai nelikumīgām darbībām rodas vai ar to starpniecību tiek pārvietoti līdzekļi, ar kuriem tiek atbalstīti PF dalībnieki vai darbības. Bieži tiek pielietoti tādi paņēmieni kā vairāku kontu un viltotu dokumentu izmantošana, tostarp saistībā ar tirdzniecības finansēšanu.

50. Korespondentbankas ir neaizsargātas pret sankciju apiešanu, jo bieži vien tām nav iepriekšēju attiecību ar respondentbankas klientu.[30] Vairāki privātā sektora uzņēmumi ir identificējuši dažādus sarežģītus kontu veidus un darījumus, kas ir pakļauti PF un sankciju apiešanas riskam, kas ir īpaši svarīgi korespondentbanku attiecībām, kas saistītas ar valstīm ar augstāku PF risku un/vai neefektīvu CPF kontroli. Piemēram, tirdzniecība, kas tiek veikta, izmantojot atvērtā konta darījumus, ir neaizsargāta, jo trūkst informācijas par pārvadātajām precēm. Turklāt elektroniskie pārskaitījumi ļauj ātri pārskaitīt līdzekļus, taču tajos parasti ir ierobežota informācija par darījuma mērķi vai pamatojošiem dokumentiem.

51. Dažas valstis norādīja vairākus citus būtiskus faktorus, tostarp finanšu sistēmas ar plašiem valsts mēroga tīkliem, ātru un vieglu piekļuvi banku pakalpojumiem, ieguldījumu aktīvu atlikuma pieaugumu un privātpersonu finanšu aktīvu pārpilnību.

Virtuālie aktīvi un virtuālo aktīvu pakalpojumu sniedzēji

52. Daudzas valstis ir nobažījušās par arvien plašāku virtuālo aktīvu izmantošanu pārrobežu maksājumos un pārskaitījumos. PF tīkli bieži cenšas izmantot to, ka dažādās valstīs nav efektīvi īstenoti AML/CFT/CPF pasākumi attiecībā uz VASP, tā kā 15. ieteikums tiek īstenots novēloti (skatīt 3. tipoloģiju). Ir arī gadījumi, kad VASP valstīs, kurās ir AML/CFT/CPF prasības, neizpilda piemērojamos pienākumus. Valstis ir īpaši nobažījušās par saistītajiem PF riskiem, kas saistīti ar pseidonimizētu līdzekļu piesaisti un pārvietošanu. Daudzi neatļauto darbību dalībnieki cenšas palielināt virtuālo aktīvu darījumu anonimitāti, izmantojot virtuālo aktīvu miksēšanas pakalpojumus un anonimitāti paaugstinošas kriptovalūtas (AEC), tostarp legalizējot ienākumus no liela mēroga virtuālo aktīvu zādzībām, kas atbalsta WMD proliferāciju. Miksēšanas un citu aizsegšanas paņēmienu izmantošana var apgrūtināt trešo personu iespējas izsekot vai attiecināt darījumus. Valstis arī norādīja uz virtuālo aktīvu nozīmi KTDR centienos gūt ieņēmumus.

Jauna un alternatīva maksājumu infrastruktūra

53. Daži valsts un nevalstiskie dalībnieki pēta jaunus maksājumu kanālus un alternatīvas SWIFT maksājumu sistēmai, lai izvairītos no finanšu kontaktpunktiem, kas saistīti ar valsts, pārvalstiskiem un/vai starptautiskiem sankciju režīmiem. Piemēram, atsevišķos gadījumos valsts un nevalstiskie dalībnieki varētu izmantot jaunas digitālās maksājumu sistēmas, piemēram, vienādranga maksājumu pakalpojumus vai digitālo naudas pārvedumu pakalpojumu sniedzējus.[31]

---

[30] Korespondentbanku pakalpojumi, jo īpaši tie, kas tiek piedāvāti zināmām novirzīšanas/pārvadātāju jurisdikcijām vai tādām, kurās ir neefektīva AML/CFT/CPF kontrole, var radīt paaugstinātu risku. Tomēr korespondentbanku risks saistībā ar proliferācijas finansēšanu nav vienādi augsts. Korespondentattiecību riska novērtējums jāveic katrā gadījumā atsevišķi, un tajā vienmēr jāņem vērā respondentbankas piemērotie iekšējās kontroles un riska mazināšanas pasākumi. Plašāku informāciju par korespondentbanku attiecībām skatīt FATF *2021. gada PF vadlīnijās*.

[31] Lai gan pastāv iespējamas bažas par risku pārvaldību saistībā ar alternatīvām SWIFT maksājumu ziņojumapmaiņas sistēmai, centrālo banku digitālo valūtu (CBDC) izmantošana sankciju apiešanai šobrīd ir teorētiska. No otras puses, dažas valstis uzskata, ka CBDC ļauj kompetentajām iestādēm vieglāk izsekot līdzekļu plūsmu un samazināt nelikumīgas finansēšanas riskus.

Citas nozares līmeņa ievainojamības

54. Kā norādīts 1718. UNSCR POE ziņojumos un FATF 2021. gada vadlīnijās par PF riska novērtēšanu un mazināšanu, valstīm būtu jāapzinās papildu nozares, kurās ir lielāka iespējamība saskarties ar PF-TFS pārkāpumiem, neieviešanu un izvairīšanos, ieskaitot, bet neaprobežojoties ar trasta un uzņēmumu pakalpojumu sniedzējiem (TCSP) un dārgmetālu un dārgakmeņu tirgotājiem.[32]

55. Valstis identificēja arī vairākas citas nozares, kuras ir neaizsargātas pret PF un sankciju apiešanas dalībnieku izmantošanu, tostarp aeronautikas, informācijas tehnoloģiju (IT), jūrniecības, kodolenerģētikas un kuģubūves nozares.

32. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf

4. 2. sadaļa. Ar PF saistīto sankciju apiešana – tipoloģijas

Pašreizējās tendences un metodes

56. Šajā ziņojumā gadījumu pētījumi ir iedalīti divās atsevišķās kategorijās:

a. **Izvairīšanās no PF-TFS saistībā ar KTDR**, uz ko attiecas FATF standartu 7. ieteikums

b. **Izvairīšanās no citu sankciju režīmu (piemēram, valsts un pārvalstisku sankciju) ievērošanas**, uz kuriem neattiecas FATF standartu 7. ieteikums

57. Šīs sadaļas mērķis ir sniegt neizsmeļošu sarakstu ar sarežģītās PF un sankciju apiešanas shēmās izmantotajām tipoloģijām, pamatojoties uz FATF Globālā tīkla iesniegto informāciju. Šo tipoloģiju rezultātā tika izveidots to finanšu darījumu rādītāju saraksts, kas varētu liecināt par PF (skatīt A pielikumu: Riska rādītāji).

1. tabula Tipoloģiju pārskats

Tipoloģija	Gadījumu izpētes apakštēmas	Lapas
1. Starpnieku piesaistīšana, lai izvairītos no sankcijām	Fiktīvas un čaulas kompānijas Tranzīts caur trešajām valstīm Bankas konti un finansējums	21-29
2. BOI slēpšana, lai piekļūtu finanšu sistēmai	Trešās personas, kas koordinē atbalstu finanšu pieejamībai Nelicencētu finanšu koordinatoru tīkli Dažādu juridisko personu veidu izmantošana Kredītkaršu un debetkaršu izmantošana KTDR	29-38
3. Virtuālo aktīvu un citu tehnoloģiju izmantošana	Regulējuma grūtības Virtuālo aktīvu izmantošana līdzekļu pārvietošanai Virtuālie aktīvi un līdzekļu ģenerēšana Ārvalstu struktūras un personas, kas atbalsta KTDR IT darbiniekus	38-46
4. Jūras un kuģniecības nozaru izmantošana	Kuģa identifikatora maiņa Pārvietošana no kuģa uz kuģi AIS apraides atspējošana Dokumentu viltošana	46-54

1. tipoloģija: Starpnieku piesaistīšana, lai izvairītos no sankcijām

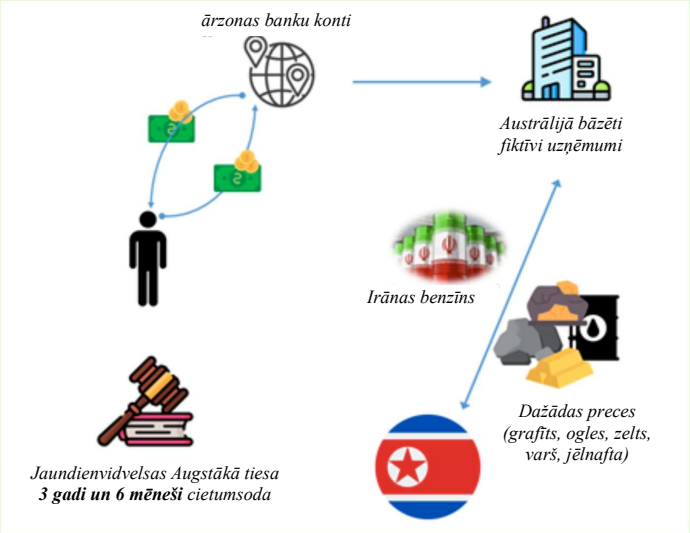
58. Valstis ziņo, ka, lai slēptu patiesos gala lietotājus, preču iepirkumu tīkli, kas paredzēti valstīm, kurās notiek proliferācija, vai sankcijām pakļautām valstīm, izmanto sarežģītas shēmas, kurās iesaistīti vairāki starpnieki. Šāda taktika apgrūtina PF un sankciju apiešanas gadījumu atklāšanu un izmeklēšanu. Šie starpnieki var būt čaulas un fiktīvi uzņēmumi, finanšu koordinatori, banku konti (tostarp korespondentbanku attiecības) un pārkraušana caur trešajām valstīm. Šo starpnieku izmantošanai ir būtiska nozīme līdzekļu izcelsmes, galamērķa un mērķa slēpšanā. Izmantojot dažādu finanšu sistēmu un tiesiskā regulējuma ievainojamības, starpnieki dod iespēju proliferācijas tīkliem izvairīties no atklāšanas un sankcijām (vairāk informācijas skatīt sadaļā "Ievainojamības").

Fiktīvu un čaulas uzņēmumu izmantošana

59. Daudzas valstis ziņoja, ka PF un sankciju apiešanas tīkli var izveidot vai sadarboties ar vietējiem uzņēmumiem trešajās valstīs, lai tie darbotos kā starpnieki un aizsega sabiedrības. Šīs struktūras var būt čaulas uzņēmumi, kas neveic nekādu darbību vai veic šķietami likumīgus darījumus, lai piekļūtu finanšu sistēmām, atvieglotu maksājumus un līgumu slēgšanu, importētu vai eksportētu preces, izmantojot nepatiesus aizbildinājumus (piemēram, deklarējot divējāda lietojuma preces kā paredzētas tikai civilām vajadzībām), un slēpt saistību ar sankciju subjektiem, darbojoties ar citiem nosaukumiem, īpašnieku struktūrām vai valstīm. Neatļauto darbību dalībnieki darbojas nozarēs, kas saistītas ar divējāda lietojuma preču vai priekšmetu kontrabandu, piemēram, elektroniku, ķīmiskām vielām vai rūpniecības iekārtām, vai citām precēm, uz kurām attiecas sankcijas vai eksporta kontroles noteikumi.

2. ierāmējums. Gadījuma izpēte: Austrālijā bāzētas korporatīvās struktūras izmantošana, lai izvairītos no sankcijām

2021. gada 23. jūlijā Jaundienvidvelsas Augstākā tiesa piesprieda Dienvidkorejā dzimušam Austrālijas pilsonim trīs gadu un sešu mēnešu cietumsodu par Austrālijas sankciju likuma pārkāpšanu attiecībā uz KTDR. Persona izmantoja ārzonas bankas kontus un vairākus Austrālijā bāzētus fiktīvus uzņēmumus, lai koordinētu dažādu preču tirdzniecību ar KTDR, ieskaitot ogles, grafītu, vara rūdu, zeltu, jēlnaftu (tostarp iegādājoties Irānas benzīnu KTDR vārdā), raķetes un ar raķetēm saistītas tehnoloģijas. Šī bija pirmā reize, kad Austrālijā tika izvirzītas apsūdzības par sankciju pārkāpumiem saistībā ar KTDR.



Avots: Austrālija

60. Starpnieki var izmantot arī juristu un grāmatvežu atbalstu, kuri palīdz izveidot sarežģītas struktūras, lai izvairītos no atklāšanas, vai kravu ekspeditoru un kuģniecības aģentu atbalstu, kuri palīdz izveidot kompleksas piegādes ķēdes un sniedz konsultācijas par to, kā izmantot sankciju režīmu nepilnības un nodrošināt, ka aizliegtās preces tiek nepareizi deklarētas un sūtītas, izmantojot viltus aizsegus.

61. Fiktīvi uzņēmumi ir bieži sastopams līdzeklis, kas aizsedz divējāda lietojuma preču virzību izmantošanai militārajā bruņojumā vai aizsardzības nozarē. Neatļautu darbību dalībnieki izmanto šāda veida sarežģītus mehānismus, lai palēninātu izmeklēšanas gaitu, kuras mērķis ir atklāt iespējamu izvairīšanos no sankcijām vai eksporta kontroles apiešanu saistībā ar paaugstināta riska precēm. Turpmāk izklāstītajos divos gadījumu pētījumos ir aprakstītas sarežģītas shēmas, kā noslēpt šādu divējāda lietojuma preču galamērķi.

Commented [LŽ4]: https://termini.gov.lv/atrast/sensitive%20goods/en?target=lv

3. ierāmējums. Gadījuma izpēte: Sankciju apiešanas shēma ASV izcelsmes elektronisko komponentu kontrabandai uz Irānas militārajiem uzņēmumiem

2024. gada janvārī Kolumbijas apgabalā četriem Ķīnas valstspiederīgajiem tika izvirzītas apsūdzības dažādos federālajos noziegumos saistībā ar gadiem ilgu sazvērestību, lai nelikumīgi eksportētu un kontrabandas ceļā no ASV uz Irānu izvestu ASV izcelsmes elektroniskas detaļas. Apsūdzētie, iespējams, nelikumīgi eksportēja un kontrabandas ceļā caur Ķīnu un Honkongu izveda ASV eksportam pakļautas preces, lai tās izmantotu ar Islāma revolucionārās gvardes korpusu (IRGC) un Aizsardzības un bruņoto spēku loģistikas ministriju (MODAFL) saistītas struktūras, kas pārrauga Irānas raķešu, ieroču un militārā gaisa aprīkojuma, tostarp bezpilota lidaparātu (UAV), izstrādi un ražošanu.

Sākot no 2007. gada maija un turpinot vismaz līdz 2020. gada jūlijam, šīs personas izmantoja fiktīvus uzņēmumus Ķīnā, lai ASV izcelsmes divējāda lietojuma preces, tostarp elektroniku un komponentus, ko varētu izmantot bezpilota lidaparātu, ballistisko raķešu sistēmu un citu militāru galapatēriņa ierīču ražošanā, nodotu sankcijām pakļautajām struktūrām, kas saistītas ar IRGC un MODAFL, piemēram, Shiraz Electronics Industries (SEI), Rayan Roshd Afzar un to saistītajām personām.

Visu sazvērestības laiku atbildētājislēpa faktu, ka preces bija paredzētas Irānai un Irānas struktūrām, un sniedza ASV uzņēmumiem būtiski maldinošu informāciju par galīgo galamērķi un galalietotājiem. Šīs maldinošās prakses rezultātā ASV uzņēmumi eksportēja divējāda lietojuma preces uz fiktīvajiem uzņēmumiem, izmantojot viltus aizbildinājumus un izliekoties, ka šo produktu galamērķis ir Ķīna, nevis Irāna, tādējādi pārkāpjot ASV sankciju un eksporta kontroles tiesību aktus un noteikumus. Apsūdzības saistībā ar šo sarežģīto sankciju apiešanas shēmu koordinēja vairāku aģentūru operatīvā grupa, ko kopīgi vadīja Tieslietu un Tirdzniecības departaments.

Avots: Amerikas Savienotās Valstis

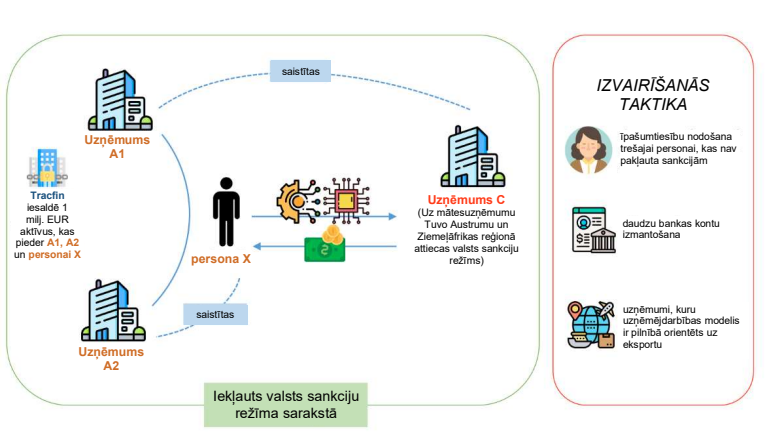
4. ierāmējums. Gadījuma izpēte: Divējāda lietojuma preču eksports Krievijas uzņēmumam, izmantojot starpniekus

Francijas uzņēmumi A1 un A2 darbojās kā starpnieki, lai iegādātos ārvalstu elektroniskās komponentes, kas tika tālāk pārdotas citam starpnieka uzņēmumam Tuvo Austrumu un Ziemeļāfrikas reģionā (uzņēmums B). Pēc tam, kad starpnieki iegādājās divējāda lietojuma preces, tie piegādāja elektroniskās sastāvdaļas Krievijas mātesuzņēmumam (uzņēmums C), kam ir piemērotas ASV sankcijas. Šī proliferācijas shēma ļāva Krievijas aizsardzības nozarei nodrošināties ar aizliegtām precēm un uzlabot savas vispārējās spējas.

Francijas FID TracFin vadīja starpinstitūciju pasākumus, lai apturētu šo shēmu, iesaldējot A1, A2 un personai X (A1 un A2 patiesā labuma guvējs) piederošos aktīvus 1 miljona eiro apmērā. Lai gan ASV Valsts kases OFAC (Ārvalstu aktīvu kontroles birojs) piemēro sankcijas A1, A2 un personai X, uz šīm personām un uzņēmumiem pagaidām neattiecas ES vai Francijas ierobežojošie pasākumi. Pēc tam TracFin sadarbojās ar Francijas bankām, lai ierobežotu viņu līdzekļus saskaņā ar kontroles kritērijiem[33], jo pastāvēja aizdomas, ka uzņēmums C joprojām kontrolē uzņēmumu A1, lai gan tā akcijas ir pārdevis ārvalstu ieguldītājam. Uzņēmums A2 pilnībā pieder personai X.

Šajā sarežģītajā sankciju apiešanas shēmā tika izmantoti daudzi izplatīti apiešanas paņēmieni, tostarp īpašumtiesību nodošana trešajai personai, uz kuru neattiecas sankcijas (personas sievai), daudzu bankas kontu izmantošana un uzņēmumi, kuru uzņēmējdarbības modelis bija pilnībā orientēts uz eksportu, bet kuri tomēr darbojās kā apiešanas struktūras.

Galvenā problēma bija neatbilstība starp sankciju režīmiem[34], kas varēja novest pie kapitāla aizplūšanas. Lai nodrošinātu sankciju efektivitāti un aktīvu iesaldēšanas juridisko pamatu visās valstīs, būtu lietderīgi veikt saskaņotus noteikšanas procesus.



Avots: Francija

Tranzīta izmantošana trešajās valstīs, lai līdzsvarotu globalizētās piegādes ķēdes un starptautisko tirdzniecību

62. Valstis aprakstīja proliferācijas tīklus, kas izmanto globalizētas piegādes ķēdes un starptautisko tirdzniecību, lai slēptu preču un tehnoloģiju iepirkuma darbības. Tie var iegādāties komponentus no vairākiem piegādātājiem, lai padarītu galapatēriņa veidu mazāk uzkrītošu, un pārvietot preces caur brīvās tirdzniecības zonām (BTZ), kurās bieži vien ir mazāk stingra uzraudzība un kurās ir atļauts pārpakot un reeksportēt ar jaunām etiķetēm. Preces var nosūtīt caur vairākām ostām vai valstīm, lai slēptu patieso izcelsmi vai galamērķi, izmantojot viltotu dokumentāciju, viltotus nosūtīšanas dokumentus, gala lietotāja sertifikātus vai konosamentus, lai sagrozītu informāciju par kravas veidu vai galīgo saņēmēju. Piemēram, aizliegtu raķešu sastāvdaļu sūtījumu ar izmainītiem dokumentiem var nomaskēt kā rūpniecisku iekārtu. Turpmāk izklāstītajos divos gadījumos ir aprakstīti sarežģīti tranzīta maršruti, lai apgrūtinātu eksporta kontroles noteikumu un sankciju apiešanas atklāšanu.

5. ierāmējums. Gadījuma izpēte: starpnieku izmantošana, lai apietu eksporta kontroles noteikumus

Vairāki gadījumi, kas ilustrē atkārtojošos tipoloģiju, norāda uz apiešanas shēmām, kurās trešo valstu uzņēmumi, kas dažkārt atrodas citā ES jurisdikcijā un ko pārvalda vai kontrolē irāņi, iegādājas divējāda lietojuma preces no Francijas piegādātājiem, kuras pēc tam tiek reeksportētas uz Irānu.

Irānas uzņēmums, kas apgādā Irānas ballistisko raķešu programmu, mēģināja iegūt kompozītmateriālus no Francijas piegādātāja. Uzņēmuma vadītājs no Irānas izmantoja trešās valsts uzņēmumu, ko vadīja cits Irānas pilsonis, kurš pēc tam reeksportēja kompozītmateriālus uz Irānu.

2020. gadā darbgalds pirms izvešanas no ES teritorijas tika secīgi eksportēts uz Eiropas valstīm A, B un C. Šis sarežģītais tirdzniecības modelis un izmaiņas dokumentācijā bija paredzētas, lai maskētu pārējo ceļojuma posmu, kas ietvēra ierašanos kādā Tuvo Austrumu jurisdikcijā, pirms darbgalds sasniedza galamērķi Irānā.

Avots: Francija

6. ierāmējums. Gadījuma izpēte: ES sankciju apiešanas caur starpniekiem atklāšana ar starptautiskās sadarbības palīdzību

2022. gadā kāds Portugāles uzņēmums mēģināja eksportēt motorus, kurus varētu izmantot bezpilota lidaparātos, izmantojot starpnieku AAE, un to galamērķis bija Kazahstānā reģistrēts uzņēmums. Uz šīm precēm attiecās ES ierobežojošo pasākumu 12. pakete attiecībā uz Krieviju, un bija pārliecinoši rādītāji, ka preču galamērķis būs Krievijas Federācija. Izmeklēšanas laikā uzņēmums pārtrauca preču eksportu, tiklīdz tika uzdoti jautājumi par galamērķi.

Uzņēmums mēģināja apiet sankcijas, izmantojot divus dažādus starpniekus: kravu ekspeditoru AAE un mazumtirgotāju Kazahstānā. Tas slēpa arī gala lietotāju. Kazahstānas uzņēmumam bija cieši komerciāli sakari ar Krievijas uzņēmumiem, un diversijas risks bija liels. Maksājumi tika veikti ar bankas pārskaitījumiem.

[33] ES tiesību aktos kontroles kritēriji palīdz noteikt, vai līdzekļus vai uzņēmumu kontrolē sankcijām pakļauts subjekts vai persona. Piemēram, ja sankcijām pakļauta persona vai subjekts ietekmē vai var pieņemt lēmumus par līdzekļiem vai uzņēmumu, tas var palīdzēt noteikt, vai pastāv kontrole.

[34] Kā norādīts 3. iedaļā (skatīt 105.-106. punktu) un secinājumos (skatīt 146. punktu un prioritārās jomas), šāda neatbilstība ir viens no galvenajiem faktoriem, kas rada problēmas, atklājot, izmeklējot un veicot krimināltvajāšanu par izvairīšanos no sankciju piemērošanas saistībā ar PF.

Pēc tam Portugāles iestādes uzraudzīja uzņēmumu un atklāja, ka vēlāk 2023. gadā šis uzņēmums ar starpnieku palīdzību Serbijā un Honkongā eksportēja citas drošības un aizsardzības jomas preces, iespējams, uz Krieviju. Abi starpnieki bija uzņēmumi ar ciešām komerciālām attiecībām ar Krievijas Federāciju.

Šajā lietā bija iesaistīts Drošības izlūkošanas dienests un Muitas pārvalde. Lieta tika atklāta, vācot izlūkdatus, un izmeklēta ar starptautiskās sadarbības un muitas izmeklēšanas palīdzību.

Šis piemērs ilustrē iepirkumu tīklu spēju pielāgoties jauniem apstākļiem un dažādiem izaicinājumiem. Tikai efektīva sadarbība valstu starpā un vienmērīga saziņa var palīdzēt mazināt šāda veida draudus.

Avots: Portugāle

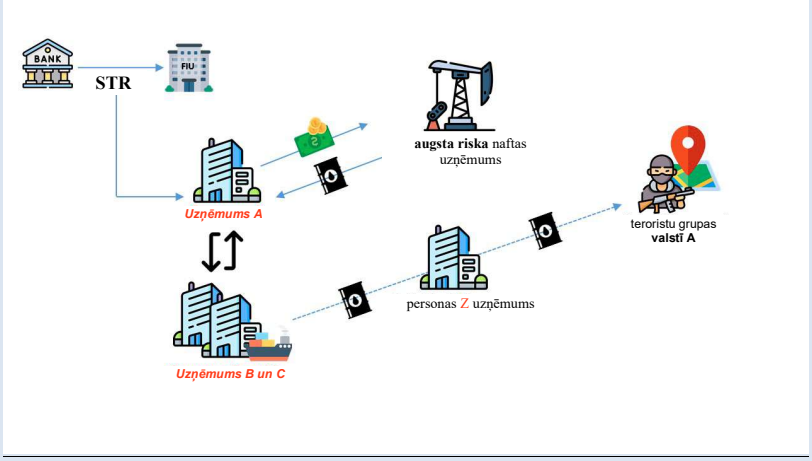
63. Turklāt reģionālie tranzīta mezgli, kas atrodas tuvu sankcijām pakļautām valstīm vai uzņēmumiem, ir sankciju apiešanas mērķis, lai pārvietotu līdzekļus un preces. Jo īpaši PF un sankciju apiešanas tīkli cenšas maskēt savu darbību starptautiskajos finanšu centros, kur, kā viņi cer, plašais komerciālo, finanšu un tirdzniecības aktivitāšu mērogs var palīdzēt maskēt to nelikumīgās darbības.

7. ierāmējums. Gadījuma izpēte: kuģniecības uzņēmumu izmantošana, lai pārdotu naftu sankcijām pakļautas personas vārdā

2022. gada septembrī tiesībaizsardzības iestādes no bankas saņēma UAEFIU ziņojumu par SAR/STR. SAR/STR bija uzsvērts, ka uzņēmums A veica bankas pārskaitījumu augsta riska naftas uzņēmumam, par kuru bija aizdomas, ka tas tiek izmantots WMD izplatīšanas atbalstam. Tiesībaizsardzības iestādes un UAEFIU veica kriminālizmeklēšanu un finanšu izmeklēšanu par uzņēmumu A un tā finanšu/komerciālo darbību.

Izmeklēšanā tika konstatēts, ka uzņēmumu A ir dibinājis ārvalstu valstspiederīgais, kas saistīts ar diviem AAE kuģniecības uzņēmumiem (uzņēmums B un C). Tika atklāts arī tas, ka uzņēmums B un C pieder personām, kas atbalsta teroristu grupējumus valstī A. Abi uzņēmumi izmantoja fiziskās personas Z uzņēmumu kā starpnieku, lai sagatavotu pārvadājuma līgumus par naftas transportēšanu no augsta riska valsts uz uzņēmumu B un C, kas vēlāk tika nosūtīti teroristu grupējumiem.

Izmeklēšanā arī atklājās, ka uzņēmums B un C pārdeva naftu teroristu grupējumam, izmantojot viltotus dokumentus, lai slēptu naftas izcelsmi un avotu. Ienākumi no naftas pārdošanas tika pārskaitīti uzņēmumam A, kas tos nosūtīja augsta riska naftas uzņēmumam – aizdomās turētai fiktīvai sabiedrībai, kuru sankcijām pakļautais uzņēmums izmantoja, lai atbalstītu proliferāciju. Izmeklēšanā tika noskaidrots, ka kopējais pārskaitīto līdzekļu apjoms bija 70 miljoni ASV dolāru. Tiesībaizsardzības iestādes arestēja visus aizdomās turamos, tostarp personu Z, kas atzina savu līdzdalību palīdzēšanā Irānai izvairīties no PF sankcijām, un apturēja uzņēmumu uzņēmējdarbību.



Avots: Apvienotie Arābu Emirāti

Bankas kontu izmantošana un finansēšana ar trešo valstu starpniecību

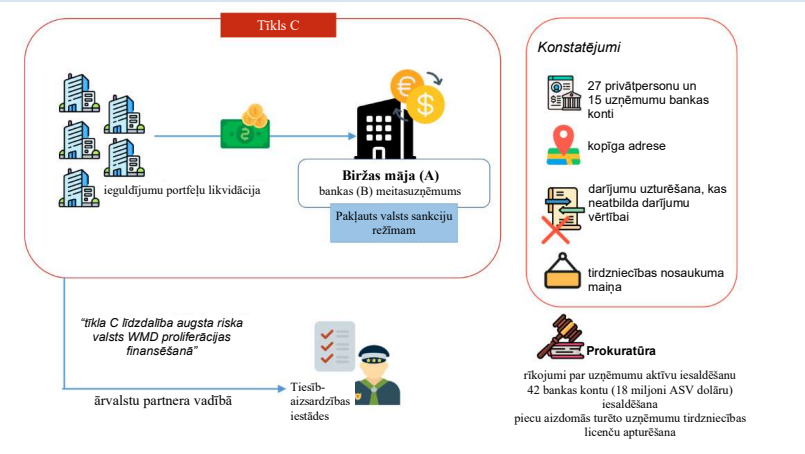
64. PF un sankciju apiešanas dalībnieki bieži izmanto vairākus finanšu darījumu līmeņus, lai slēptu līdzekļu izcelsmi, galamērķi vai nolūku, kas ir klasisks nelikumīgi iegūtu līdzekļu legalizēšanas paņēmiens. Lai apgrūtinātu izsekošanu, tie bieži vien veic maksājumus caur vairākām finanšu iestādēm vairākās valstīs, izmantojot fiktīvus uzņēmumus vai čaulas uzņēmumus, kas reģistrēti valstīs ar regulējuma nepilnībām.

8. ierāmējums. Gadījuma izpēte: finanšu sistēmas un naftas sūtījumu ļaunprātīga izmantošana PF atbalstam

Izmantojot konfidenciālus avotus, tiesībaizsardzības iestādes identificēja vairākus ienākošos/izejošos darījumus ar lielu vērtību, ko veica pieci AAE uzņēmumi ar augsta riska Biržas māju (A), kas ir bankas (B) meitasuzņēmums. Gan Biržas māja A, gan banka B ir daļa no "tīkla C", un tās ir iekļautas ASV Valsts kases OFAC sarakstā. Divi no pieciem aizdomās turētajiem uzņēmumiem ieguva līdzekļus, likvidējot ieguldījumu portfeļus un pārskaitot tos Biržas mājai A, kas savukārt pārskaitīja līdzekļus bankai B, lai atbalstītu sankcijām pakļauto uzņēmumu. Tiesībaizsardzības iestādes uzsāka izmeklēšanu kopā ar attiecīgajām ieinteresētajām personām (UAEFIU, CBUAE, vietējiem reģistratoriem un muitu).

CBUAE identificēja 27 privātpersonu un 15 uzņēmumu bankas kontus, kas bija saistīti ar šo tīklu. Tāpat vietējie reģistri sniedza tiesībaizsardzības iestādēm ziņojumus par pārbaudēm uz vietas; šajos ziņojumos atklājās, ka aizdomās turētajām struktūrām bija viena un tā pati adrese, pirms objekta apmeklējuma tās mēdza mainīt savu komercnosaukumu un veica darbības, kas neatbilda darījumu vērtībai. Vienlaikus tiesībaizsardzības iestādes saņēma informāciju no ārvalstu partnera, kas apstiprina tīkla C iesaistīšanos augsta riska valsts WMD proliferācijas finansēšanā.

Pamatojoties uz šiem konstatējumiem, prokuratūra, sadarbojoties ar UAEFIU un CBUAE, izdeva rīkojumus iesaldēt šo struktūru aktīvus, apķīlājot 42 banku kontus ar kopējo atlikumu aptuveni 18 miljoni ASV dolāru (63 725 065 AAE dirhamu). Turklāt vietējie reģistratori apturēja piecu aizdomās turēto uzņēmumu tirdzniecības licences.



Avots: Apvienotie Arābu Emirāti

65. PF tīklu mērķis ir finanšu iestādes trešajās valstīs, kurās tie cenšas izmantot jurisdikciju starptautisko un valstu sankciju režīmu īstenošanas atšķirības. Neatļautu darbību dalībnieki izmanto bankas, lai atvērtu kontus un atvieglotu starptautisko elektronisko pārskaitījumu veikšanu, neradot brīdinājuma signālus, izmantojot korespondentbanku attiecības, lai netieši piekļūtu starptautiskajiem finanšu tirgiem. Nelegālie tīkli var izmantot arī neoficiālas finanšu sistēmas, kurās ir mazāka iespēja atklāt aizdomīgus darījumus un kuras paļaujas uz valstīm ar mazāk stingrām ziņošanas vai pārrobežu darījumu izpildes prasībām.

9. ierāmējums. Gadījuma izpēte: uzņēmumi un personas, kam piemēro sankcijas par to, ka tās veido paralēlo banku tīklu, ko IRGC izmanto ieņēmumu gūšanai

OFAC 2024. gada jūnijā noteica sankcijas gandrīz 50 uzņēmumiem un personām, kas veido vairākas filiāles plašā paralēlo banku tīklā, kuru izmanto MODAFL un IRGC ieņēmumu gūšanai, cita starpā nelikumīgi iepērkot ASV izcelsmes elektroniskās komponentes modernu ieroču, piemēram, bezpilota lidaparātu, izstrādei un atbalstot Jemenas hutiešus un Krievijas karu Ukrainā.

Lai piekļūtu starptautiskajai finanšu sistēmai, MODAFL izmanto Irānas biržas mājas, kas pārvalda daudzus fiktīvus uzņēmumus Honkongā, AAE un citur, lai ārvalstu komercdarbībā, tostarp naftas pārdošanā, gūtos ienākumus legalizētu tīrā ārvalstu valūtā. Tie paši fiktīvie uzņēmumi izmanto legalizēto ārvalstu valūtu, lai starptautiskā tirgū iegādātos ieroču komponentus.

Avots: Amerikas Savienotās Valstis

10. ierāmējums. Gadījuma izpēte: starpnieku izmantošana, lai apietu TFS un pārskaitītu no nekustamā īpašuma gūtos ienākumus

2015. gadā kāds KTDR diplomāts, kas bija norīkots darbā Francijā, nopirka dzīvokli Parīzē un to izīrēja, pirms 2017. gadā ANO viņu iekļāva sarakstā. Pēc sankciju piemērošanas viņš turpināja saņemt ieņēmumus no dzīvokļa izīrēšanas. Persona izstrādāja shēmu, kurā bija iesaistīti dažādi starpnieki ar bankas kontiem vairākās trešajās valstīs, kas slēpa viņa kā galīgā saņēmēja statusu. Pēc tam, kad 2019. gadā Eiropas banka bija izziņojusi brīdinājumu, ieņēmumi tika noguldīti darījuma kontā.

Avots: Francija

2. tipoloģija: BOI slēpšana, lai izvairītos no sankcijām un piekļūtu finanšu sistēmai

66. Sarežģīta PF un izvairīšanās no sankcijām bieži vien ir saistīta ar BOI viltošanu, slēpjot galalietotāju/galīgo lietojumu un galīgo galamērķi, ko ir grūti atklāt gan valsts, gan privātajam sektoram. Daudzas no šīm maskēšanas metodēm tiek izmantotas arī digitālajā vidē, kas var radīt papildu problēmas atklāšanā. Tā kā TFS attiecas uz noteiktām personām un uzņēmumiem, kā arī uz līdzekļiem, kas ir šo noteikto personu kontrolē vai īpašumā, patieso labuma guvēju identificēšana var palīdzēt mazināt riskus, kas saistīti ar sankciju apiešanu.

Trešās personas, kas atbalsta KTDR piekļuvi finanšu sistēmai

67. KTDR regulāri izmanto maldinošu praksi, tostarp slēpj BOI, lai apietu ANO un valstu sankciju režīmus un piekļūtu oficiālajai finanšu sistēmai. KTDR turpina izmantot ārvalstīs bāzētus fiktīvus un čaulas uzņēmumus, slēptus pārstāvjus ārvalstīs un trešās personas starpniekus, lai apslēptu darījumu patieso iniciatoru, saņēmēju un nolūku, tādējādi ļaujot starptautiskās finanšu sistēmas apritē cirkulēt miljardiem dolāru vērtām KTDR nelikumīgām finanšu darbībām. Valsts dalībnieki, kas atbalsta KTDR sarežģītās shēmas, lai piekļūtu finanšu sistēmai, apgrūtina sankciju apiešanas novēršanu.

11. ierāmējums. Gadījuma izpēte: KTDR un Krievijas finanšu uzņēmumi organizēja sarežģītu sankciju apiešanas shēmu

ASV Valsts kases departamenta OFAC 2024. gada septembrī iekļāva sarakstā piecu uzņēmumu un vienas fiziskas personas tīklu, kas atrodas Krievijā un Krievijas okupētajā Gruzijas Dienvidosetijas reģionā, kas izmantoja nelikumīgas finanšu shēmas, lai nodrošinātu KTDR piekļuvi starptautiskajai finanšu sistēmai, tādējādi pārkāpjot 1718. UNSCR prasītās TFS[35]. Turklāt šie uzņēmumi un fiziskā persona pārkāpa 2270. UNSCR noteikto aizliegumu uzturēt korespondentattiecības ar KTDR bankām.

Šī rīcība bija vērsta pret sarežģītām shēmām, ko organizēja divas KTDR valsts pārvaldītas organizācijas – Foreign Trade Bank (FTB) un Korea Kwangson Banking Corporation (KKBC) –, kuras abas ir iekļautas 1718. UNSCR Sankciju sarakstā.[36] FTB ir KTDR galvenā ārvalstu valūtas maiņas banka un ir ļoti svarīga nelikumīgiem finanšu tīkliem, ko KTDR izmanto, lai finansētu savas WMD un ballistisko raķešu programmas. FTB un KKBC ar Krievijas Federācijas palīdzību turpināja paplašināt KTDR piekļuvi nelikumīgiem finanšu tīkliem.

Krievijas Centrālās bankas organizētajā shēmā MRB Bank (MRB), kas atrodas Gruzijas Dienvidosetijas reģionā, rīkojās kā Krievijas bankas TSMR Bank OOO (TSMR Banka) starpnieks, lai izveidotu slepenas banku attiecības ar FTB. TSMR Bankas augsta ranga amatpersona īstenoja skaidras naudas noguldījumus no FTB caur TSMR Banku uz MRB. TSMR Bankas augsta ranga amatpersona organizēja FTB un KKBC korespondentkontu atvēršanu MRB un koordinēja ar KTDR pārstāvjiem, lai nodrošinātu miljoniem dolāru un rubļu banknošu piegādi uz FTB un KKBC kontiem MRB. Vismaz daži no KTDR kontiem MRB tika izmantoti, lai maksātu par degvielas eksportu no Krievijas uz KTDR.

Atsevišķas shēmas ietvaros 2023. gada beigās Russian Financial Corporation Bank JSC (RFC) sadarbojās ar FTB, lai nodibinātu Maskavā bāzētu uzņēmumu Stroytreyd LLC (Stroytreyd), kas saņemtu iesaldētos KTDR līdzekļus, kuri glabājās neeksistējošās Krievijas bankās. Īstenojot šos centienus repatriēt KTDR iesaldētos aktīvus, RFC piederošā Timer Bank AO (Timer Bank) pārskaitīja līdzekļus uz Stroytreyd miljoniem dolāru vērtībā, kas bija paredzēti FTB galīgajam labumam. KTDR valdības amatpersonas sadarbojās ar RFC, lai palielinātu augsta līmeņa ekonomisko apmaiņu starp KTDR un Krieviju un veicinātu abu valstu finansiālo sadarbību. FTB ir sadarbojusies arī ar RFC, lai atvērtu kontus citām KTDR bankām, tostarp KTDR bāzētajai Lauksaimniecības attīstības bankai.[37]

Avots: Amerikas Savienotās Valstis

[35] https://home.treasury.gov/news/press-releases/jy2590

[36] 1718. UNSCR sarakstā FTB ir apzīmēta ar KPe.047, bet KKBC – ar KPe.025.

[37] 2025. gada 10. janvārī Japāna norādīja četras personas un piecus uzņēmumus (MRB Bank, Russian Financial Cooperation, Stroytreyd LLC, TsMRBank un Timer Bank AO) kā KTDR un Krievijas sadarbības veicinātājus.

68. Kā minējušas daudzas valstis, KTDR paļaujas arī uz to, ka tās pilsoņi, tostarp diplomātiskais personāls, atvieglos finanšu pakalpojumu sniegšanu vai aktīvu vai resursu nodošanu, tostarp liela apjoma skaidras naudas pārvadāšanu. Šo taktiku ir grūti atklāt, un diplomātiskie protokoli vēl vairāk apgrūtina savlaicīgu rīcību, lai pārtvertu vai pārtrauktu šādas darbības.

12. ierāmējums. Gadījuma izpēte: KTDR diplomāta dzīvesbiedrs pārvieto līdzekļus ar apdrošināšanas sabiedrības starpniecību

Nigērijā bāzētas apdrošināšanas sabiedrības tika turētas aizdomās par sadarbību ar sankcijām pakļautās valsts diplomāta dzīvesbiedru, lai palīdzētu KTDR valsts apdrošināšanas korporācijai Korea National Insurance Company (KNIC) parādu atgūšanā, uzņēmējdarbības attīstībā, naudas iekasēšanā, finanšu pārskaitījumos un darbotos kā aģenti vai pārstāvji, lai apietu Apvienoto Nāciju Organizācijas sankcijas. 2017. gadā KNIC tika iekļauts 1718. UNSCR Sankciju režīmā (KPe.048). Ar KNIC starpniecību saņemtā nauda tiek novirzīta KTDR WMD programmām.

Finanšu iestādes iesniegtais SAR/STR palīdzēja Nigērijas iestādēm atklāt finanšu darbības, kas saistītas ar nepamatoti lielām naudas summām. Aprēķinātā kopējā darījumu vērtība pārsniedza 616 000 eiro. Pēc tam, kad tika konstatētas aizdomīgas darbības, finanšu iestādes iesaldēja attiecīgos kontus un ziņoja Nigērijas iestādēm. Nigērija apsver arī papildu pretpasākumus.

Ievainojamība apdrošināšanas nozarē bija veids, kādā apdrošināšanas sabiedrības iegādājas starptautisko apdrošināšanu vai pārapdrošināšanu valsts infrastruktūrai, izmantojot trešo personu uzņēmumus. Arī apdrošināšanas klienti un darījumi tika izmantoti sankciju apiešanas shēmās, kas liecina par nepieciešamību stiprināt attiecīgo struktūru riska kontroli.

Avots: Nigērija

69. Daudzas valstis apzinās to, ka KTDR izmanto ārvalstu valstspiederīgos un šo pašu personu reģistrētus fiktīvus uzņēmumus, lai slēptu BOI un piekļūtu oficiālajai finanšu sistēmai un pārvietotu līdzekļus caur to. Piemēram, FTB un KKBC slēpa finansiālās saiknes ar KTDR, izveidojot fiktīvu uzņēmumu tīklus Ķīnas valstspiederīgo vārdā, kuriem ir konti Ķīnā bāzētās bankās, lai pārvietotu līdzekļus caur starptautisko finanšu sistēmu.

13. ierāmējums. Gadījuma izpēte: KTDR banku un finanšu pakalpojumi – Foreign Trade Bank

2020. gada maijā ASV iestādes izvirzīja apsūdzības kriminālietās pret vairāk nekā 30 personām, kuras strādāja dažādos amatos, lai, iespējams, sniegtu pakalpojumus un veiktu aizliegtus darījumus ASV dolāros ANO norādītās FTB labā. Apsūdzības rakstā ir norādīti konkrēti maksājumi, kas veikti ASV uzņēmumiem KTDR valdības vārdā. Citi maksājumi starp FTB fiktīvajiem uzņēmumiem un citiem trešo personu uzņēmumiem tika veikti, izmantojot ASV korespondentbankas.

Apsūdzības rakstā minētās personas lika korespondentbankām apstrādāt vismaz 2,5 miljardus ASV dolāru nelegālos maksājumos, kuri sazvērestības laikā caur vairāk nekā 250 fiktīviem uzņēmumiem tika pārskaitīti caur ASV. Šie uzņēmumi tika dibināti Austrijā, Ķīnā, Kuveitā, Lībijā, Māršala salās, Krievijā un Taizemē. Daudzas apsūdzētās personas bija izvietotas šajās valstīs, vadot slepenas FTB "filiāles", un vairākas nozīmīgas darbības koncentrējās Ķīnas pilsētās.

Personas sadarbojās ar trešo personu finanšu starpniekiem, lai izveidotu fiktīvus uzņēmumus, kas KTDR vārdā varētu veikt maksājumus preču un citu priekšmetu iegādei, tostarp maksājumus, kas saistīti ar rafinētas naftas un ogļu tirdzniecību. Citi maksājumi tika veikti metālu, elektronikas un telekomunikāciju uzņēmumiem. Apsūdzētie izveidoja jaunus fiktīvus uzņēmumus, tiklīdz darījuma partneri uzskatīja vecos par aizdomīgiem. FTB aģenti savstarpējai saziņai izmantoja šifrētas maksājumu atsauces, lai FTB centrālais birojs varētu virzīt pirkumus un precīzi novērtēt līdzekļu plūsmu no fiktīvajiem uzņēmumiem uz maksājumu saņēmējiem. Visbeidzot, kad runa bija par faktisko preču nosūtīšanu, apsūdzētie līgumus un rēķinus marķēja, norādot nepatiesus galapunktus un galalietotājus.

Avots: Amerikas Savienotās Valstis

Nelicencētu finanšu starpnieku tīkli sankciju apiešanas atbalstam

70. Vairākas valstis arī konstatēja, ka Irāna izmanto sarežģītas sankciju apiešanas shēmas, tostarp BOI slēpšanu, lai iegūtu divējāda lietojuma preces savai WMD programmai. Bieži vien novērots, ka Irāna izmanto galvenajos finanšu centros reģistrētus fiktīvus uzņēmumus, lai pārskaitītu līdzekļus no naudas maiņas punktiem, kas ir Irānas valdības kontrolē.

14. ierāmējums. Gadījuma izpēte: nelegālu TCSP izmantošana divējāda lietojuma preču tirdzniecībai

Irānas pilsoņi Nīderlandē nodibināja vairākas juridiskas personas, kas darbojās vai darbojas tehnoloģiju nozarē. Tas ietver uzņēmuma, kas ir atzīts sponsors,[38] izmantošanu, lai augsti kvalificētiem migrantiem atvieglotu Nīderlandes uzturēšanās atļaujas saņemšanu. Tāpat uzņēmums, kas ir atzīts sponsors ietilpst vai ir cieši saistīts ar TCSP, kas sniedz dažādus pakalpojumus, piemēram, reģistrē uzņēmumu, atver bankas kontu un pārbauda, vai vismaz puse no uzņēmuma direktoriem ir Nīderlandes pilsoņi (lai izmantotu Nīderlandes nodokļu priekšrocības un nodokļu nolīgumus).

Lai gan legālos TCSP uzrauga Nīderlandes Centrālā banka, nelegālie TCSP sadala savus pakalpojumus un izvieto tos vairākās juridiskās personās. Tādējādi šie pakalpojumi ir lētāki, un kļūst grūtāk atpazīt šādus trasta pakalpojumus. Tāpēc Nīderlandes Centrālajai bankai ir grūti uzraudzīt šos uzņēmumus. Šajā gadījumā nauda, kas, iespējams, nāk no Irānas caur pazīstamiem finanšu centriem, tiek nelikumīgi pārskaitīta Nīderlandes juridiskajām personām, kuras izveidoja nelegālais TCSP. Pēc tam nauda tiek pārskaitīta šajā struktūrā un galu galā nonāk pie augsti kvalificētiem migrantiem.

Šajā gadījumā bankas pārskatos ir norādīti vairāki darījumi, kas rada riskus saistībā ar divējāda lietojuma preču piegādi Irānai. Šīs preces ir izmantojamas arī proliferācijas nolūkos. Šie darījumi ir saistīti arī ar tehnoloģiju uzņēmumiem, kurus kontrolē Irānas augsti kvalificēti migranti. Tāpēc var secināt, ka šie uzņēmumi darbojas kā fiktīvi uzņēmumi. Izmantojot TCSP, jo īpaši nelegālos, un izveidojot uzņēmumu tīklu, ir ārkārtīgi grūti atpazīt šos finanšu darījumus.

Avots: Nīderlande

71. Nelicencēti MSB (naudas pakalpojumu sniedzēji) tiek izmantoti arī, lai pārskaitītu naudu personām, kuras rīkojas iekšzemes un ANO sarakstā iekļauto teroristu grupu labā. Turpmāk minētajā lietā AAE iestādes atklāja sarežģītu shēmu, kas izmantoja fiktīvu uzņēmumu kā aģentu *hawaladar,*[39] lai pārskaitītu miljoniem dolāru. Lai gan šis ir piemērs, kad privātpersonas nevalstisku dalībnieku vārdā izvairās no TF-TFS, tas varētu attiekties arī uz sarežģītām shēmām, ko izmanto, lai izvairītos no ar PF saistītām sankcijām.

[38] Atzīts sponsors ir uzņēmums, skola vai organizācija, kas gūst labumu no ārvalstnieku ierašanās.
[39] Hawaladar ir naudas pārvedējs, kas sniedz Hawala (uz uzticību balstītu naudas pārskaitījumu) pakalpojumus.

15. ierāmējums. Gadījuma izpēte: izmanto nelicencētu MSB, lai izvairītos no sankcijām ANO 1267. sarakstā iekļautai teroristu grupai

2022. gada 1. ceturksnī vietējais biržas nams iesniedza UAEFIU SAR/STR par naudas pārvedumiem no augsta riska jurisdikcijas, ko saņēma AAE ārvalstu rezidents. Visas pārskaitījumos iesaistītās puses bija UAEFIU iegūtās finanšu izlūkošanas informācijas subjekti.

Saskaņā ar UAEFIU veikto izmeklēšanu un analīzi galvenais aizdomās turētais saņēma septiņus elektroniskos pārskaitījumus par kopējo summu 3,5 miljoni ASV dolāru un AAE bija izveidojis fiktīvu uzņēmumu, kas darbojās kā *hawaladar*, lai pārskaitītu līdzekļus uz augsta riska valstīm un atbalstītu Dāiš (ISIL) un Al Nusra frontes dalībniekus. Abas grupas ir iekļautas AAE nacionālajā sarakstā un ANO konsolidētajā sarakstā – 1267/1989. UNSCR.

UAEFIU atklāja Valsts drošības dienestam lietas datus, kuros bija sīki izklāstīta informācija par aizdomās turēto un viņa fiktīvo uzņēmumu. Valsts drošības dienests sadarbībā ar UAEFIU un Centrālo banku izmeklēja aizdomās turēto finanšu darbības. Attiecīgi Valsts drošības dienests izdeva rīkojumu iesaldēt aizdomās turētā naudas līdzekļus un citus aktīvus par kopējo summu 500 000 ASV dolāru un 4 kg zelta. Tika apturēta arī fiktīvā uzņēmuma uzņēmējdarbība. Izmeklēšanas laikā aizdomās turamais atzina, ka ir nodrošinājis līdzekļus Dāiš (ISIL) un Al Nusra frontei, lai iegādātos militāro aprīkojumu, tostarp ieročus un munīciju.

Avots: Apvienotie Arābu Emirāti

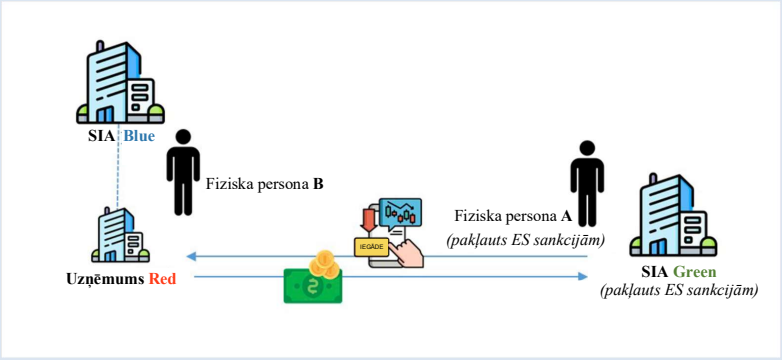
Dažādu juridisko personu veidu izmantošana, lai izvairītos no sankcijām

72. Dažas valstis ziņoja par meitasuzņēmumu un citu juridisko personu izmantošanu, lai slēptu patiesā labuma guvēja informāciju. Kopējā taktika ietvēra gan sarežģītu shēmu piemērus, lai izvairītos no sankcijām, gan vienkāršākas pieejas, lai mērķētu uz nozarēm, kurās nav stingras AML/CFT/CPF kontroles.

16. ierāmējums. Gadījuma izpēte: sarežģīta shēma, lai izvairītos no ES sankcijām

Persona A, kura ir pakļauta ES sankcijām, koordinēja sarežģītu shēmu ar personu B, lai veicinātu sankciju apiešanu. Pirmkārt, fiziskā persona B, sabiedrības ar ierobežotu atbildību (SIA) Blue īpašnieks, nodibināja meitasuzņēmumu ar nosaukumu Red. Otrkārt, fiziskā persona B izmantoja uzņēmumu Red, lai iegādātos fiziskās personas A līdzdalību SIA Green. Lai gan SIA Green pieder 28,5 miljoni akciju kādā Eiropas uzņēmumā, šīs akcijas tika iesaldētas, jo SIA Green kontrolēja fiziskā persona A. Tādējādi, kad sabiedrība Red iegādājās fiziskās personas A līdzdalību SIA Green, tā iegādājās arī iesaldētās Eiropas uzņēmuma akcijas. Apmaiņā pret SIA Green pārdošanu persona A saņēma līdzvērtīgu ekonomisku labumu.

Fiziskā persona B veicināja sankciju apiešanu, jo viņš un Krievijā bāzētie uzņēmumi (SIA Blue, uzņēmums Red un SIA Green) izmantoja šo shēmu, lai pārdotu uzņēmumu ārpus ES, kuru kontrolē sarakstā iekļauta fiziska persona un kuram pieder ES uzņēmuma iesaldētās akcijas, ar vienīgo mērķi atcelt šo akciju iesaldēšanu Eiropas Savienībā.



Avots: Eiropas Komisija

17. ierāmējums. Gadījuma izpēte: sarežģīta īpašumtiesību struktūra, ko izmanto, lai slēptu transportlīdzekļu patieso īpašnieku

Lai slēptu vairāku simtu tūkstošu eiro vērtu vairāku luksusa transportlīdzekļu patieso īpašnieku, tika izmantoti dažādi fiktīvi uzņēmumi. Pēdējam uzņēmumam ķēdē, Vācijā reģistrētai sabiedrībai ar ierobežotu atbildību, piederēja luksusa klases transportlīdzekļi. Lai gan SIA oficiālais pienākums bija pārvaldīt šos transportlīdzekļus, Centrālajam sankciju izpildes birojam, veicot plašu izmeklēšanu, izdevās pierādīt, ka uzņēmums kalpoja vienīgi tam, lai slēptu transportlīdzekļu patiesos īpašniekus.

Faktiski uzņēmumu un līdz ar to arī transportlīdzekļus kontrolēja persona, kas ES ir iekļauta Krievijas sankciju režīmā. Kad izmeklēšanā atklājās šī saikne starp minēto personu un SIA, transportlīdzekļi bija jāapķīlā. Turpmākā izmeklēšana ļāva attiecināt arī citus aktīvus uz sankciju sarakstā iekļauto personu.

Avots: Vācija

18. ierāmējums. Gadījuma izpēte: meitasuzņēmuma izmantošana, lai slēptu saikni ar ANO sarakstā iekļautu KTDR uzņēmumu

Uzņēmums BETA darbojas būvniecības un valsts pasūtījumu nozarē, kas ietver smagās tehnikas, stacionāro celtņu, mobilo celtņu, ekskavatoru, iekrāvēju un kravas automašīnu piegādi citiem uzņēmumiem. BETA galvenie klienti ir uzņēmums GAMMA un vairāki mazie un vidējie uzņēmumi, kas darbojas tajā pašā nozarē. BETA faktiskais īpašnieks, persona X, un vadītājs, persona Y, ir KTDR, valsts, uz kuru attiecas ANO sankcijas, pilsoņi.

Uzņēmums GAMMA, kas darbojas lauksaimniecības un pārtikas nozarē, iegādājās lauksaimniecības un pārtikas tehniku no uzņēmuma BETA. Kad uzņēmums BETA iekasēja neparastu skaitu čeku, kas pārsniedza 300 000 eiro (200 000 000 CFA franku), kāda Senegālas finanšu iestāde veica klienta uzticamības pārbaudi, kuras laikā atklājās, ka BETA mātesuzņēmums, kas atrodas Phenjanā, KTDR, ir iekļauts Apvienoto Nāciju Organizācijas 1718. sankciju sarakstā.

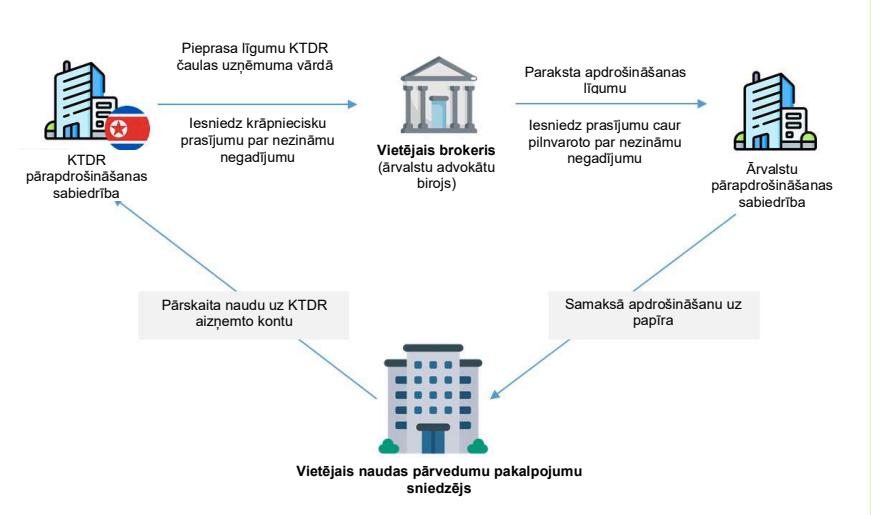
Kad tika pārbaudīta saikne ar sankcijām pakļauto uzņēmumu, finanšu iestāde iesniedza STR Senegālas FID (CENTIF), un uzņēmuma BETA aktīvi tika iesaldēti. STR ļāva CENTIF veikt izmeklēšanu, kas neatklāja GAMMA apzinātu līdzdalību sankciju apiešanas shēmā.

Avots: Senegāla

73. KTDR ir nopelnījusi miljoniem dolāru gadā, safabricējot negadījumus un apkrāpjot starptautisko apdrošināšanas tirgu. Tā kā Ziemeļkorejā nav iespējams pārbaudīt pieteikumus, KTDR pārapdrošināšanas uzņēmumi iegādājas starptautisko apdrošināšanu vai pārapdrošināšanu visai valsts infrastruktūrai, piemēram, tiltiem un rūpnīcām, un pēc tam vilto dokumentus, lai saņemtu apdrošināšanas atlīdzību. KTDR mobilizē čaulas uzņēmumus vai aizņemas kontus, lai parakstītu pārapdrošināšanas līgumus un saņemtu apdrošināšanas atlīdzību.[40]

[40] KTDR labā noslēgtā apdrošināšana un/vai pārapdrošināšana ir pretrunā 2270. UNSCR 33. un 36. pantam, kas aizliedz valstīm sniegt skaidras naudas, zelta un apdrošināšanas pakalpojumus, kas varētu veicināt KTDR kodolprogrammu vai ballistisko raķešu programmu.

19. ierāmējums. Ilustratīvs piemērs: KTDR izmanto necaurredzamus korporatīvos instrumentus, lai veiktu apdrošināšanas krāpšanu



Kredītkaršu un debetkaršu izmantošana KTDR

74. Vairākas valstis apzinās, ka ar KTDR saistītas personas aizvien biežāk slēpj savus finanšu profilus, izmantojot nelegāli iegūtus kontus Ķīnas valstspiederīgo vārdā un izmantojot virtuālos aktīvus, lai veiktu maksājumus un piekļūtu vietējai valūtai, tādējādi ļaujot KTDR turpināt apiet ANO sankcijas.

75. Pastāv aizdomas, ka KTDR baņķieri krāpnieciski pārvalda daudzas nelikumīgi iegūtas UnionPay debetkartes, ko simtiem vietējo kontu turētāju vārdā izsniegušas lielākās Ķīnā bāzētās komercbankas, lai veiktu maksājumus vietējā valūtā. Ir norādes, ka tas ir mēģinājums apiet sankcijas, slēpjot darījumus un saiknes ar KTDR, vienlaikus apejot valstis, kas piemēro stingrus KTDR sankciju režīmus, lai saņemtu peļņu un iegādātos aizliegtas preces.

76. Šo finanšu tīklu šķietami decentralizētais raksturs arī mazina jebkādu atsevišķu traucējumu ietekmi, kā arī ievērojami apgrūtina valsts iestādēm identificēt visus KTDR kontus. Ir norādes, ka KTDR izmanto nelikumīgi iegūtas UnionPay debetkartes, lai saņemtu iemaksas *fiat* valūtā, kas iegūta no nozagtām kriptovalūtām, kā arī koordinētu darījumus dažādām ar WMD saistītām struktūrām.

3. tipoloģija: Virtuālo aktīvu un citu tehnoloģiju izmantošana

77. Ir vērojama pieaugoša tendence, ka sankcijām pakļauti dalībnieki arvien vairāk iesaistās digitālās ekonomikas izmantošanas jomā. Virtuālie aktīvi un citas jaunās tehnoloģijas tiek izmantotas, lai apietu starptautiskos, pārnacionālos un valstu sankciju režīmus un finansētu WMD dalībniekus un darbības.[41] Virtuālie aktīvi tiek izmantoti, lai veicinātu finanšu plūsmas:

a) tieši uz valstīm, uz kurām attiecas sankcijas; un

b) netieši, izmantojot starpniekvalstis, kas nepiemēro sankciju pasākumus. Līdz ar to lielākā daļa valstu uzskata, ka virtuālo līdzekļu un citu jauno tehnoloģiju izmantošana, ko veic neatļautu darbību dalībnieki, ir galvenie PF apdraudējumi/ievainojamības faktori.

78. Plašākā kontekstā valstis tāpat ir identificējušas sankciju apiešanas problēmas, ko rada citas jaunās tehnoloģijas, piemēram, mākslīgais intelekts. Tomēr pierādījumi un tendences šajā jomā ir pārāk jaunas, lai izdarītu secinājumus, un ir maz gadījumu izpēšu.

Regulējuma grūtības

79. Neraugoties uz centieniem novērst jaunos riskus, kas saistīti ar virtuālajiem aktīviem un citām tehnoloģijām, daudzās valstīs nav AML/CFT prasību, kas piemērojamas VASP. 2024. gada aprīlī trīs ceturtdaļas FATF Globālā tīkla valstu tika novērtētas kā neatbilstošas vai daļēji atbilstošas starptautiskajiem standartiem attiecībā uz virtuālajiem aktīviem un VASP.[42] Trūkumi regulējumā un uzraudzībā starptautiskā līmenī ir padarījuši šo nozari neaizsargātu pret PF tīklu ļaunprātīgu izmantošanu. Kamēr dažādās jurisdikcijās pastāv nepilnības FATF standartu īstenošanā attiecībā uz virtuālajiem aktīviem un VASP, PF tīkli var izmantot VASP jurisdikcijās ar vāju regulējumu vai bez tā, un tas netiek atklāts un apturēts. Kā norādīts turpmāk minētajā gadījumā, ir arī situācijas, kad VASP, uz kuriem attiecas AML/CFT sistēmas, neievēro piemērojamās prasības.

20. ierāmējums. Gadījuma izpēte: Binance izpildes nodrošināšana

2023. gada novembrī Binance Holdings Limited (“Binance”) atzina savu vainu un piekrita samaksāt vairāk nekā 4 miljardus ASV dolāru, lai atrisinātu ASV Tieslietu departamenta izmeklēšanu par pārkāpumiem saistībā ar vairākām sankciju programmām, tostarp par to, ka uzņēmums nav reģistrējies kā naudas pārvedējs, un par Starptautiskā ārkārtas ekonomisko pilnvaru likuma (IEEPA) pārkāpumiem. Binance dibinātājs un izpilddirektors atzina savu vainu par efektīvas AML programmas neievērošanu, tādējādi pārkāpjot Banku slepenības likumu (BSA).

Daļēji tāpēc, ka Binance nespēja īstenot efektīvu AML programmu, neatļautu darbību dalībnieki izmantoja Binance biržu dažādos veidos, tostarp veicot darījumus, kas slēpa virtuālo aktīvu izcelsmi un īpašumtiesības, pārskaitot nelikumīgus ieņēmumus no izpirkuma maksu variantiem un pārvietojot ieņēmumus no tumšā tīkla tirgus darījumiem, biržas uzlaušanas un dažādām ar internetu saistītām krāpšanām.

---

41 2025. gada martā Indijā notikušajā Privātā sektora konsultatīvajā forumā dalībnieki uzsvēra paaugstinātos riskus, kas saistīti ar jaunajām finanšu tehnoloģijām, jo īpaši virtuālo aktīvu izmantošanu kibernoziegumos, ko veic valsts dalībnieki, tostarp KTDR, kas izmanto arvien sarežģītākas un izsmalcinātākas metodes.

42 https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2024-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf

Binance lietotāji veica darījumus ar virtuālo aktīvu biržām tādās ASV sankcijām pakļautās valstīs kā Irāna, neiesniedzot SAR/STR. Binance lietotāju makos tika veikti ievērojami tiešie darījumi ar dažādām Irānas virtuālo aktīvu biržām, katrs no tiem bija vairāk nekā 2000 ASV dolāru vērtībā, un to kopējā vērtība bija vairāk nekā pusmiljards dolāru. Šajā kopsummā ir iekļauti arī vairāki darījumi ar virtuālo aktīvu makiem, kas saistīti ar juridiskām un fiziskām personām, uz kurām attiecas sankcijas.

Avots: Amerikas Savienotās Valstis

Virtuālo aktīvu izmantošana līdzekļu pārvietošanai

80. Virtuālie aktīvi tiek izmantoti, lai slēptu līdzekļu plūsmu uz valstīm, kurām piemēro sankcijas, un ar tām saistītiem dalībniekiem. Virtuālie aktīvi var nodrošināt lietotājiem augstāku anonimitātes līmeni, ja tos apvieno ar noteiktiem paņēmieniem, un tos var nekavējoties pārskaitīt pāri robežām. Turklāt virtuālo aktīvu starptautiskais raksturs var radīt problēmas, kas saistītas ar ārvalstu VASP jurisdikciju pārbaudi, starptautiskai sadarbībai nepieciešamo laiku un resursiem, kā arī atšķirībām starp regulējuma sistēmām un sankciju režīmiem dažādās jurisdikcijās. Jo īpaši valstu sniegtie piemēri liecināja par virtuālo aktīvu maku un apmaiņas platformu izplatītu izmantošanu iespējamai sankciju apiešanai.

21. ierāmējums. Gadījuma izpēte: līdzekļi, kas pārskaitīti valsts sankcijām pakļautam VASP

Veicot plašāku pētījumu par jauno tehnoloģiju izmantošanu nelikumīgi iegūtu līdzekļu legalizēšanai un sankciju apiešanai, Ukrainas FID atklāja aizdomīgu līdzekļu apriti starp kriptovalūtu biržām, tostarp ar iekšzemes sankcijām pakļautu VASP.

FID konstatēja, ka kriptobirža (birža A), ko veido Eiropā un citās valstīs reģistrēti (tostarp Britu Virdžīnās, Honkongā, Apvienotajā Karalistē un Igaunijā) uzņēmumi, bija virtuālo aktīvu saņēmēja no divām citām augsta riska kriptobiržām (birža B un C). Lai gan biržas A īpašnieks bija reģistrēts kā Igaunijas pilsonis, šis gadījums ieinteresēja Ukrainas FID, jo īpašnieks tika uzskatīts par Ukrainas politiski nozīmīgu personu (PEP) un Ukrainas politiķa dēlu.

Birža A saņēma lielas līdzekļu summas no biržas B un C. Birža B tika identificēta kā Krievijai piederošs VASP, kam Ukraina 2023. gadā piemēroja sankcijas saskaņā ar tās iekšzemes sankciju režīmu. Birža C tika identificēta kā augsta riska birža, kuras īpašnieki tika arestēti aizdomās par 700 miljonu ASV dolāru atmazgāšanu. Ukrainas FID norāda, ka birža B un C, izmantojot Tron blokķēdi, pārskaitīja virtuālos aktīvus uz kriptobiržu A, lai slēptu līdzekļu izcelsmi un apriti.

FID konstatējumi pašlaik tiek izskatīti kā daļa no pirmstiesas izmeklēšanas.

Avots: Ukraina

22. ierāmējums. Gadījuma izpēte: dažādu metožu izmantošana, lai pārskaitītu līdzekļus uz KTDR

Dienvidkoreja 2024. gada decembrī piemēroja sankcijas vienam uzņēmumam un 15 personām, tostarp Kimam Čolam Minam (Kim Chol Min) un Kimam Rju Songam (Kim Ryu Song), kas abi ir kaimiņvalstī esošā 313. ģenerālbiroja ģenerāldirektori, par līdzekļu ģenerēšanu, kiberuzbrukumu veikšanu un virtuālo aktīvu zādzību KTDR vārdā.[43] Ar kaimiņvalstī esošo starpnieku palīdzību KTDR līdzekļu pārvietošanai izmantoja virtuālos makus, bankas, e-finansēšanas platformas un citus *fiat* valūtas kontus. Kad daļa no nelikumīgi iegūtajiem līdzekļiem tika konvertēta *fiat* valūtā, KTDR nosūtīja lielu naudas summu uz Phenjanu un izmantoja *fiat* valūtā iegūtos līdzekļus no konvertētajiem virtuālajiem aktīviem, lai iegādātos sankcijām pakļautās preces un finansētu režīma WMD programmu.

313. ģenerālbirojs kontrolē KTDR pētniecību un izstrādi, kā arī ieroču un cita militārā aprīkojuma ražošanu. Turklāt 313. ģenerālbirojs ir iesaistīts KTDR IT darbaspēka izvietošanā kaimiņvalstīs un visā pasaulē.

Avots: Dienvidkoreja

81. Ar PF un sankciju apiešanu saistītie dalībnieki izmanto arvien sarežģītākas metodes, lai nelikumīgi iegūtu līdzekļu legalizācijai izmantotu virtuālos aktīvus un slēptu līdzekļu avotus. Tādas valstis kā KTDR veic šo darbību, izmantojot anonimitāti veicinošas tehnoloģijas, piemēram, virtuālo valūtu mikserus, šķietami decentralizētas finansēšanas (DeFi) mehānismus, starpķēdes tiltus, kā arī VASP bez AML/CFT kontroles. Pēc līdzekļu legalizēšanas sankciju apiešanas dalībnieki bieži konvertē virtuālos aktīvus *fiat* valūtā pie ārpusbiržas (OTC) brokeriem, kas koncentrēti noteiktās jurisdikcijās.[44] Dažos gadījumos KTDR dod norādījumus OTC brokeriem nosūtīt konvertētos līdzekļus uz bankas kontiem, kas pieder fiktīviem uzņēmumiem, kuri iegādājas preces KTDR vārdā. Kā minēts iepriekš, dažos gadījumos KTDR izmanto nelikumīgi iegūtas UnionPay debetkartes, lai saņemtu iemaksas *fiat* valūtā, kas iegūta no nozagtiem virtuālajiem aktīviem.

Commented [LŽ5]: https://fid.gov.lv/uploads/files/2022/VVRN/VVRN%202022_FINAL%20%28002%29.pdf

23. ierāmējums. Gadījuma izpēte: sankciju noteikšana mikseriem, ko izmanto noziedzīgi iegūtu līdzekļu legalizēšanai

OFAC 2023. gada novembrī iekļāva sarakstā virtuālo valūtu mikserus, kas iesaistīti noziedzīgi iegūtu līdzekļu legalizēšanā KTDR vajadzībām, tostarp Sinbad.io (Sinbad).45 Sinbad kalpoja kā galvenais noziedzīgi iegūtu līdzekļu legalizēšanas rīks Lazarus Group – KTDR sponsorētai hakeru grupai. Sinbad apstrādāja miljoniem dolāru vērtus virtuālos aktīvus, ko Lazarus Group bija nozagusi, tostarp, veicot augsta profila zādzības no Horizon Bridge, Axie Infinity un Atomic Wallet. Līdzīgi kā Blender.io, Sinbad darbojās ar Bitcoin blokķēdi un bez izšķirības veicināja nelikumīgus darījumus, slēpjot to izcelsmi, galamērķi un darījumu partnerus.

Avots: Amerikas Savienotās Valstis

---

43 https://www.mofa.go.kr/www/brd/m_4080/view.do?seq=375771

44 https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html

24. ierāmējums. Gadījuma izpēte: KTDR kriminālvajāšana un saistītās izpildes darbības

ASV Tieslietu departaments 2023. gada aprīlī izdeva divus apsūdzības rakstus, kuros KTDR FTB pārstāvim izvirzītas apsūdzības par viņa lomu noziedzīgi iegūtu līdzekļu legalizēšanas sazvērestībās, kuru mērķis bija gūt ieņēmumus KTDR, izmantojot virtuālos aktīvus. Persona, iespējams, bija sazvērējusies ar diviem ārpusbiržas tirgotājiem, lai legalizētu nozagtos virtuālos aktīvus un izmantotu līdzekļus preču iegādei KTDR valdības vārdā ASV dolāros, izmantojot Honkongā bāzētus fiktīvos uzņēmumus.

Tāpat OFAC sarakstā iekļāva personu, kura saņēma desmitiem miljonu dolāru virtuālos aktīvos, kas daļēji iegūti no KTDR personām, kuras ASV esošie uzņēmumi neapzināti pieņēma darbā ASV, lai nodrošinātu IT izstrādes darbus. Ir zināms, ka, stājoties darba attiecībās, IT darbinieki pieprasa, lai viņiem maksā virtuālos aktīvos, un lielāko daļu algas nosūta, izmantojot sarežģītu naudas atmazgāšanas shēmu, lai šos nelikumīgi iegūtos līdzekļus novirzītu atpakaļ uz KTDR. Kad FTB pārstāvis acīmredzami bija saņēmis naudu no IT izstrādes darbiniekiem, viņš lika OTC virtuālo aktīvu tirgotājiem nosūtīt maksājumus fiktīviem uzņēmumiem, lai šie fiktīvie uzņēmumi KTDR režīma vārdā varētu veikt maksājumus *fiat* valūtā par precēm, piemēram, tabaku un sakaru ierīcēm. Šis process ir OFAC pastāvīgās sadarbības ar Tieslietu departamenta un Federālo izmeklēšanas biroju rezultāts. Šis process tika cieši koordinēts arī ar Korejas Republiku, kas norādīja uz to pašu personu par tās nelikumīgajām darbībām.

Avots: Amerikas Savienotās Valstis

Virtuālo aktīvu un fondu veidošana

82. Dažas valstis konstatēja, ka KTDR izmanto virtuālo aktīvu zādzības un kiberuzbrukumus, lai piesaistītu līdzekļus visā pasaulē, tostarp WMD un ballistisko raķešu programmām. Veicot šīs darbības, KTDR un ar to saistītie dalībnieki parasti koncentrējas uz organizācijām, kas darbojas blokķēdes tehnoloģiju un virtuālo aktīvu nozarē, tostarp VASP, DeFi pakalpojumiem, blokķēdes tiltu izstrādātājiem, virtuālo aktīvu tirdzniecības uzņēmumiem un riska kapitāla fondiem, kas iegulda virtuālajos aktīvos.

83. 2024. gada ANO ekspertu grupas ziņojumā par KTDR tika uzsvērta KTDR režīma globālā kiberaktivitāte, kurā tika izmeklēti kopumā 58 iespējamie KTDR kiberuzbrukumi ar virtuālajiem aktīviem saistītiem uzņēmumiem no 2017. līdz 2023. gadam, kuru vērtība bija aptuveni 3 miljardi ASV dolāru.[46] Saskaņā ar Chainalysis datiem ar KTDR saistītie hakeri 2023. gadā no DeFi platformām nozaga aptuveni 428,8 miljonus ASV dolāru, kā arī vērsās pret centralizētajiem dienestiem (nozagti 150,0 miljoni ASV dolāru), biržām (330,9 miljoni ASV dolāru) un maku nodrošinātājiem (127,0 miljoni ASV dolāru).[47] Valstis arī uzsvēra KTDR krāpniecisko IT pakalpojumu darbinieku izvietošanu, lai iegūtu līdzekļus (dažos gadījumos saņemot samaksu virtuālajos aktīvos) un izvairītos no sankcijām. KTDR dalībnieki izmanto iepriekš minētajā sadaļā aprakstītās metodes, lai legalizētu virtuālajos aktīvos gūtos ienākumus.

---

46 S/2024/215

47 Chainalysis 2024 Crypto Crime Report (Chainalysis 2024. gada kriptovalūtu noziegumu ziņojums) (44.-46. lpp.) Gadījuma izpēte: KTDR Atomic Wallet izmantošana.

25. ierāmējums. Gadījuma izpēte: kibertelpā veiktās zādzības un krāpšana

2021. gada februārī Tieslietu departaments apsūdzēja trīs KTDR datorprogrammētājus par dalību plašā noziedzīgā sazvērestībā, kuras mērķis bija veikt virkni destruktīvu kiberuzbrukumu, nozagt un izspiest no finanšu iestādēm un uzņēmumiem vairāk nekā 1,3 miljardus ASV dolārus naudā un kriptovalūtā, izveidot un izvietot vairākas ļaunprātīgas kriptovalūtu lietojumprogrammas, kā arī izstrādāt un krāpnieciski tirgot blokķēdes platformu.

Apsūdzības rakstā apgalvots, ka trīs apsūdzētie ir bijuši KTDR militārās izlūkošanas aģentūras – Izlūkošanas ģenerālbiroja (RGB) – vienību dalībnieki, kas nodarbojās ar noziedzīgu uzlaušanu.[48] Šīs KTDR militārās hakeru vienības kiberdrošības kopienā ir pazīstamas ar vairākiem nosaukumiem, tostarp Lazarus Group un Advanced Persistent Threat 38 (APT38).

Apsūdzības rakstā apgalvots, ka sazvērestība Amerikas Savienotajās Valstīs un ārvalstīs ir veikusi plašu kibernoziegumu klāstu, lai atriebtos vai gūtu finansiālu labumu. Iespējamās shēmas ietver ļaunprātīgu kriptovalūtas lietojumprogrammu izveidi un izvietošanu, vēršanos pret kriptovalūtas uzņēmumiem un kriptovalūtas zādzību, mērķētas pikšķerēšanas kampaņas, kā arī *Marine Chain Token* un sākotnējo monētu piedāvājumu.

Saskaņā ar apsūdzībā ietvertajiem apgalvojumiem trīs apsūdzētie bija RGB vienību dalībnieki, kurus KTDR valdība dažkārt izvietoja citās valstīs, tostarp Ķīnā un Krievijā. Lai gan šie apsūdzētie bija daļa no RGB vienībām, kuras kiberdrošības pētnieki dēvē par Lazarus Group un APT 38, apsūdzības rakstā apgalvots, ka šīs grupas bija iesaistītas vienotā sazvērestībā, lai nodarītu kaitējumu, nozagtu datus un naudu un citādi veicinātu KTDR stratēģiskās un finansiālās intereses.

Valsts kase un Tieslietu departaments vērsās arī pret diviem Ķīnas pilsoņiem, kuri tika apsūdzēti par vairāk nekā 100 miljonu ASV dolāru kriptovalūtas legalizēšanu, uzlaužot kriptovalūtas biržu. Saskaņā ar procesuālajiem dokumentiem KTDR līdzdalībnieki 2018. gadā uzlauza virtuālās valūtas biržu un nozaga virtuālo valūtu gandrīz 250 miljonu ASV dolāru vērtībā. Pēc tam noziedzīgi iegūtie līdzekļi tika legalizēti, izmantojot simtiem automatizētu kriptovalūtas darījumu, kuru mērķis bija novērst iespēju tiesībaizsardzības iestādēm izsekot šo līdzekļu izcelsmei. Apsūdzības rakstā arī apgalvots, ka laikā no 2017. gada decembra līdz 2019. gada aprīlim abi apsūdzētie legalizēja virtuālo valūtu vairāk nekā 100 miljonu ASV dolāru vērtībā, kas galvenokārt tika iegūti no virtuālo valūtu biržas uzlaušanas. OFAC iekļāva abas personas sarakstā par materiālu atbalstu Lazarus Group.

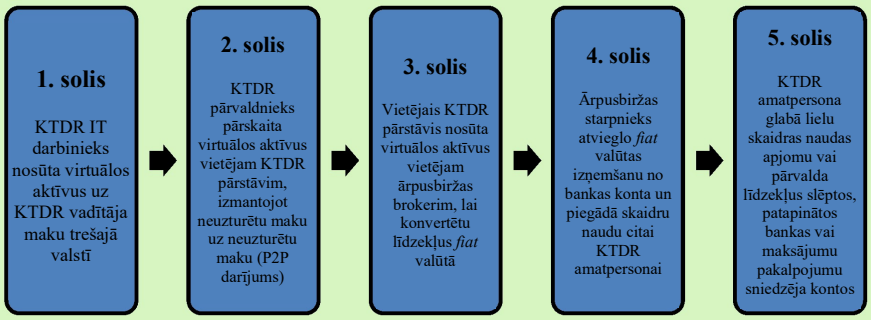
Avots: Amerikas Savienotās Valstis

84. Turklāt KTDR ir nosūtījusi tūkstošiem augsti kvalificētu IT darbinieku visā pasaulē, lai gūtu ienākumus, kas veicina tās WMD un ballistisko raķešu programmas. Šie IT darbinieki izmanto esošo pieprasījumu pēc specifiskām IT prasmēm, piemēram, programmatūras un mobilo lietojumprogrammu izstrādes, lai saņemtu ārštata darba līgumus no klientiem visā pasaulē, tostarp Āzijā, Eiropā un Ziemeļamerikā. Daudzos gadījumos KTDR IT darbinieki sevi dēvē par starptautiski strādājošiem un/vai tālstrādniekiem, kas nav no KTDR. KTDR IT darbinieki, kas saņem projektus, izmantojot starpnieka identitāti, var vēl vairāk slēpt savu identitāti un/vai atrašanās vietu, slēdzot apakšlīgumus par projektiem.

[48] 1718. UNSCR sarakstā RGB ir apzīmēts kā KPe.031.

Nauda tiek nosūtīta atpakaļ uz KTDR, izmantojot dažādas metodes, lai apietu sankcijas, tostarp izmantojot starpniekus un slēpjot BOI (skatīt 1. un 2. tipoloģiju). Tāpat virtuālie aktīvi tiek izmantoti, lai pārskaitītu līdzekļus uz KTDR.

26. ierāmējums. Ilustratīvs piemērs: KTDR IT darbinieka nelikumīgi iegūto līdzekļu pārvietošanas process



Ārvalstu uzņēmumi un privātpersonas veic krāpšanu, lai slēptu izdevīgus darījumus ar KTDR IT darbiniekiem

85. Turklāt KTDR IT darbinieki sadarbojas arī ar ārvalstu privātpersonām un uzņēmumiem, lai vēl vairāk maskētu savu līdzdalību sankciju apiešanas shēmās un tādējādi pelnītu naudu. Vienā no turpmāk minētajiem gadījumiem ar KTDR saistītie IT darbinieki mērķtiecīgi vērsās pret Japānas uzņēmumiem, lai piesaistītu un pārvietotu līdzekļus. Citā pētījumā ASV pilsonis piedalījās shēmā, kas ietvēra noziedzīgi iegūtu līdzekļu legalizēšanu un identitātes zādzību, lai atbalstītu KTDR IT darbiniekus.

27. ierāmējums. Gadījuma izpēte: krāpšanas shēmas, lai maskētu ienesīgas darījumu attiecības ar KTDR IT darbiniekiem

2024. gada martā par krāpšanu un citiem noziegumiem tika arestēts Dienvidkorejas pilsonis, kurš bija ar IT saistīta uzņēmuma prezidents un bijušais darbinieks. Izmeklēšanas laikā tika konstatēts, ka aizdomās turētie bija viltojuši dokumentus un lūguši KTDR IT darbiniekus, kas, kā viņi uzskatīja, atrodas Ķīnā, izstrādāt Japānas uzņēmuma pasūtītas lietojumprogrammas, izmantojot tiešsaistes platformu. Pastāvēja aizdomas, ka šīs iespējamās darbības ir paredzētas, lai atbalstītu shēmu sankciju apiešanai, jo šos līdzekļus varētu izmantot KTDR WMD programmai, kas ir pretrunā 1718. UNSCR.

2024. gada septembrī tika arestētas divas Japānas personas par sazvērestību ar iespējamo KTDR IT darbiniekus, lai izmantotu aizliegtu "automātisko tirdzniecības sistēmu" valūtas maiņas darījumu veikšanai, kā arī par nelikumīgu reģistrēšanos klientu datubāzē un kontu atvēršanu. Aizdomās turētie tiek turēti aizdomās par šo nelikumīgo valūtas maiņas darījumu rezultātā iegūto līdzekļu pārskaitīšanu uz Ziemeļkoreju.

Avots: Japāna

28. ierāmējums: ASV Tieslietu departaments izjauc KTDR attālo IT darbinieku krāpšanas shēmas, izvirzot apsūdzības un arestējot Nešvilas starpnieku

2024. gada augustā ASV Tieslietu departaments publiskoja apsūdzības rakstu, kurā ASV pilsonis tiek apsūdzēts sazvērestībā ar mērķi legalizēt noziedzīgi iegūtus naudas līdzekļus un vairākos citos noziegumos, lai gūtu ienākumus KTDR nelikumīgo ieroču programmai, kas ietver WMD. Saskaņā ar tiesas dokumentiem apsūdzētais piedalījās shēmā, kuras mērķis bija palīdzēt ārzemju IT darbiniekiem iegūt attālinātu IT darbu ASV uzņēmumos, kuri uzskatīja, ka nodarbina ASV strādājošu personālu. IT darbinieki, kuri bija KTDR pilsoņi, izmantoja nozagtu ASV pilsoņa identitāti, lai iegūtu šo attālināto IT darbu.

Saskaņā ar tiesas dokumentiem apsūdzētais vadīja "klēpjdatoru fermu" savās dzīvesvietās Nešvilā no aptuveni 2022. gada jūlija līdz 2023. gada augustam. Cietušie uzņēmumi nosūtīja klēpjdatorus, kas adresēti "Andrew M.", uz apsūdzētā dzīvesvietām. Pēc klēpjdatoru saņemšanas apsūdzētais lejupielādēja un instalēja neatļautas attālās darbvirsmas lietojumprogrammas un piekļuva cietušo uzņēmumu tīkliem, tādējādi nodarot datoriem kaitējumu. Attālinātās darbvirsmas lietojumprogrammas ļāva KTDR IT darbiniekiem strādāt no vietām Ķīnā, bet cietušajiem uzņēmumiem šķita, ka "Andrew M." strādā no apsūdzētā dzīvesvietas Nešvilā.

Ar apsūdzētā klēpjdatoru fermu saistītajiem ārzemju IT darbiniekiem no 2022. gada jūlija līdz 2023. gada augustam par viņu darbu tika samaksāti vairāk nekā 250 000 ASV dolāru, no kuriem liela daļa tika nepatiesi uzrādīta ASV Iekšējo ieņēmumu dienestam un Sociālā nodrošinājuma pārvaldei, izmantojot tās ASV personas vārdu, kuras identitāte tika nozagta. Apsūdzētā un viņa konspiratoru darbības cietušajiem uzņēmumiem radīja arī vairāk nekā 500 000 ASV dolāru izmaksas, kas bija saistītas ar to ierīču, sistēmu un tīklu revīziju un labošanu. Apsūdzētais un citas personas slepus sadarbojās, lai veiktu nelikumīgi iegūtu līdzekļu legalizēšanu, veicot finanšu darījumus, lai saņemtu maksājumus no cietušajiem uzņēmumiem, pārskaitītu šos līdzekļus apsūdzētajam un uz kontiem ārpus Amerikas Savienotajām Valstīm, mēģinot gan veicināt savu nelikumīgo darbību, gan slēpt, ka pārskaitītie līdzekļi ir no tās gūtie ienākumi. Starp kontiem, kas nav ASV konti, ir konti, kas saistīti ar KTDR un Ķīnas dalībniekiem.

Avots: Amerikas Savienotās Valstis

4. tipoloģija: Jūras un kuģniecības nozaru izmantošana

86. Saskaņā ar Starptautiskās Jūrniecības organizācijas (SJO) definīciju *ēnu flote* jeb *tumšā flote* ir "[...] kuģi, kas iesaistās nelikumīgās operācijās, lai apietu sankcijas vai iesaistītos citās nelikumīgās darbībās [...]."[49] Jūras nozare ir kļuvusi par galveno mērķi, ko izmanto neatļautu darbību dalībnieki, izmantojot tās sarežģītību, starptautisko pārklājumu, anonimitāti un ierobežoto AML/CFT/CPF kontroli. Jūras nozare ietver plašu kuģu, ostu, loģistikas un starptautisko noteikumu tīklu, ko neatļautu darbību dalībnieki var izmantot, lai apietu sankcijas un gūtu ieņēmumus, kas var veicināt PF. Lai gan FATF standarti neattiecas uz jūrniecības nozari, vairākas valstis savā PF riska novērtējumā norādīja, ka šīs nozares izmantošana ir viens no galvenajiem ievainojamības faktoriem.

[49] Starptautiskā jūrniecības organizācija, "Aicinājums dalībvalstīm un visām attiecīgajām ieinteresētajām pusēm veicināt darbības, lai novērstu "tumšās flotes" vai "ēnu flotes" nelikumīgas darbības jūrniecības nozarē" (2023. gada 6. decembris). A 1192 33

Tādēļ sankciju apiešanas un PF riskiem potenciāli ir pakļauti dažādi jūrniecības nozares aspekti un darbības, tostarp jūrniecības apdrošināšanas līgumi, jūrniecības uzņēmumi, atklātie reģistri, preču tirgotāji un divējāda lietojuma preču ražotāji.[50]

87. Neatļautu darbību dalībnieki var izmantot dažādas krāpnieciskas kuģošanas taktikas, lai slēptu kuģi, tā izcelsmi vai apzīmējumu, aizklātu savu darbību patieso būtību un izvairītos no atklāšanas. Lai gan paņēmieni pārklājas, taktiku var iedalīt četrās galvenajās kategorijās: kuģa identifikācija, pārvietošana no kuģa uz kuģi, AIS raidījumu atspējošana vai maskēšana un dokumentu viltošana. Tomēr ir svarīgi atzīmēt, ka neatļautu darbību dalībnieki, kas mēģina īstenot PF un sankciju apiešanas shēmas, var izmantot vairāk nekā vienu taktiku, lai sasniegtu savus mērķus.

Kuģa identifikācijas maiņa

88. Kā minēts 2. tipoloģijā, neatļauto darbību dalībnieki var slēpt informāciju par patieso labuma guvēju, lai apietu sankciju režīmus un piekļūtu oficiālajai finanšu sistēmai. Jūras nozarē neatļauto darbību dalībnieki var fiziski pārveidot tirdzniecības kuģus, lai tos pasniegtu kā citus transportlīdzekļus, un slēpt to identitāti, lai slēptu to patiesos īpašniekus un darbības. Piemēram, kuģa fizisko identitāti var viltot, pārkrāsojot kuģa nosaukumu, izmantojot citu valstu karogus un mainot tā unikālo SJO kuģa identifikācijas numuru. Fiziski pārveidojot tirdzniecības kuģus un slēpjot to identitāti, neatļauto darbību dalībnieki iegūst anonimitāti un var maskēt kuģa nelikumīgo darbību vēsturi. Turpmākajā pētījumā ir piemērs, kad kuģis mainīja savu identifikāciju, lai apietu Apvienoto Nāciju Organizācijas Drošības padomes rezolūcijas par KTDR.

[50] Lai palīdzētu biedriem sagatavoties savstarpējiem novērtējumiem un reaģēt uz jauniem reģionāliem riskiem, APG sekretariāts ar Apvienoto Nāciju Organizācijas Narkotiku un noziedzības apkarošanas biroja atbalstu publicēja Informatīvo lapu par kuģniecības reģistriem un PF riskiem: Āzijas/Klusā okeāna valstu grupa par noziedzīgi iegūtu līdzekļu legalizāciju.

29. ierāmējums. Gadījuma izpēte: ieņēmumu gūšana no nelegālām oglēm jūrniecības nozarē

2022. gadā Indonēzijas iestādes, patrulējot Indonēzijas ūdeņos, aizturēja Petrel 8. 2017. gadā Komoru salu karoga sauskravu kuģis Petrel 8 tika iekļauts ANO Sankciju sarakstā par nelegālu ogļu pārvadāšanu uz KTDR. Šajā lietā Indonēzijas iestādes koordinēja savu darbību ar ANO 1718. Sankciju komiteju. Indonēzijas Ārlietu ministrija (MOFA) pieprasīja informāciju no Indonēzijas Finanšu izmeklēšanas dienesta (PPATK), kas, pateicoties starptautiskai sadarbībai, ļāva atklāt šo gadījumu.

Izmeklēšanā atklājās, ka Indonēzijas kuģniecības korporācija PT Lintas Bahari Nusantara bija iegādājusies kuģi no Japānas uzņēmuma UYO Co. Ltd. par aptuveni 500 000 jenu, un finansējumu nodrošināja Bank BCA. Lai gan sākotnējā izmeklēšanā netika konstatētas nekādas tiešas finansiālas saiknes ar KTDR, kuģa aizturēšanas iemesls bija tā iesaistīšanās nepārtrauktā KTDR sankciju apiešanā. Lai izvairītos no atklāšanas, tika izmantotas tādas metodes kā kuģa identitātes viltošana un citu valstu karogu izmantošana. Kuģis tika iegādāts par aptuveni 61 miljardu Indonēzijas rūpiju (4 miljoniem ASV dolāru), un tas tika izmantots ogļu transportēšanai uz KTDR. Lai iegādātos Petrel 8, Indonēzijas uzņēmums pārskaitīja līdzekļus Japānas uzņēmumam.

Šis gadījums atklāja ievainojamību kuģu īpašumtiesību maiņas un nelikumīgas tirdzniecības prakses uzraudzībā, uzsverot vajadzību pēc pastiprinātas starptautiskās sadarbības, lai novērstu sankciju apiešanu. Pēc diskusijām ar ANO 1718. Sankciju komiteju 2023. gadā lēmums par Petrel 8 nodošanu metāllūžņos tika atzīts par visefektīvāko risinājumu, lai novērstu turpmākas sankciju apiešanas darbības.

Avots: Indonēzija

Pārvietošana no kuģa uz kuģi

89. Pārvietošana no kuģa uz kuģi notiek, kad preces tiek pārceltas no viena kuģa uz otru atklātā jūrā. Lai gan pārvietošana no kuģa uz kuģi var būt likumīga prakse, šī prakse ir identificēta kā augsta riska prakse sankciju apiešanas jomā, jo neatļautu darbību dalībnieki var izmantot šo metodi, lai slēptu sūtījumu izcelsmi vai galamērķi. Tas apgrūtina valsts iestādēm izsekot sankcijām pakļautas preces un identificēt starptautisko sankciju pārkāpumus. Turklāt atklātības trūkums var izraisīt to, ka jūrniecības apdrošinātāji neapzināti apdrošina tādu kuģu kuģošanu, kas iesaistīti nelikumīgā pārvietošanā no kuģa uz kuģi.

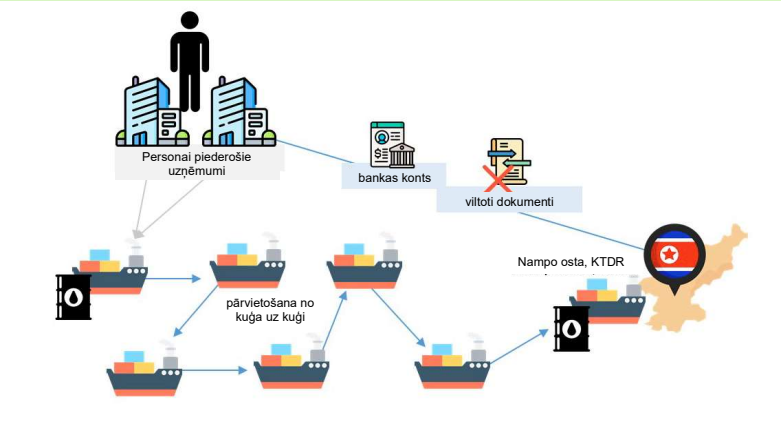
90. Kā ziņo viena jurisdikcija, KTDR flotē ir vismaz 28 tankkuģi, kas var veikt rafinētu naftas produktu pārvietošanu no kuģa uz kuģi, un vismaz 33 kuģi, kas var pārvadāt ogles. KTDR veiktā pārvietošana no kuģa uz kuģi bieži vien ir skaidras naudas darījumi, kas nenotiek ar finanšu iestāžu starpniecību, tādējādi uzsverot papildu neaizsargātību saistībā ar PF un sankciju apiešanas risku. Turpmāk izklāstītajos gadījumu pētījumos detalizēti aprakstīts, kā neatļautu darbību dalībnieki var izmantot pārvietošanu no kuģa uz kuģi, lai pārvadātu aizliegtus priekšmetus, apietu sankcijas un maskētu patieso izcelsmi vai galamērķi, lai izvairītos no atklāšanas.

30. ierāmējums. Gadījuma izpēte: jūras nozares izmantošana, lai piegādātu gāzeļļu KTDR

Iespējams, ka 2019. gada beigās kāda persona kopā ar piecām citām personām ārvalstīs septiņas reizes slepus sadarbojās, lai, izmantojot kuģi MT Courageous, piegādātu KTDR aptuveni 12 260 tonnas gāzeļļas. Pirmajos sešos gadījumos piegādes tika veiktas, pārvietojot no kuģa uz kuģi, bet pēdējā pārkraušana notika KTDR Nampo ostā. Iespējamās darbības ir Singapūras ANO KTDR noteikumu un 1718. UNSCR sankciju režīma pārkāpums.

Persona tiek apsūdzēta par to, ka četras reizes izmantojusi uzņēmuma, kura direktors bija viņš, bankas kontu, lai veiktu maksājumus par gāzeļļas iegādi un piegādi KTDR. Šī persona arī, iespējams, divos gadījumos viltojusi uzņēmumam piederošus dokumentus un piecas reizes izmantojusi cita viņa kontrolēta uzņēmuma bankas kontu, lai saņemtu maksājumus par aizliegtām gāzeļļas piegādēm KTDR. Turklāt apsūdzētais, iespējams, melojis izmeklēšanas amatpersonai, iznīcinājis pierādījumus un nav informējis policiju par gāzeļļas piegādi KTDR no cita kuģa 2019. gada februārī.

Līdz ar to apsūdzētajam izvirzītas vairākas apsūdzības, tostarp par aizliegtu priekšmetu piegādi KTDR, kontu viltošanu, labumu gūšanu no noziedzīgām darbībām, tiesvedības procesa aizkavēšanu un neatklāšanu par aizliegtu darījumu. Turklāt pirmajam uzņēmumam, kura direktors bija apsūdzētais, ir izvirzītas četras apsūdzības par tādu finanšu aktīvu nodošanu, kas var veicināt aizliegtu darbību, pārkāpjot Singapūras ANO noteikumus par KTDR, un otrajam uzņēmumam izvirzītas piecas apsūdzības par labumu gūšanu no noziedzīgas darbības. Tiesvedība tiesā turpinās.



Avots: Singapūra

31. ierāmējums. Gadījuma izpēte: naftas nodošana KTDR kuģiem atklātā jūrā

No 2017. gada janvāra līdz 2022. gada oktobrim Ķīnas Taipejas prokurori izmeklēja 11 lietas, kas bija saistītas ar KTDR sankciju pārkāpumiem.[51] Visbiežāk sastopamā ar PF saistītā tipoloģija ir naftas nodošana KTDR kuģiem atklātā jūrā no trešo jurisdikciju kuģiem, kurus kontrolē Ķīnas Taipejas naftas uzņēmumi, vai naftas nodošana trešo jurisdikciju kuģiem, kuri to tālāk pārdod KTDR kuģiem.

Naftas produkti joprojām ir visizplatītākā prece, ko tirgo Ķīnas Taipejas privātpersonas, pārkāpjot ANO sankcijas. Saskaņā ar vietējiem tiesību aktiem naftas tirdzniecība atklātā jūrā ir likumīga. Kuģniecības uzņēmumu pārstāvji vai patiesie labuma guvēji, tostarp ārvalstu valstspiederīgie, citi starpnieki, iesaistot sarežģītas uzņēmējdarbības struktūras, rīkojas kā starpnieki šķietami likumīgos darījumos, lai slēptu nelikumīgu naftas nodošanu, veicot pārvietošanu no kuģa uz kuģi jūrā. Tiek izmantota arī viltota eksporta informācija un ārzonas uzņēmumi un konti, lai kavētu līdzekļu izsekošanu.[52]

Avots: Ķīnas Taipeja

Automātiskās identificēšanas sistēmas raidījumu atspējošana un manipulēšana ar tiem

91. Automātiskās identificēšanas sistēma (AIS) ir piekrastes izsekošanas sistēma, ko izmanto uz kuģiem, lai sniegtu identifikācijas un atrašanās vietas informāciju, ļaujot iestādēm izsekot pārvietošanos.[53] Neatļautu darbību dalībnieki var manipulēt ar datiem, kas pārraidīti, izmantojot AIS raidījumus, tostarp mainīt kuģu nosaukumus, SJO numurus vai citu unikālu identifikācijas informāciju, lai palīdzētu slēpt kuģa reisu. Turklāt ēnu flotes bieži vien atspējo AIS apraidi, faktiski ejot "pa kluso" un pārtraucot kustības izsekošanu.[54]

92. Kā ziņo valstis un atspoguļots 2397. UNSCR (2017), ar KTDR karogu peldoši, kontrolēti, fraktēti vai ekspluatēti kuģi apzināti atslēdz vai manipulē ar AIS transponderiem, lai izvairītos no ANO sankcijām un gūtu ieņēmumus, kas vēsturiski ir veicinājuši valsts WMD un ballistisko raķešu programmas.[55] Turpmāk izklāstītajā pētījumā ir sīki aprakstīti divi atsevišķi gadījumi, kad, pārkāpjot ar KTDR saistītās UNSCR, uz civiliem kuģiem tika atklātas, arestētas un konfiscētas KTDR izcelsmes ogles.

---

51 Piecās lietās tika pasludināti notiesājoši spriedumi, trijās lietās apsūdzētie tika atzīti par nevainīgiem, bet trīs lietās kriminālvajāšana netika uzsākta.

52 Terorisma finansēšanas apkarošanas likuma 9. panta 1. daļas 1. apakšpunkta subjektīvais elements prasa, lai aizdomās turētais "apzināti" veiktu tirdzniecību ar sankciju objektu, un starpnieku iejaukšanās ir apgrūtinājusi šī elementa pierādīšanu.

53 Starptautiskā jūrniecības organizācija, "PĀRSKATĪTĀS PAMATNOSTĀDES KUĢU AUTOMĀTISKĀS IDENTIFICĒŠANAS SISTĒMU (AIS) DARBĪBAI UZ KLĀJA" (2015. gada 2. decembris). A 1106 29

54 SJO ir noteikusi, ka AIS lieto visi kuģi, kuru bruto tonnāža pārsniedz 300 tonnas un kuri veic starptautiskus reisus, kā arī visi pasažieru kuģi neatkarīgi no to lieluma.

55 2397. UNSCR

32. ierāmējums. Gadījuma izpēte: KTDR izcelsmes ogļu atklāšana uz kuģiem, arests un konfiskācija

Divos atsevišķos incidentos Kambodža atklāja, ka KTDR izmanto civilos kuģus, lai palīdzētu eksportēt ogles, tādējādi pārkāpjot 2397. un 2375. UNSCR, kas aizliedz šādas darbības. Abos gadījumos kuģi un to krava tika konfiscēta, un personas tika atzītas par vainīgām 1) nelikumīgā iebraukšanā Kambodžā un 2) mēģinājumā veikt preču kontrabandu Kambodžas muitas zonā.

Saskaņā ar ANO pienākumiem Kambodža regulāri izmeklē un pārbauda īpašumus un kuģus, kas iebrauc no atklātās jūras, lai konstatētu iespējamus ar KTDR saistīto ANO sankciju pārkāpumus. Dažkārt kuģi izmanto maskēšanas paņēmienus, lai maldinātu par savu kravu izcelsmi, piemēram, izslēdzot automātiskās identificēšanas sistēmu (AIS), lai slēptu uz kuģa esošās preces, izdomātu to atrašanās vietu vai veiktu pārvietošanu no kuģa uz kuģi. Divi nesen apķīlātie kuģi atspoguļo taktiku, ko izmanto KTDR kuģi, lai maskētu nelegālās kravas izcelsmi.

Pirmajā gadījumā Kambodžas iestādes 2024. gada februārī arestēja motorkuģi (M/V) HJL. Pēc tam, kad ārvalstīs reģistrētais kuģis pietuvojās KTDR ūdeņiem, kuģis izslēdza AIS apraidi. Nākamajā dienā kuģa AIS pārraidīja atrašanās vietu, kas norādīja, ka HJL ir noenkurojies, lai gan kuģis joprojām atradās ceļā ar viltus nosaukumu. Kad HJL iebrauca Kambodžas teritoriālajos ūdeņos, Kambodžas iestādes kuģi aizturēja, saņemot palīdzību no citas jurisdikcijas, kas dalījās ar informāciju par aizdomīgu kuģi. Šīs starptautiskās sadarbības rezultātā tika konfiscēts kuģis HJL, kas pārvadāja 12 000 tonnu akmeņogļu rūdas no KTDR. Kuģis iebrauca Kambodžas teritoriālajos ūdeņos, lai noenkurotos, iespējams, tur, kur tas sagaidītu savus pircējus. Saskaņā ar pastāvīgajiem rīkojumiem un ņemot vērā uz kuģa esošo saturu, prokuratūra apķīlāja kuģi un tā kravu turpmākai izmeklēšanai un tiesvedībai.

Otrajā gadījumā 2024. gada maijā Kambodžas iestādes apķīlāja M/V CNI pēc tam, kad kuģis veica pārvietošanu no kuģa uz kuģi ar KTDR kuģi KTDR ūdeņos, pārvadājot ANO aizliegtu kravu, tostarp 4800 tonnas ogļu rūdas. Turpmākajā izmeklēšanā tika noskaidrots, ka sūtījumu organizēja loģistikas uzņēmums trešajā valstī un ka šis uzņēmums organizēja KTDR izcelsmes ogļu rūdu importu, bet slēpa to izcelsmi, izmantojot viltotus dokumentus.

Avots: Kambodža

93. Divos iepriekš minētajos gadījumos konstatētās ievainojamības liecina, ka valstīm ir jāapsver iespēja palielināt uzraudzības biežumu un patrulēšanas spēku klātbūtni, kā arī uzlabot izsekošanas sistēmas teritoriālajos ūdeņos, jo īpaši tajos, kas ģeogrāfiski atrodas tuvu starptautiskajiem ūdeņiem.

Dokumentu viltošana

94. Papildu taktika, kā slēpt kravas izcelsmi vai galamērķi, ir viltotu dokumentu izmantošana, pārvadājot preces, kuru izcelsme ir KTDR vai kuras ir paredzētas KTDR, jo īpaši divējāda lietojuma preču eksportam. Šajā gadījumā neatļautu darbību dalībnieki pēc nosūtīšanas izmaina sūtījuma transporta dokumentus, tādējādi slēpjot faktisko preču galamērķi. Šāda prakse parasti ietver čaulas uzņēmumu trešajā valstī, kuru vairāk vai mazāk tieši kontrolē proliferācijas uzņēmums. Muitas iestāžu un kravas nosūtītāja priekšā čaulas uzņēmums ir oficiālais kravas saņēmējs. Tomēr pēc preču nosūtīšanas sponsors izdara izmaiņas pārvadājuma dokumentācijā, lai sūtījumu varētu novirzīt uz augsta riska jurisdikciju, kas saistīta ar PF.

95. Papildus dokumentācijas viltošanas praksei, kas saistīta ar KTDR, tā ir izplatīta taktika, lai izvairītos no sankcijām un eksporta kontroles arī citur. Turpmāk aprakstītajos piemēros ir parādīts, kā neatļauto darbību dalībnieki var manipulēt ar transporta dokumentiem jau pārvadāšanas procesa sākumā, lai slēptu divējāda lietojuma preču eksportu.

33. ierāmējums. Gadījuma izpēte: rēķinu viltošana un nepatiesas deklarācijas par divējāda lietojuma sūtījumiem

2021. gada atļauju apstiprināšanas procesā Federālā kodolenerģijas regulēšanas iestāde (FANR) konstatēja aizdomīgu sūtījumu, kurā bija divējāda lietojuma preces. Uzņēmums X, kas atrodas AAE brīvajā zonā, bija iesniedzis trīs atļaujas eksportēt invertorus aptuveni 25 000 ASV dolāru (95 040 AED) vērtībā. Invertori bija iekļauti AAE eksporta kontroles sarakstā un klasificēti kā divējāda lietojuma preces. Uzņēmuma X iesniegtajos dokumentos bija konosaments un pirkšanas un pārdošanas pavadzīme (PPPZ), kurā bija pretrunīga informācija par pārdevēja datiem un sūtījuma izcelsmes valsti. Dokumentos bija norādīts, ka šīs preces ir paredzētas augsta riska valstij.

Tiesībaizsardzības iestāžu izmeklēšanā tika konstatēts, ka uzņēmums X iesniedza viltotu konosamentu, kurā sevi deklarēja kā kravas nosūtītāju, bet PPPZ identificēja pārdevēju kā citu uzņēmumu, kas atrodas valstī T. Pēc papildu izmeklēšanas tiesībaizsardzības iestādes arī konstatēja, ka iespējamais pārdevējs galvenokārt tirgo riekstus un tādējādi tā uzņēmējdarbība neatbilst tirdzniecības darījumam. Turpmākā izmeklēšanā atklājās, ka pārdevējs faktiski importēja preces no valsts H uz AAE. Uzņēmums X iesniedza arī viltotus dokumentus par to, ka tam ir vairākas filiāles valstī U, lai maldinātu iestādes un izvairītos no sankcijām, kas noteiktas saistībā ar Irānas kodolprogrammu.

Tiesībaizsardzības iestādes veica kriminālizmeklēšanu un finanšu izmeklēšanu sadarbībā ar UAEFIU, CBUAE, EOCN, Federālo muitas iestādi un FANR. Veicot fizisku pārbaudi uzņēmuma X telpās, tika konstatēts, ka tas darbojas kā invertoru pircēja aizsegs, kas atrodas augsta riska valstī. UAEFIU un CBUAE identificēja un iesaldēja trīs bankas kontus ar kopējo atlikumu 34 000 AED (9500 USD) apmērā, kas saistīti ar uzņēmumu X. Turklāt muita sniedza tiesībaizsardzības iestādēm visus identificētos viltotos dokumentus, kas saistīti ar apakšuzņēmējiem, kuri mēģina slēpt patieso labuma guvēju.

FANR ir sagatavojis tehnisku ziņojumu par sūtījumu un sniedzis tiesībaizsardzības iestādēm apstiprinājumu, ka prece ir divējāda lietojuma prece, kas iekļauta AAE eksporta kontroles sarakstā. Muitas iestādes apķīlāja sūtījumu, un tiesībaizsardzības iestādes lika iesaldēt sūtījumu (95 040 AED (26 000 USD)).

Avots: Apvienotie Arābu Emirāti

34. ierāmējums. Gadījuma izpēte: divējāda lietojuma preču nedeklarēšana saskaņā ar eksportētājvalsts noteiktajiem eksporta tiesību aktiem

2020. gadā Indijas muitas iestādes arestēja kuģi, kas kuģoja ar Āzijas karogu un devās uz Pakistānu. Izmeklēšanas laikā Indijas iestādes apstiprināja, ka dokumentos nepareizi deklarētas sūtījumā esošās divējāda lietojuma preces. Indijas izmeklētāji apstiprināja, ka sūtījumam paredzētās preces ir "autoklāvs", ko izmanto jutīgiem augstas enerģijas materiāliem un raķešu dzinēju izolācijai un ķīmiskajam pārklājumam. Šīs sensitīvās preces ir iekļautas Raķešu tehnoloģiju kontroles režīma, Indijas un citu jurisdikciju divējāda lietojuma preču eksporta kontroles sarakstos.[56]

Apķīlātās kravas pavadzīme liecināja par importētāja saistību ar Nacionālo attīstības kompleksu, kas nodarbojas ar tāla darbības rādiusa ballistisko raķešu izstrādi.

Avots: Indija

[56] Šādu iekārtu eksports bez oficiāla dažādu iestāžu apstiprinājuma ir spēkā esošo tiesību aktu un līgumu pārkāpums.

5. 3. sadaļa. Ar PF saistīto risku mazināšanas grūtības un labā prakse

Atklāšana, izmantojot SAR/STR un sankciju skrīningu

96. Lai atklātu PF un sankciju apiešanas metodes, valstis lielā mērā paļaujas uz SAR/STR sniegšanas pienākumiem un stingrām sankciju pārbaudes atbilstības pārbaudēm. Lai papildinātu šos paņēmienus un efektīvi identificētu un novērstu nelikumīgas darbības globālā mērogā, citas atklāšanas metodes ietver pārrobežu izlūkdatu savstarpējo atklāšanu, koordināciju starp aģentūrām, starptautisko sadarbību un uzraudzības rīkus, tostarp atklāto datu un blokķēdes analīzi.

97. Daudzas valstis ziņoja, ka tās paļaujas uz stingriem SAR/STR pienākumiem, lai atklātu PF un sankciju apiešanas shēmas, tādējādi identificējot un apkarojot sarežģītas un mainīgas taktikas. Atšķirīgs iekšzemes tiesiskais regulējums un ziņošanas pienākumi var noteikt ziņotājiem pienākumu iesniegt SAR/STR saistībā ar PF un sankciju apiešanu plašākā nozīmē. Vairākas valstis norāda, ka ziņotāju pienākumu apjoms var ietvert rūpīgas klienta uzticamības pārbaudes veikšanu, normatīvo aktu noteikumu ievērošanu, tādu darījumu uzraudzību, kuros iesaistītas augsta riska valstis, un visu SAR/STR pienākumu izpildi, ja tiek konstatēti aizdomīgi darījumi.

Labā prakse PF un sankciju apiešanas atklāšanā, izmantojot SAR/STR un sankciju skrīningu

98. Turklāt vairākas valstis pieprasa, lai ziņotāji integrētu automatizētās sankciju pārbaudes sistēmas ziņotāju iestāžu pienākumos, tostarp saistībā ar iekšējo politiku un procedūrām, lai uzlabotu SAR/STR efektivitāti. Starptautisko un/vai valstu sankciju saraksti ir integrēti sankciju pārbaudes sistēmās, ar kuru palīdzību ziņotāji var atrast atbilstību personām vai struktūrām un izmantot atslēgvārdus, kas attiecas uz augsta riska darījumiem un personām, struktūrām vai darbībām, uz kurām attiecas sankcijas. Dažās valstīs pārbaudes laikā konstatēta pozitīva sakritība var radīt turpmākus pienākumus ziņotāju iestādēm iesniegt SAR/STR un informēt varas iestādes par iesaldētajiem aktīviem, uz kuriem attiecas sankcijas, vai darījumiem, kas saistīti ar struktūrām, uz kurām attiecas sankcijas. Turpmākajos divos piemēros parādīts, kā SAR/STR tika izmantoti, lai uzsāktu izmeklēšanu.

35. ierāmējums. Gadījuma izpēte: negatīvo ziņu pārbaude un SAR/STR atklāj divējāda lietojuma preču nelikumīgu iegādi

Divi Francijas uzņēmumi rīkojās kā starpnieki, lai iegādātos ASV izcelsmes divējāda lietojuma elektroniskās komponentes, kas ar vairāku struktūru starpniecību tika tālāk pārdotas ASV sankcijām pakļautam uzņēmumam Krievijā.

Šis gadījums tika atklāts, Francijas iestādēm sadarbojoties ar privāto sektoru, izmantojot ar Krieviju saistīto negatīvo ziņu (publiskās informācijas skrīnings noziegumu identificēšanai) un banku SAR/STR uzraudzību pēc tam, kad TracFin izdeva "aicinājumu būt modriem", kas bija vērsts pret attiecīgo personu un uzņēmumiem (uzņēmumu patiesajiem labuma guvējiem). TracFin publikācijā arī norādīts uz personas sievu, kura tika iecelta par viena uzņēmuma vadītāju mazāk nekā mēnesi pirms viņas vīrs tika iekļauts OFAC SDN sarakstā.

Izmeklēšanai bija nepieciešama cieša sadarbība starp aģentūrām un veiksmīga partnerība ar finanšu iestādēm, tostarp regulāra sadarbība ar iesaistītajām bankām, lai novērstu kapitāla aizplūšanu un nodrošinātu, ka izmeklēšanas laikā esošais finansējums faktiski nav pieejams.

Avots: Francija

99. Vairākas valstis ir ieguldījušas līdzekļus apmācībā, informēšanā, specializētās vadlīnijās un uzraudzības mehānismos, izmantojot valsts un privātā sektora partnerības, lai stiprinātu atbilstību un uzlabotu atklāšanas spējas. Šajā nolūkā ieteikumu, norādījumu vai valsts vai starptautiski noteiktu indikatoru publicēšana var palīdzēt ziņotāju struktūrām atklāt aizdomas par sankciju apiešanu un PF darbību un iesniegt īpašus SAR/STR, lai izpildītu savus pienākumus. Dažas valstis ir ieviesušas arī iekšzemes tiesisko regulējumu, kas pieprasa, lai regulētās struktūras, pamatojoties uz šiem ieteikumiem vai brīdinājumiem, iesniegtu SAR/STR, tādējādi vēl vairāk uzlabojot atklāšanas iespējas.

36. ierāmējums. Gadījuma izpēte: detalizētu brīdinājumu izdošana, lai FI būtu vieglāk iesniegt SAR/STR

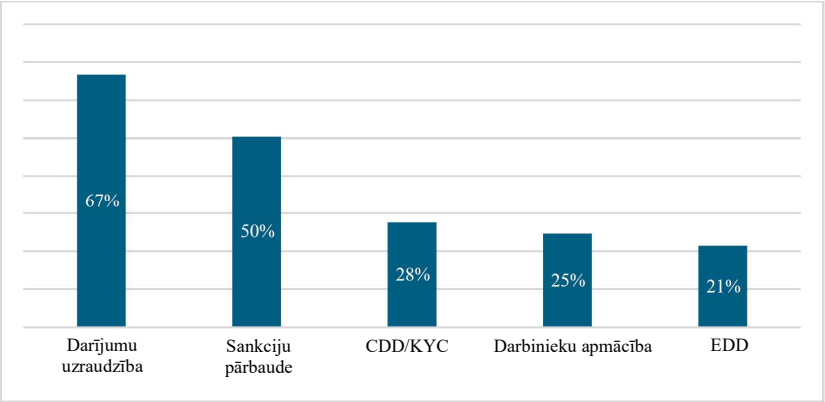
Lai finanšu iestādēm atvieglotu SAR/STR iesniegšanu saistībā ar izvairīšanos no ASV eksporta kontroles attiecībā uz Krieviju un Baltkrieviju, BIS un FinCEN izdeva 2022. gada kopīgu brīdinājumu, kurā finanšu iestādēm tika sniegts pārskats par BIS spēkā esošajiem eksporta ierobežojumiem; to preču saraksts, kas rada bažas par iespējamu izvairīšanos no eksporta kontroles; kā arī atsevišķi apdraudējuma signāli par darījumiem un uzvedību, lai palīdzētu finanšu iestādēm identificēt aizdomīgus darījumus saistībā ar iespējamu izvairīšanos no eksporta kontroles. Brīdinājumā arī tika pieprasīts, lai FI, iesniedzot SAR/STR, lietotu atslēgas terminu "FIN-2022-RUSSIABIS".

Pamatojoties uz šo brīdinājumu, BIS un FinCEN 2023. gada novembrī izdeva kopīgu brīdinājumu, kurā uzsvēra apdraudējuma signālus saistībā ar globālu izvairīšanos no eksporta kontroles. Šajā brīdinājumā tika pieprasīts, lai FI, iesniedzot SAR/STR, izmantotu atslēgas terminu "FIN-2023-GLOBALEXPORT". FI ir iesniegušas vairāk SAR/STR ar atslēgas terminu, kas attiecas uz Krieviju, nekā ar globālo eksporta atslēgas terminu, galvenokārt tāpēc, ka Krievijai un Baltkrievijai noteiktie eksporta ierobežojumi ir plašāki un FI ir vieglāk identificēt potenciāli saistītus finanšu darījumus saņemtajā informācijā.

Avots: Amerikas Savienotās Valstis

100. Lielākā daļa privātā sektora uzņēmumu, kas piedalījās FATF publiskajā apspriešanā, uzskata, ka labākie veidi, kā mazināt risku, kas saistīts ar izvairīšanos no sankciju piemērošanas un PF, ir saistīti ar galvenajiem preventīvajiem AML/CFT pasākumiem, piemēram, klienta uzticamības pārbaudi, visaptverošu risku novērtējumu, sankciju pārbaudes rīkiem, pastāvīgu uzraudzību, kas var novest pie SAR/STR iesniegšanas, darbinieku apmācību, politiku un procedūrām, negatīvu ziņu pārbaudi un padziļināto uzticamības pārbaudi (skatīt 3. attēlu, kurā norādīta labā prakse, ko visvairāk min privātā sektora pārstāvji). Kā svarīgi tika minēti arī uz tirdzniecību balstīti nelikumīgi iegūtu līdzekļu legalizēšanas novēršanas pasākumi, reāllaika brīdinājumi un mūsdienīgi tehnoloģiju risinājumi. Tomēr, ja nav stabilu informācijas apmaiņas mehānismu, privātajam sektoram var būt grūti atklāt sarežģītas PF un sankciju apiešanas shēmas, izmantojot standarta riska pārvaldības procesus.

3. attēls. Laba prakse, kā atklāt izvairīšanos no sankciju piemērošanas



PF un sankciju apiešanas atklāšanas problēmas, izmantojot SAR/STR un sankciju skrīningu

101. Gandrīz trešdaļa valstu nav ziņojušas par SAR/STR izmantošanu kā PF atklāšanas metodi. Tā kā ievērojams skaits valstu PF nav krimināli sodāma, tas var izskaidrot, kāpēc dažas valstis zināmā mērā nepaļaujas uz SAR/STR. Valstīs, kurās PF netiek uzskatīta par noziedzīgu nodarījumu, ir mazāka iespējamība, ka ziņotāju iestādēm SAR/STR būs jāpieprasa identificēt PF. Savukārt ziņotāji var iesniegt SAR/STR, kuros iesaistīti PF dalībnieki, bet būtiska informācija, kas tos saista ar PF darbībām, var nebūt pieejama, ja netiks sniegti papildu norādījumi par šīs nelikumīgās darbības atklāšanas sarežģītību.

102. Arī sankciju sarakstu iekļaušanai valstu SAR/STR sistēmās un pārbaudes rīku izmantošanai var būt būtiska nozīme aizdomu par PF un sankciju apiešanu atklāšanā. Dažas valstis norādīja uz problēmām, kas saistītas ar sankciju skrīninga sakritību pārbaudēm, jo tās saskārās ar viltus pozitīviem personu/subjektu sakritības gadījumiem vai neatbilstošu informāciju, pamatojoties uz vispārīgiem atslēgvārdu meklējumiem. Turklāt, tā kā ir jāsalīdzina vairāki identifikatori, tostarp dzimšanas datumi, vārdi, aizstājvārdi, vairākas vārdu versijas, vārdu fonētiskās un rakstības atšķirības un pasu numuri, atbilstības algoritmi var būt pakļauti viltus pozitīvu rezultātu atklāšanai. Tomēr riska mazināšanas pasākumi var ietvert EDD, atklāto datu analīzi, izmantojot, piemēram, uzņēmumu reģistru vai BOI, un informācijas apstiprināšanu ar citām datubāzēm.

103. Valstis ziņoja par vēl vienu problēmu, kas saistīta ar to, ka izraudzītie nefinanšu uzņēmumi un profesionāļi (DNFBP) slikti izprot un ievēro PF pienākumus. Daudzas DNFBP struktūras nezina par saviem pienākumiem uzraudzīt un ziņot par darbībām, kas saistītas ar PF.[57] Dažās valstīs tas var apgrūtināt iestādēm atklāt PF darbības nozarēs, kas nav finanšu iestādes. Tomēr privātā sektora struktūras visās nozarēs ziņoja, ka valsts sektoram trūkst atgriezeniskās saites par attiecīgajiem SAR/STR, kas var apgrūtināt šīs problēmas risināšanu.

[57] Plašāku informāciju par riska mazināšanas pasākumiem, ko veic FI, DNFBP un VASP, skatīt 2021. gada FATF PF vadlīniju otrajā sadaļā "PF risku mazināšana".

Citas noteikšanas metodes

104. Lai papildinātu SAR/STR un sankciju skrīninga sakritību, citas atklāšanas metodes ietver pārrobežu izlūkdatus, informācijas apmaiņu, izmantojot starpinstitūciju koordināciju un starptautisko sadarbību, kā arī uzraudzības rīkus. Ir svarīgi atzīmēt, ka valstis bieži vien integrē vairākus atklāšanas avotus, lai veidotu visaptverošu priekšstatu par nelikumīgu finansējumu un izvairīšanās shēmām.

105. Daudzas valstis ziņo, ka muitas iestādēm un pārrobežu izlūkošanai ir būtiska nozīme ar PF saistītu darbību atklāšanā un izmeklēšanā, jo īpaši attiecībā uz saikni ar augsta riska valstīm un tirdzniecības maršrutiem. Muitas aģentūras sadarbojas ar reģionālām un starptautiskām iestādēm un var savstarpēji atklāt informāciju par izmeklēšanu, muitas deklarācijām, importa/eksporta datiem un licencēšanas pieteikumiem, lai labāk atklātu un izmeklētu iespējamos pārkāpumus, kas saistīti ar sankciju apiešanu no proliferācijas finansētājiem. Šī informācijas apmaiņa uzlabo atklāšanas iespējas un palīdz izmeklēt iespējamos pārkāpumus. Konkrēti, galvenie pasākumi šajā jomā ietver ārējās tirdzniecības operāciju un preču aprites analīzi un uzraudzību, tostarp uzraugot aktīvu plūsmu uz augsta riska valstīm, aizsardzības materiālus, stratēģiskas un divējāda lietojuma preces. Izlūkdatu atklāšana apvienojumā ar jurisdikciju regulējošiem noteikumiem atbilstības nodrošināšanai uzsver muitas iestāžu izšķirošo nozīmi, lai atklātu iespējamos pārkāpumus, kas saistīti ar PF un izvairīšanos no sankcijām.

PF un sankciju apiešanas atklāšanas labā prakse, izmantojot citus atklāšanas pasākumus

Starpaģentūru koordinācija

106. Lielākā daļa valstu uzsvēra, cik svarīga ir starpaģentūru koordinācija PF un sankciju apiešanas atklāšanā. Konkrēti, tiesībaizsardzības iestāžu izmeklēšana un informācijas apmaiņa ar citām kompetentajām iestādēm var novest pie vietējo aģentūru lietu pārsūtīšanas, kopīgas izmeklēšanas un informētības palielināšanas, kas var palīdzēt identificēt norādīto personu un uzņēmumu līdzekļu un/vai aktīvu finanšu plūsmu. Izlūkdatu vākšana, ko papildina izmeklēšanas darbs, ir daudzdisciplīnu pieeja, lai identificētu un atklātu iespējamos PF un sankciju apiešanas gadījumus.

37. ierāmējums. Gadījuma izpēte: starpaģentūru koordinācija attiecībā uz kontrolētu divējāda lietojuma preču eksportu

2017. gadā FINTRAC saņēma brīvprātīgi sniegtu informāciju no Kanādas tiesībaizsardzības iestādēm, kas liecināja, ka Kanādas elektronikas uzņēmums tiek turēts aizdomās par iesaistīšanos kontrolētu divējāda lietojuma mikroshēmu sūtījumos.

SAR/STR norādīja, ka uzņēmuma darījumi atbilst dažām galvenajām pazīmēm, kas raksturo Krievijas un Austrumeiropas noziedzīgi iegūtu līdzekļu legalizēšanas shēmas. Kā norādīja viens SAR/STR:

- Līdzekļi nāk no augsta ranga personām;
- Personas, kas atrodas tādās valstīs kā Krievija, Azerbaidžāna, kā arī citās Austrumeiropas valstīs;
- Augsta ranga personas atvēra čaulas uzņēmumus, lai legalizētu noziedzīgi iegūtus līdzekļus;
- Nodokļu oāžu valstīs reģistrēti čaulas uzņēmumi;
- Līdzekļi, kas pārskaitīti, izmantojot čaulas uzņēmumus nodokļu oāžu valstīs.
- Uzņēmums saņēma elektroniskos naudas pārskaitījumus no iespējamām starpniekvalstīm divējāda lietojuma preču pārkraušanai vai citām nelikumīgām finanšu darbībām (tostarp no vairākām Eiropas valstīm). Dažos gadījumos izcelsmes valsts nesakrita ar to uzņēmumu norādīto adresi, kuri bija atbildīgi par elektronisko naudas līdzekļu pārskaitījumu pasūtīšanu. Turklāt uzņēmums bija saņēmējs elektroniskajiem naudas pārskaitījumiem, kurus bija pasūtījušas fiziskas un juridiskas personas ar Krievijā norādītām adresēm.

SAR/STR norādīja, ka uzņēmuma līdzekļi tika izsmelti, izmantojot daudzus akcionāriem adresētus izejošos čekus un izejošos elektroniskos naudas pārskaitījumus tiešsaistes maksājumu apstrādes uzņēmumam.

Vaicāti par FINTRAC izpaustās izlūkdienestu informācijas ietekmi uz uzņēmumu, Kanādas tiesībaizsardzības iestādes norādīja, ka izpaustā informācija izraisīja jaunu izmeklēšanu un sniedza tām papildu un nezināmus subjektus. Viņi norādīja, ka FINTRAC atklātā informācija un sadarbība bija galvenie faktori, kas palīdzēja izprast iesaistītos tīklus un gūtu vispārējus izpildes panākumus viņu lietās. Viņi piebilda, ka FINTRAC sniegtā informācija palīdzēja partnervalstī izvirzīt oficiālas apsūdzības.

Avots: Kanāda

107. Turklāt dažas valstis uzsvēra, ka aizdomīgu darbību atklāšanā būtiska nozīme ir vadlīniju publicēšanai, kas var ietvert tendences, tipoloģiju un rādītājus (skatīt sadaļu par koordināciju un sadarbību iekšzemē).

Starptautiskā sadarbība

108. Ņemot vērā PF un sankciju apiešanas globālo raksturu, starptautiska sadarbība, izmantojot izlūkdatus un informācijas apmaiņu, ir galvenais atklāšanas un novēršanas instruments. Lai veiktu efektīvus atklāšanas pasākumus, ir nepieciešama koordinēta pieeja starp vietējām iestādēm un starptautiskajiem partneriem. Piemēram, FID var turpināt informācijas apmaiņu, izmantojot Finanšu izlūkošanas vienības apvienojošo grupu (Egmont Group), kurai ir būtiska loma informācijas apmaiņas veicināšanā starp FID, tādējādi sekmējot aizdomīgu finanšu darbību atklāšanu saistībā ar PF vai sankcijām. Turklāt starptautiskā sadarbība var palīdzēt valstīm sistemātiski analizēt riskus, kas saistīti ar starptautisko tirdzniecības apriti, kas var palīdzēt stiprināt valstu riska profilus.

Commented [LŽ6]: https://fid.gov.lv/uploads/files/Dokumenti/Vadl%C4%ABnijas%2C%20rekomend%C4%81cijas/FIU_Operational_Independence_and_Autonomy_LV_FINAL.pdf

Uzraudzības rīki

109. Uzraudzības rīkiem ir svarīga loma arī PF un sankciju apiešanas atklāšanā. Šie rīki izmanto dažādus datu avotus, tostarp atklāto datu analīzi un sarežģītas blokķēdes analīzes metodes. Kompetentās iestādes var izmantot atklāto datu analīzi, lai piekļūtu plašam informācijas klāstam, kas var ietvert korporatīvos reģistrus, informāciju par faktiskajiem īpašniekiem, satelītattēlus un ģeotelpiskos datus, kas var atklāt neatļautu darbību dalībnieku tīklus.

110. Vairākas valstis arī norādīja, ka blokķēdes analīzes rīki palīdz atklāt izvairīšanos no sankcijām un PF darbību. Virtuālo aktīvu izmantošana var radīt papildu sarežģījumu atklāšanā, taču darījumus ar virtuālajiem aktīviem, kas darbojas publiskās blokķēdēs, var izsekot. Blokķēdes analīze ļauj kompetentajām iestādēm uzraudzīt un izsekot līdzekļu plūsmai, identificēt aizdomīgas darbības un mazināt dažus virtuālo aktīvu slēpšanas centienus. Lai iegūtu vairāk informācijas, lūdzu, skatiet 3. tipoloģiju (Virtuālo aktīvu un citu tehnoloģiju izmantošana).

PF un sankciju apiešanas atklāšanas problēmas, izmantojot citus atklāšanas pasākumus

111. Valstis ziņoja par vairākām problēmām, kas saistītas ar atklāšanu, tostarp sankciju programmu atšķirībām starp jurisdikcijām un ar tām saistītajiem atšķirīgajiem sankciju subjektu sarakstiem, valstu juridiskajām prasībām un dažādiem izpildes noteikumiem. Vēl viena būtiska problēma ir tā, ka KTDR izmanto diplomātisko personālu, lai atvieglotu finanšu pakalpojumu sniegšanu vai sankcijām pakļautu aktīvu vai resursu nodošanu, tostarp skaidras naudas pārvadāšanu. KTDR paļaujas uz diplomātisko imunitāti, lai izvairītos no kontroles un izmeklēšanas pasākumiem. Daudzas valstis ir nobažījušās par nekonsekventu patiesā labuma guvēju informācijas vākšanu un/vai pieejamību, kas vēl vairāk apgrūtina PF un sankciju apiešanas atklāšanu (plašāku informāciju skatīt 2. tipoloģijā un sadaļā par ievainojamībām).

Izmeklēšana un kriminālvajāšana

112. Kopš FATF publicēja ziņojumu "*PF apkarošana: ziņojums par politikas izstrādi un konsultācijām*"[58] 2010. gadā, tiesiskais regulējums PF un sankciju apiešanas novēršanai un apkarošanai, iespējams, ir ievērojami nostiprināts, taču efektīvas izmeklēšanas un kriminālvajāšanas piemēru 2025. gadā joprojām trūkst. Kā aprakstīts FATF 2010. gada ziņojumā, grūtības PF lietu kriminālvajāšanā tika skaidrotas ar vairākām problēmām, tostarp ar to, ka PF nav krimināli sodāma; ar pierādījumu vākšanu PF lietās; PF darbību starptautisko raksturu; finanšu starpnieku izmantošanu, lai maskētu nelikumīgas darbības; neefektīvu eksporta kontroles sistēmu; vispārēji pieņemtas WMD PF definīcijas trūkumu; un atšķirīgām jurisdikciju pieejām šim jautājumam, tostarp starptautiskai sadarbībai. Pamatojoties uz FATF Globālā tīkla iesniegto informāciju, šķiet, ka daudzas no tām pašām galvenajām problēmām joprojām kavē sekmīgu izmeklēšanu un kriminālvajāšanu sarežģītās PF (un sankciju apiešanas) lietās.

[58] PROLIFERĀCIJAS FINANSĒŠANAS APKAROŠANA

Izmeklēšanas metodes un mehānismi

PF izmeklēšanas labā prakse

113. Daudzas valstis ziņoja, ka efektīva PF un sankciju apiešanas izmeklēšana ir atkarīga no standarta procedūru izmantošanas finanšu noziegumu lietās un sadarbības, iesaistot attiecīgos starpaģentūru partnerus. SAR/STR ir galvenais ieguldījums, lai noteiktu un izprastu neparastus finanšu darbību modeļus. SAR/STR izmantošana palīdz arī atklāt saiknes starp uzņēmumiem un personām, kas iesaistītas sankciju apiešanā un nelikumīgās darbībās.

114. Dažas valstis ziņoja, ka vēl viens svarīgs izmeklēšanas rīks ir virtuālo līdzekļu izsekošana, kurus dažkārt izmanto, lai izvairītos no atklāšanas. Izmeklētāji, izmantojot blokķēdes analīzi, var izsekot naudas plūsmu, pat ja summas ir nelielas, atklājot finanšu modeļus un saikni ar attiecīgajām struktūrām un personām.

115. Padziļinātai analīzei ir svarīga loma PF apkarošanā, jo tā palīdz atrast finanšu datu modeļus un neparastas darbības. Šie rīki var palīdzēt izmeklētājiem atklāt saiknes starp personām un identificēt sankciju apiešanā iesaistīto personu vai uzņēmumu tīklus. Piemēram, padziļinātā analītika nodrošina savstarpējo saikņu analīzes atbalstu, kas ļauj konstatēt saistību starp kontiem, darījumiem un pusēm, lai parādītu, kā darbojas nelegālie tīkli. Reāllaika uzraudzības rīki ļauj iestādēm ātri rīkoties, ja tiek konstatētas aizdomīgas darbības. Apkopojot datus no dažādiem avotiem, piemēram, finanšu iestādēm, muitas reģistriem un izlūkošanas ziņojumiem, izmeklēšana kļūst efektīvāka un pilnīgāka. Ar šiem rīkiem var arī identificēt neparastus darījumu modeļus vai noteikt, kad tiek izmantotas privātumu uzlabojošas tehnoloģijas, lai slēptu līdzekļu izcelsmi. Ja šo informāciju savstarpēji atklāj aģentūras, rīki kļūst vēl efektīvāki PF apkarošanā.

116. Dažas valstis ziņoja par to, cik svarīgi ir apsvērt tādu pašu taktiku, kādu izmanto starptautisku kriminālu organizāciju un narkotiku kontrabandistu izmeklēšanā, piemēram, slepeno aģentu un konfidenciālu avotu izmantošanu.

38. ierāmējums. Gadījuma izpēte: slepeno aģentu un konfidenciālu avotu izmantošana pret kodolmateriālu kontrabandistiem

2024. gada 21. februārī Amerikas Savienoto Valstu Tieslietu departaments (DOJ) un ASV Narkotiku apkarošanas pārvalde (DEA) paziņoja par papildinoša apsūdzības raksta izdošanu, kurā apsūdzētais apsūdzēts sazvērestībā ar līdzdalībnieku tīklu, lai pārvadātu kodolmateriālus no Mjanmas uz citām valstīm. Šīs sazvērestības laikā apsūdzētais un viņa līdzdalībnieki parādīja kodolmateriālu paraugus Taizemē DEA slepenajam aģentam ("UC-1"), kurš uzdevās par narkotiku un ieroču tirgotāju. Ar Taizemes iestāžu palīdzību kodolmateriālu paraugi tika konfiscēti un pēc tam nodoti ASV tiesībaizsardzības iestāžu uzraudzībā. ASV kodolenerģētikas ekspertīžu laboratorija vēlāk analizēja paraugus un apstiprināja, ka paraugi satur urānu un ieroču klases plutoniju.

Apsūdzētajam un viņa līdzapsūdzētajam 2022. gada aprīlī tika izvirzītas apsūdzības par starptautisku narkotiku tirdzniecību un šaujamieroču noziegumiem, un abiem tika piemērots apcietinājums.

Saskaņā ar apsūdzību papildinošajā apsūdzības rakstā ietvertajiem apgalvojumiem, sākot ar 2020. gada sākumu, apsūdzētais informēja UC-1 un DEA konfidenciālo avotu ("CS-1"), ka apsūdzētajam ir pieejams liels daudzums kodolmateriālu, kurus viņš vēlas pārdot. Vēlāk tajā pašā gadā apsūdzētais nosūtīja UC-1 virkni fotogrāfiju, kurās bija attēlotas iežiem līdzīgas vielas ar Geigera skaitītājiem, kas mēra radiāciju, kā arī lapas, ko apsūdzētais uzdeva kā laboratorijas analīzes, kas liecināja par torija un urāna klātbūtni attēlotajās vielās. Atbildot uz atkārtotiem apsūdzētā pieprasījumiem, UC-1 piekrita DEA izmeklēšanas ietvaros palīdzēt apsūdzētajam būt par starpnieku viņa kodolmateriālu pārdošanā UC-1 sabiedrotajam, kurš uzdevās par Irānas ģenerāli ("Ģenerālis"), lai tos izmantotu kodolieroču programmā. Pēc tam apsūdzētais piedāvāja Ģenerālim piegādāt "plutoniju", kas šim nolūkam būtu vēl "labāks" un "jaudīgāks" nekā urāns.

Sarunu laikā par apsūdzētā piekļuvi kodolmateriāliem apsūdzētais arī sazinājās ar UC-1 par viņa vēlmi iegādāties militārus ieročus. Šajā nolūkā 2021. gada maijā apsūdzētais nosūtīja UC-1 sarakstu ar ieročiem, tostarp zeme-gaiss raķetēm, ko viņš vēlējās iegādāties no UC-1 Mjanmas etnisko nemiernieku grupas ("CC-1") līdera vārdā. Kopā ar diviem citiem līdzdalībniekiem ("CC-2" un "CC-3") apsūdzētais ierosināja UC-1, ka CC-1 ar apsūdzētā starpniecību pārdos urānu Ģenerālim, lai finansētu CC-1 ieroču iegādi.

2025. gada 8. janvārī apsūdzētais atzina savu vainu sazvērestībā par kodolmateriālu, tostarp urāna un ieroču kvalitātes plutonija, pārvadāšanu no Mjanmas uz citām valstīm, kā arī par starptautisku narkotiku kontrabandu un ieroču kontrabandu.

Avots: Amerikas Savienotās Valstis

117. Visbeidzot, daudzas valstis uzsvēra, cik svarīga ir starpaģentūru sadarbība regulārās sanāksmēs, tostarp izveidojot specializētas darba grupas un ekspertu darba grupas. Ja finanšu iestādes, muitas iestādes un tiesībaizsardzības iestādes sadarbojas, tās var uzlabot izmeklēšanu un proaktīvi panākt aktīvu iesaldēšanu un tādu sūtījumu apturēšanu, kas saistīti ar PF un izvairīšanos no sankcijām.

39. ierāmējums. Jurisdikcijas piemēri: specializētas operatīvās un darba grupas, lai apkarotu PF un izvairīšanos no sankcijām

- **Francija**: TracFin (finanšu izlūkošanas dienests) vadītā specializētā darba grupa izmeklēja divus uzņēmumus (uzņēmums A1 un A2), kas piegādāja elektroniskas detaļas sankcijām pakļautam Krievijas uzņēmumam. Šie uzņēmumi rīkojās kā starpnieki, iepērkot komponentus un nododot tos sankcijām pakļautajām grupām ar cita uzņēmuma starpniecību trešajā valstī. Darba grupā strādāja TracFin, finanšu iestādes un tiesībaizsardzības iestādes. Tās analizēja banku iesniegtos SAR/STR, uzraudzīja uzņēmumu finanšu plūsmas un patieso labuma guvēju iesaisti. Koordinēto centienu rezultātā tika iesaldēti uzņēmumu aktīvi un apturēta to darbība.
- **Indonēzija**: darba grupa izmeklēja sauskravu kuģi Petrel 8, kas bija iesaistīts ogļu transportēšanā uz KTDR, pārkāpjot ANO sankcijas. Darba grupas sastāvā bija Ārlietu ministrija, muitas iestādes un Finanšu izlūkošanas dienests (PPATK). Apvienojot finanšu izlūkošanas datus un kuģošanas datus, tika noskaidrots, ka kuģis pieder Indonēzijas uzņēmumam un ka tam jau iepriekš ir piemērotas sankcijas par līdzīgām darbībām. Darba grupa koordinēja savu darbību ar ANO Sankciju komiteju, kā rezultātā kuģis tika aizturēts un pēc tam demontēts.

Avoti: Francija un Indonēzija

Izaicinājumi PF izmeklēšanas veikšanā

118. Kopumā PF izmeklēšana daudzējādā ziņā atšķiras no nelikumīgi iegūtu līdzekļu legalizēšanas (ML) un terorisma finansēšanas (TF) izmeklēšanas. PF koncentrējas uz tādu pasākumu finansēšanu, kas palīdz atbalstīt WMD programmas. Lai izvairītos no sankcijām, bieži vien tiek iesaistīti ietekmīgi valsts dalībnieki vai grupas, kas izmanto fiktīvus uzņēmumus, tirdzniecību un sarežģītas īpašumtiesību struktūras. Atšķirībā no ML, kas slēpj nelegālās naudas izcelsmi, un TF, kas finansē terorismu, PF izmeklēšana vairāk balstās uz izlūkdatiem par iespējamiem eksporta kontroles un sankciju pārkāpumiem. PF var būt grūtāk izmeklēt, jo ir mazāka izpratne par tā riskiem un bieži vien tas ir saistīts ar legālu preču (tostarp kontrolētu preču) izmantošanu nelegāliem mērķiem. Izmeklētājiem ir vajadzīga ciešāka sadarbība gan vietējā, gan starptautiskā līmenī, kā arī progresīvi analītiskie rīki, lai risinātu PF lietas, kas var būt sarežģītākas nekā tās, kas parasti nepieciešamas ML vai TF lietās.

119. Daudzas valstis ziņoja, ka saskaras ar līdzīgām problēmām, tostarp PF shēmām, kurās izmanto fiktīvus uzņēmumus, īpašumtiesību daudzslāņainību un mazus, bet biežus darījumus. Šāda taktika ļoti apgrūtina attiecīgo ieinteresēto personu, tostarp tiesībaizsardzības iestāžu, regulatoru, finanšu iestāžu, FID un prokuroru, darbību, kas paļaujas uz precīziem datiem un ciešu sadarbību, lai izsekotu faktiskos īpašniekus vai sarežģītās shēmās iesaistītās organizācijas (skatīt 2. tipoloģiju).

120. Vēl viena problēma ir nepietiekama informētība par PF riskiem, tendencēm un metodēm finanšu iestādēs un citās regulētajās struktūrās, tostarp nepietiekama apmācība par PF riskiem, lai uzlabotu SAR/STR kvalitāti. Kā minēts šā ziņojuma iepriekšējā nodaļā, daudzās valstīs PF nav krimināli sodāma. Daļēji tas var izskaidrot trūkumus, kas saistīti ar attiecīgo SAR/STR skaitu un kvalitāti.

121. Plašākā nozīmē daudzās valstīs problēmas rada arī ierobežotie valsts iestāžu un privātā sektora struktūru resursi. Īpaši mazām valstīm var nepietikt finansējums vai speciālās zināšanas, lai izskatītu sarežģītas lietas. Tā varētu būt arī prioritāšu noteikšanas problēma, kas izpaužas resursu sadalē valsts un privātajā sektorā. Lai gan dažas valstis var būt noteikušas primāru noziedzīgu nodarījumu, kas ietver PF, vai arī izmanto palīgnoziegumus, lai sauktu pie atbildības par PF darbībām, tas, ka nav valstu ar konsekventu pieeju kriminālatbildības noteikšanai, var traucēt starptautisko sadarbību ar PF saistītu lietu izmeklēšanā un kriminālvajāšanā.

122. Visbeidzot, pārrobežu lietās ir nepieciešama sadarbība ar citām valstīm, taču juridisko sistēmu atšķirības, piemēram, atšķirīgi noteikumi par to, kas ir pieņemami pierādījumi, atšķirīgas finanšu noziegumu definīcijas un abpusējas sodāmības neesamība, rada problēmas pārrobežu izmeklēšanā. Ja starp valstīm nav noslēgti nolīgumi par informācijas apmaiņu, var ievērojami aizkavēties vai var tikt noraidīti izmeklēšanas informācijas pieprasījumi (skatīt sadaļu "Starptautiskā sadarbība").

Kriminālvajāšana un citas metodes

PF kriminālvajāšanas labā prakse

123. Daudzas valstis ziņoja, ka kriminālvajāšana sarežģītās PF un sankciju apiešanas lietās ir vēl sarežģītāka nekā to izmeklēšana. Veiksmīgai kriminālvajāšanai PF un sankciju apiešanas lietās ir nepieciešams stingrs tiesiskais regulējums, tostarp skaidri tiesību akti, kas definē PF un ar to saistītās darbības, kā arī spēja savākt un iesniegt tiesā pierādījumus.

124. Lai izveidotu pārliecinošas lietas, būtiski ir arī koordinēti izmeklēšanas vienību un prokuroru centieni. Mācīšanās no precedentiem un zināšanas par tipoloģijām un jaunām metodēm, ko izmanto PF un sankciju apiešanas izmantotāji, var uzlabot izmeklēšanas un līdz ar to arī kriminālvajāšanas izdošanās iespējas. Turklāt PF kriminālvajāšanā nozīmīga loma var būt globālām partnerībām, uzsverot starptautiskās sadarbības vērtību šo sarežģīto noziegumu apkarošanā. Visbeidzot, nopietni konfiskācijas un līdzekļu atgūšanas noteikumi varētu veicināt kriminālvajāšanu, jo īpaši attiecībā uz līdzekļiem, kas aizplūst no valsts.

PF lietu kriminālvajāšanas izaicinājumi

125. Lielākā daļa valstu ziņoja, ka sarežģītu PF un sankciju apiešanas lietu kriminālvajāšana ir problemātiska. Dažas valstis minēja pierādīšanas grūtības, lai pierādītu, ka kontrolētās vai aizliegtās preces ir nosūtītas uz jurisdikciju, kurai piemēro sankcijas. Gadījumos, kad šādas pierādīšanas problēmas ir nepārvaramas, ir piemēri, kad prokurori vajā likumpārkāpējus par citiem noziedzīgiem nodarījumiem, kas izdarīti, lai slēptu viņu izdarīto PF nodarījumu, piemēram, par tiesvedības kavēšanu vai viltojumiem. Citi minēja, ka diplomātiskā imunitāte var ierobežot dažu PF vai sankciju apiešanas lietu izskatīšanu.

126. Vēl viena problēma, ar ko saskaras valstis, ir pierādīt, ka finanšu darbības ir tieši saistītas ar PF vai sankciju apiešanu, jo īpaši, ja pierādījumi ir izkliedēti dažādās valstīs. Tam nepieciešama detalizēta dokumentācija un cieša starptautiska sadarbība, ko ne vienmēr ir viegli panākt šādos sarežģītos gadījumos.

127. Informācijas un izlūkdatu apmaiņa starp valstīm var palīdzēt novērst nepilnības tiesībaizsardzības jomā, un valstis var efektīvāk risināt pārrobežu lietas un novērst PF tīklu iespējas izmantot globālās finanšu sistēmas nepilnības. Tomēr daudzās valstīs šādu mehānismu nav.

128. Veiksmīgai kriminālvajāšanai būtiska ir arī apmācība un informētības veicināšana, lai gan daudzas finanšu iestādes, uzņēmumi un pat prokurori neizprot PF riskus un sarežģītību. Pienācīga apmācība var palīdzēt viņiem atpazīt aizdomīgas darbības un saprast, kā darbojas PF shēmas. Tas ir svarīgi, jo īpaši valstīs ar ierobežotiem resursiem vai pieredzi PF lietu izskatīšanā.

Citi pasākumi, kas attur no sankciju pārkāpšanas

129. Kā jau izklāstīts šajā sadaļā, valsts iestādes var apsvērt kriminālvajāšanu par TFS pārkāpumiem. Turklāt dažas valstis apsver citas izpildes iespējas, lai novērstu TFS pārkāpumus, tostarp saistībā ar PF. Tā kā daudzas valstis, šķiet, saskaras ar ievērojamām grūtībām sarežģītu PF un sankciju apiešanas lietu kriminālvajāšanā, attiecīgajos apstākļos var būt vērts apsvērt citu pasākumu īstenošanu.

40. ierāmējums. Jurisdikcijas piemēri: civiltiesiskās un krimināltiesiskās izpildes darbības kā papildinājums vai alternatīva kriminālvajāšanai

- **Eiropas Komisija**: ar ES 2024. gada 24. aprīļa Direktīvu 2024/1226 tika ieviesti jauni noteikumi, lai visās dalībvalstīs noteiktu kopīgus pamata standartus krimināltiesiskiem sodiem fiziskām personām un krimināltiesiskiem sodiem vai ar krimināltiesiskiem sodiem nesaistītiem sodiem juridiskām personām, novēršot esošās juridiskās nepilnības un palielinot preventīvo rezultātu, kas attur no ES sankciju pārkāpšanas.[59]
- **Apvienotā Karaliste**: finansiālo sankciju pārkāpums var būt krimināInoziegums, par ko pēc notiesāšanas var sodīt ar brīvības atņemšanu uz laiku līdz septiņiem gadiem. Lai novērstu finanšu sankciju pārkāpumus, ir gan civiltiesiskas, gan krimināltiesiskas izpildes iespējas. Tiesībaizsardzības iestādes var apsvērt kriminālvajāšanu par finanšu sankciju pārkāpumiem. Ar 2017. gada likumu izveidotais naudas sodu režīms ir alternatīva kriminālvajāšanai par finanšu sankciju tiesību aktu pārkāpumiem. OFSI ir Viņa Majestātes Valsts kases struktūrvienība, kas piemēro šos naudas sodus.[60]
- **Amerikas Savienotās Valstis**: OFAC izmeklēšanas un izpildes pilnvaras ir tikai civiltiesiskas atšķirībā no krimināltiesisko sankciju izpildes pilnvarām, ko šajā jomā īsteno DOJ, DHS un Tirdzniecības departaments. Vajadzības gadījumā tiesībaizsardzības pasākumos tiek uzsvērta stingru un efektīvu sankciju atbilstības programmu nozīme, jo īpaši attiecībā uz uzņēmumiem, kas iesaistīti sarežģītos starptautiskos darījumos, lai nodrošinātu, ka tiek īstenoti pasākumi, kas novērš iesaistīšanos sankciju apiešanas shēmās.
- 2023. gada aprīlī tabakas un cigarešu ražotājs British American Tobacco (BAT) piekrita samaksāt 508 612 492 ASV dolārus, lai nokārtotu savu iespējamo civiltiesisko atbildību par OFAC sankciju pret KTDR un WMD izplatītājiem acīmredzamiem pārkāpumiem. Eksportējot tabaku un saistītos produktus un saņemot samaksu par šo eksportu, BAT lika ASV finanšu iestādēm apstrādāt elektroniskos pārskaitījumus, kuros bija ietvertas sankcijām pakļauto KTDR banku bloķētās īpašuma tiesības, kā arī eksportēt finanšu pakalpojumus un veicināt tabakas eksportu uz KTDR.[61]
- 2022. gada aprīlī OFAC noslēdza izlīgumu ar Toll Holdings Limited ("Toll"), Austrālijā reģistrētu starptautisku kravu pārvadājumu un loģistikas uzņēmumu, par acīmredzamiem vairāku sankciju programmu pārkāpumiem, tostarp par tādu darījumu apstrādi, kuros iesaistīta KTDR, Irāna un Sīrija. Galvenā ievainojamība bija nepietiekama riska pārvaldība un pienācīga rūpība Toll atbilstības nodrošināšanas funkcijā.[62]

Avoti: Eiropas Komisija, Apvienotā Karaliste un Amerikas Savienotās Valstis

Iekšzemes koordinācija un sadarbība

Starpaģentūru mehānismi

130. Efektīvs starpaģentūru regulējums palīdz mazināt riskus, kas saistīti ar sarežģītām PF un sankciju apiešanas shēmām. Lai izstrādātu efektīvas starpaģentūru sistēmas, valstis ziņo, ka ir nepieciešama pastāvīga sadarbība un koordinācija starp attiecīgajām valsts iestādēm.

Daudzās valstīs attiecīgie dalībnieki ietver AML/CFT/CPF amatpersonas, tiesībaizsardzības iestādes, uzraudzības iestādes, tiesu iestādes, importa un eksporta kontroles un licencēšanas iestādes, muitas, robežkontroles un izlūkošanas aģentūras. Valstis ziņo, ka cieša sadarbība un koordinācija starp daudzām no šīm kompetentajām iestādēm atvieglo attiecīgas un savlaicīgas informācijas apmaiņu. Izmantojot šo starpaģentūru procesu, valsts iestādes var vislabāk palīdzēt uzsākt un turpināt izmeklēšanu par iespējamiem TFS režīma pārkāpumiem un citām attiecīgām PF darbībām.

Starpaģentūru sadarbības labā prakse

131. Pamatojoties uz FATF Globālā tīkla iesniegumiem, valstis izmanto starpaģentūru mehānismus, lai novērstu PF un izvairīšanos no sankcijām, izmantojot vienu no trim kategorijām, kas savstarpēji pārklājas: 1) vispārēja koordinācija TFS jomā, kas ietver PF-TFS; 2) specializēta koordinācija PF-TFS un eksporta kontroles noteikumu jomā; vai 3) specializēta koordinācija PF-TFS un eksporta kontroles noteikumu jomā, kā arī plašāka koordinācija, lai uzsāktu sarežģītu PF un sankciju apiešanas izmeklēšanu, kriminālvajāšanu un citus pasākumus.

132. Saskaņā ar FATF 7. ieteikumu FATF Globālajam tīklam ir pienākums nekavējoties ieviest TFS, lai izpildītu visas ANO DP rezolūcijas, kas attiecas uz PF.[63] Lielākā daļa valstu pārbaudīja, vai ir izveidots tiesiskais regulējums PF-TFS ieviešanai, kas bieži vien ietver esošo starpaģentūru mehānismu izmantošanu TFS jomā. Šāda veida starpaģentūru mehānisms ļauj valstīm izpildīt to minimālās uz noteikumiem balstītās prasības, lai novērstu 7. ieteikumā minētos iespējamos TFS pārkāpumus, neizpildi vai izvairīšanos no to izpildes.

---

59 Jauno noteikumu mērķis ir nodrošināt, ka par šādiem pārkāpumiem visās dalībvalstīs var veikt krimināli zmeklēšanu un saukt pie kriminālatbildības. Tajos ir uzskaitīti noziedzīgi nodarījumi, kas saistīti ar ES sankciju pārkāpšanu un apiešanu, piemēram, aktīvu neiesaldēšana; ceļošanas aizliegumu un ieroču embargo pārkāpšana; aizliegtu vai ierobežotu ekonomisko un finanšu pakalpojumu sniegšana; iesaldējamo līdzekļu pārskaitīšana trešajām personām vai nepatiesas informācijas sniegšana, lai noslēptu iesaldējamos līdzekļus. Tie ietver arī stingrākus noteikumus par ES sankcijām pakļauto ieņēmumu, līdzekļu un aktīvu iesaldēšanu un konfiskāciju. Turklāt jauno noteikumu mērķis ir stiprināt sadarbību un saziņu starp dalībvalsts kompetentajām iestādēm, kā arī starp dalībvalstīm un citām attiecīgajām ES iestādēm, struktūrām, birojiem un aģentūrām.

60 Norādījumi par finanšu sankciju izpildi un naudas sodiem – GOV.UK.

61 Saskaņā ar tiesas dokumentiem BAT Marketing Singapore (BATMS) atzina savu vainu Kolumbijas apgabalā iesniegtajā kriminālinformācijā, kurā BAT un BATMS apsūdzētas sazvērestībā, lai veiktu krāpšanu bankās, un sazvērestībā, lai pārkāptu IEEPA. Saistībā ar šīm apsūdzībām BAT noslēdza vienošanos par kriminālvajāšanas atlikšanu.

62 Toll īstenoja gandrīz 3000 maksājumu saistībā ar jūras, gaisa un dzelzceļa pārvadājumiem, kurus veica vai saņēma tās globālās struktūrvienības, izmantojot ASV finanšu iestādes, un no kuriem labumu guva fiziskas vai juridiskas personas, uz kurām attiecās ASV sankcijas vai kuras atradās ANO vai ASV sankcijām pakļautās valstīs. Vairāk nekā pusi no attiecīgā perioda Toll atbilstības nodrošināšanas funkcija neņēma vērā politikas un kontroles pasākumus, kas būtu samērīgi ar Toll darbības sarežģītību, kurā bija gandrīz 600 rēķinu izrakstīšanas, datu, maksājumu un citu sistēmu lietojumprogrammu, kas bija izvietotas dažādās uzņēmuma struktūrvienībās. Tiesībaizsardzības pasākumā atklājās, ka pēc tam, kad banka pauda bažas, vai Toll pilda ASV sankcijas, Toll veica risku mazināšanas pasākumus, 2016. gada jūnijā pārtraucot visu sadarbību ar ASV sankcijām pakļautajām valstīm. Tomēr Toll nieviesa nepieciešamās atbilstības politikas un procedūras, lai novērstu maksājumus, kuros iesaistītas sankcijām pakļautas personas vai organizācijas, kā arī nepārbaudīja, vai sūtījumos ir iesaistītas personas, kas atrodas ANO vai ASV sankcijām pakļautā jurisdikcijā.

63 Tas prasa valstīm nekavējoties iesaldēt līdzekļus vai citus aktīvus un nodrošināt, ka līdzekļi un citi aktīvi netiek tieši vai netieši darīti pieejami jebkurai personai vai uzņēmumam, ko Apvienoto Nāciju Organizācijas Drošības padome norādījusi vai uz ko attiecas Apvienoto Nāciju Organizācijas Statūtu VII nodaļa, vai personām un organizācijām, kas rīkojas to vārdā, pēc to norādījumiem vai kas ir to īpašumā vai kontrolē, vai to labā. Ar nosacījumu, ka personas, kas darbojas sarakstā iekļauto personu un uzņēmumu vārdā vai to kontrolē vai kas ir to īpašumā vai kontrolē, nav iekļautas sarakstā saskaņā ar valsts/pārvalstisku sankciju režīmiem.

41. ierāmējums. FSRB sekretariāta piemērs: GAFILAT dalībvalstīm rīko TFS iesaldēšanas paraugmēģinājumus

GAFILAT rīko paraugmēģinājumus, kas ļauj dalībvalstīm pārbaudīt savus starpaģentūru procesus TFS ieviešanai saskaņā ar FATF standartiem. Pamatojoties uz GAFILAT izstrādāto metodoloģiju un rokasgrāmatu, dalībvalstis reaģē uz scenārijiem, kuru mērķis ir pārbaudīt TFS spējas un kontroles mehānismus (tostarp tos, kas ir ieviesti valsts un privātajā sektorā).

Ar šo treniņu palīdzību GAFILAT cenšas nodrošināt dalībvalstīm praktisku instrumentu, lai identificētu iespējamās vājās vietas un stiprinātu to TFS sistēmas. Pēc mācībām GAFILAT sniedz valstij nepublisku ziņojumu ar atsauksmēm un norādījumiem. Kopš 2024. gada GAFILAT trīs dalībvalstīm ir veicis trīs paraugmēģinājumus par TF-TFS procesiem. Nākotnē GAFILAT plāno rīkot papildu paraugmēģinājumus pārējām savām dalībvalstīm, tostarp sesijas, kas vērstas uz PF-TFS procesiem.

Avots: GAFILAT

133. Saistībā ar divējāda lietojuma precēm eksporta kontroles iestādes ir atbildīgas par lielākās daļas komerciālo preču eksporta regulēšanu, kuras bieži dēvē par "divējāda lietojuma" precēm, proti, precēm, kurām ir gan komerciāls, gan militārs vai proliferācijas pielietojums.[64] Daudzas valstis pārsniedz TFS prasības saskaņā ar 1718. UNSCR un piešķir prioritāti eksporta kontroles noteikumu īstenošanai kā plašākam riska pārvaldības instrumentam pret PF un sankciju apiešanu.

42. ierāmējums. Jurisdikcijas piemēri: starpaģentūru mehānismi, kas ietver eksporta kontroles noteikumus

- **Indija:** Izveidoja vairākus mehānismus darbības un politiku koordinācijai PF jomā, tostarp starpministriju darba grupu (IMWG) SCOMET (speciālo ķīmisko vielu, organismu, materiālu, iekārtu un tehnoloģiju) licencēšanai, kas apspriež divējāda lietojuma preču eksporta licencēšanas pieteikumus un ar to saistītos jautājumus. Kā arī vairāku aģentūru koordinācijas mehānismu, kas izveidots saskaņā ar Indijas 2005. gada WMD likumu, vada Indijas FID, un tajā piedalās regulatori, tiesībaizsardzības iestādes un citas attiecīgās organizācijas.[65]

---

[64] Divējāda lietojuma preču eksporta licences ir nepieciešamas noteiktās situācijās, kas saistītas ar valsts drošību, ārpolitiku, deficītu, kodolieroču neizplatīšanu, raķešu tehnoloģijām, ķīmiskajiem un bioloģiskajiem ieročiem, reģionālo stabilitāti, noziedzības kontroli vai bažām par terorismu. Licences prasības ir atkarīgas no priekšmeta tehniskajiem parametriem, galamērķa, galapatēriņa un galalietotāja, kā arī citām galalietotāja darbībām. Pat ja licence nav nepieciešama, pirms eksportēšanas var būt jāizpilda papildu prasības. Divi turpmāk minētie piemēri ilustrē īpašu uzmanību eksporta kontroles noteikumiem, kas attiecas uz PF un sankciju apiešanu.

[65] Saskaņā ar attiecīgajiem WMD likuma noteikumiem Indijas dažādās konsultāciju komitejas WMD un to piegādes sistēmu, kodolieroču un ar kodolieročiem saistītu priekšmetu, ķīmisko ieroču un ar tiem saistītu priekšmetu, bioloģisko ieroču un ar tiem saistītu priekšmetu, kā arī divējāda lietojuma preču eksporta kontroles jautājumos periodiski sasauc sanāksmes. Sanāksmēs piedalās attiecīgās Indijas valdības organizācijas, lai izskatītu politikas un saistītos jautājumus par attiecīgajiem WMD likuma un citu attiecīgo Indijas valdības aktu noteikumiem, kas attiecas uz WMD, to piegādes sistēmām un saistītām divējāda lietojuma precēm un tehnoloģijām.

- **Singapūra:** Eksporta kontroles starpministriju komiteja (IMC-EC), kas pārrauga Singapūras eksporta kontroles sistēmu, tostarp politikas un operatīvos jautājumus saistībā ar WMD proliferāciju un PF. IMC-EC vada Ārlietu ministrija, un tās sastāvā ir attiecīgās politikas un tiesībaizsardzības iestādes. IMC-EC arī uzrauga, kā Singapūra īsteno attiecīgās UNSCR, un koordinē starpaģentūru papildu pasākumus, kad Singapūra saņem informāciju/izlūkdatus saistībā ar WMD proliferāciju un PF.

Avoti: Indija un Singapūra

134. Kā aprakstīts iepriekš šajā ziņojumā, izpratne par šo plašāko WMD izplatīšanas risku un tā pamatā esošo finansējumu var pozitīvi ietekmēt izpratni par PF-TFS pārkāpšanas, neīstenošanas vai apiešanas risku (t. i., FATF standartos ietverto PF risku šaurā definīcija) un palīdzēt īstenot uz risku balstītus pasākumus un TFS. Šajā kontekstā turpmāk minētie piemēri ilustrē plašāku koordinēšanas tvērumu, lai uzsāktu sarežģītu izmeklēšanu, kriminālvajāšanu un citus pasākumus saistībā ar PF un izvairīšanos no sankcijām.

43. ierāmējums. Jurisdikcijas piemēri: starpaģentūru mehānismi, lai risinātu plašāku PF risku

- **Japāna:** saskaņā ar AML, CFT un CPF politikas starpministriju padomi, kuras līdzpriekšsēdētāji ir Valsts policijas aģentūra un Finanšu ministrija, Finanšu ministrija un Finanšu pakalpojumu aģentūra veic "kopīgas pārbaudes", kurās tās kopīgi veic Finanšu ministrijas ārvalstu valūtas maiņas pārbaudes un Finanšu pakalpojumu aģentūras AML pārbaudes, lai apmainītos ar inspekcijas amatpersonu zināšanām un pārbaudes informāciju starp attiecīgajām uzraudzības iestādēm un efektīvi un lietderīgi nodrošinātu finanšu iestāžu atbilstību attiecīgajiem tiesību aktiem un noteikumiem. Turklāt, ja JMSDF (Japānas Jūras pašaizsardzības spēki) kuģi vai citi līdzekļi atklāj darbības, par kurām ir aizdomas, ka tās ir nelikumīgas jūrniecības darbības, tostarp UNSCR aizliegtās pārvietošanas no kuģa uz kuģi, Aizsardzības ministrija sniedz informāciju attiecīgajām ministrijām un aģentūrām.
- **Malaizija:** Malaizijas CPF režīma vairāku aģentūru sadarbību un koordināciju papildina divas galvenās starpaģentūru grupas: Stratēģiskā tirdzniecības rīcības komiteja (STAC), ko vada Stratēģiskais tirdzniecības kontrolieris (STC) Investīciju, tirdzniecības un rūpniecības ministrijā, un Nacionālā koordinācijas komiteja cīņai pret nelikumīgi iegūtu līdzekļu legalizēšanu (NCC), ko vada Bank Negara Malaysia. STAC galvenokārt koncentrējas uz 2010. gada Stratēģiskās tirdzniecības likuma (STA 2010) īstenošanu, kas regulē stratēģiskas nozīmes preču un tehnoloģiju eksportu, tranzītu, pārkraušanu un starpniecību, kurā galvenokārt piedalās tiesībaizsardzības iestādes un ar PF jautājumiem saistītās tehniskās aģentūras.

NCC, ko pārstāv attiecīgās AML/CFT/CPF ministrijas un aģentūras, izstrādā, īsteno un uzrauga nacionālās stratēģijas cīņai pret ML/TF/PF.

- **Amerikas Savienotās Valstis:** eksporta tiesību aktu izpildei (Tirdzniecības departamenta Rūpniecības un drošības birojā, BIS) ir piekļuve FinCEN Banku slepenības likuma (BSA) datiem, tā sadarbojas ar eksporta kopienu un veic izmeklēšanu, lai atbalstītu krimināltiesisko un administratīvo sodu piemērošanu. Tikmēr BIS pārvalda un īsteno eksporta kontroli attiecībā uz divējāda lietojuma precēm, konkrētu munīciju un komerciālām precēm, izmantojot Eksporta administrācijas noteikumus (EAR) saskaņā ar 2018. gada Eksporta kontroles reformas likumu (ECRA). BIS sadarbojas ar eksportētāju kopienu, lai novērstu pārkāpumus, un veic izmeklēšanu, lai vāktu pierādījumus krimināltiesisko un administratīvo sodu piemērošanai. BIS arī cieši sadarbojas ar FinCEN un OFAC, kā arī ar ASV tiesībaizsardzības iestādēm, lai uzraudzītu, vai netiek veikti nelikumīgi iepirkumi, izmantojot PF, izvairīšanos no sankcijām un eksporta kontroles shēmu apiešanu.

Avoti: Japāna, Malaizija un Amerikas Savienotās Valstis

Starpaģentūru koordinācijas izaicinājumi

135. Valstis ziņoja par dažādiem šķēršļiem veiksmīgai koordinācijai valsts iekšienē, bet daudzas problēmas bija saistītas ar vispārēju izpratnes un/vai ieinteresētības trūkumu PF risku risināšanā, jo īpaši salīdzinājumā ar ML un TF. Tā kā PF un sankciju apiešanas tīklus bieži vien var atbalstīt valsts dalībnieki, ir nepieciešama regulāra saziņa ar izlūkdienestu kopienu, un piekļuve operatīvai informācijai ir būtiska, lai atklātu sarežģītas korporatīvās struktūras un novērstu sankciju apiešanas shēmas.

136. Tomēr dažas valstis ziņoja par šķēršļiem, kas kavē savstarpēju apmaiņu ar izlūkdatiem, tostarp gadījumos, kad tas attiecas uz ārvalstu partneriem, kuri ierobežo piekļuvi informācijai. Šī problēma apgrūtina savlaicīgu informācijas apmaiņu un iespējas nekavējoties rīkoties pret PF dalībniekiem vai darbībām. Vienā jurisdikcijā izpratnes trūkums ietekmē PF prioritāšu noteikšanu, apgrūtinot attiecīgo iestāžu koncentrēšanos uz šo tematu, dalīšanos ar attiecīgo informāciju un savlaicīgu reaģēšanu uz starpvaldību pieprasījumiem.[66]

137. Dažas valstis ziņoja, ka tām trūkst attiecīgo resursu, zināšanu, pieredzes un tehnoloģiju, lai pienācīgi novērstu riskus, kas saistīti ar PF un sankciju apiešanas shēmām. Lai gan daudzas FATF Globālā tīkla valstis pēdējos desmit gados ir veltījušas resursus tiesiskā regulējuma atjaunināšanai, lai risinātu ar PF saistītos jautājumus saskaņā ar FATF standartiem, tas nav ievērojami veicinājis ar PF saistīto pasākumu efektīvu īstenošanu. Lai gan 2025. gada aprīlī vairāk nekā puse no 194 valstīm (54 %; 105 valstis), kas tika novērtētas 4. savstarpējā novērtējuma kārtā, ir izpildījusi (13 %; 26 valstis) vai lielā mērā izpildījusi R.7 (41 %; 79 valstis), tikai 24 % no šīm 105 valstīm (25 no 105 valstīm) ir ieguvuši ļoti vai lielā mērā efektīvu novērtējumu attiecībā uz IO.11. Kopumā 17 % no novērtētajām valstīm (32 no 194) ir ieguvušas ļoti vai lielā mērā efektīvu IO.11 vērtējumu (skatīt 1. un 2. attēlu).

[66] Šajā projektā dažas valstis ziņoja, ka sastapušās ar šķēršļiem starp aģentūrām, kas ierobežoja attiecīgās informācijas un gadījumu izpētes apmaiņu. Ņemot vērā sarežģīto PF un sankciju apiešanas shēmu raksturu, dažas valstis ziņoja, ka nespēj atcelt izlūkdatu slepenību un/vai dalīties ar citu sensitīvu informāciju ar pārējām FATF Globālā tīkla dalībvalstīm.

138. Tomēr 1. ieteikuma kontekstā 7. ieteikumā minētie pienākumi identificēt, novērtēt un izprast PF-TFS riskus veicina globālus centienus novērtēt PF riskus, kas var palielināt efektivitāti turpmākajos gados. Vairāk nekā puse valstu ziņoja, ka pēdējo piecu gadu laikā ir pabeigušas PF riska novērtējumu vai NRA PF nodaļu, savukārt gandrīz ceturtā daļa valstu pašlaik veic savu pirmo PF riska novērtējumu un plāno pabeigt šo procesu līdz 2025. gada beigām.

Informācijas apmaiņa starp valsts un privāto sektoru

139. Valsts un privātā sektora partnerība (PPP) var būt vērtīga platforma ieinteresēto personu sadarbības stiprināšanai. Šo partnerību mērķis ir ļaut valdībām dalīties ar noderīgu informāciju (piemēram, tipoloģiju, izvairīšanās no nodokļu maksāšanas rādītājiem, labo praksi, problēmām) ar privātā sektora kontaktpersonām. Ja valsts sektors atklāj rīcībai izmantojamu informāciju, privātais sektors var labāk analizēt savus klientu un darījumu ierakstus, lai identificētu pašreizējās un vēsturiskās potenciāli nelikumīgās darbības, tostarp iespējamo izvairīšanos no sankcijām. Tādējādi šāda veida apmaiņa veicina valsts sektora spēju identificēt un mazināt riskus un izdot mērķtiecīgus norādījumus, kas paredzēti privātā sektora uzņēmumiem, vienlaikus saglabājot atbildību par klientu privātuma saglabāšanu.

140. Lai atbalstītu informācijas apmaiņu, daudzas valstis ziņoja, ka ir izstrādājušas un uzrauga riska rādītājus un brīdinājuma signālus par PF un sankciju apiešanas shēmām, galveno uzmanību pievēršot darījumiem un tirdzniecības modeļiem (skatīt A pielikumu: attiecas uz proliferācijas finansēšanu). Parasti valstis ar riska rādītāju sarakstu iepazīstina gan publisko, gan privāto sektoru, periodiski īstenojot informatīvus un izpratni veicinošus pasākumus. Tomēr gandrīz puse valstu nav ziņojušas par šādu riska rādītāju un brīdinājuma signālu izstrādi vai uzturēšanu. Tas var liecināt par to, ka PF riska rādītāji netiek nošķirti no citiem finanšu noziegumiem vai ka šajās valstīs nav piešķirta prioritāte sarežģītiem PF un sankciju apiešanas gadījumiem. Tā kā lielākā daļa valstu, lai atklātu PF un sankciju apiešanas darbības, paļaujas uz SAR/STR, pastāv iespējama informācijas plaisa starp valsts un privāto sektoru, kas mazina preventīvo pasākumu efektīvu īstenošanu.

Valsts sektora labā prakse

141. Aptuveni viena trešdaļa valstu ziņoja, ka koncentrējas uz privātā sektora informēšanu, īstenojot TFS tiesisko regulējumu, tostarp SAR/STR saņemšanu un TFS īstenošanu bez kavēšanās. Tomēr tikpat liels skaits valstu ziņoja par spēcīgāku valsts un privātā sektora sadarbību, izmantojot dažādas PPP, kuru galvenais mērķis parasti nav PF, lai gan pastāv darba grupas vai citi mehānismi, kas ļauj apspriest ar PF un sankciju apiešanu saistītus jautājumus. Dažas valstis ziņoja arī par tiesībaizsardzības iestāžu un izlūkdienestu vadītu sadarbību ar privāto sektoru papildus finanšu ministriju, FID un regulatoru līdzdalībai.

44. ierāmējums. Jurisdikcijas piemēri: valsts sektora informācijas sniegšana privātajam sektoram par PF un izvairīšanos no sankcijām

- **Francija**: lai informētu privāto sektoru un apmainītos ar informāciju, ir ieviesti "izpratnes veidošanas" mehānismi, izmantojot Banku un apdrošināšanas uzraudzības iestādi, kas atrodas Centrālās bankas pakļautībā, un Valsts kasi. Papildus finanšu iestādēm valsts un privātā sektora informācijas apmaiņa galvenokārt ir vērsta uz profesionāļiem nozarēs, kuras tiek uzskatītas par visvairāk pakļautām riskam, tostarp DNFBP un humānās palīdzības bezpeļņas organizācijām (NPO).

FID organizē īpašas neregulāras tikšanās ar Francijas finanšu iestādēm (bankām un kredītiestādēm), no kurām dažas skar proliferācijas finansēšanu. Šīs ziņotāju iestādes Aģentūrai ir vissvarīgākās, ņemot vērā to, ka 2023. gadā tās veidoja 52,6 % no ienākošajiem SAR/STR. Šīm sanāksmēm ir divējāds mērķis: i) informētības palielināšana un ii) akūto grūtību un problēmu risināšana, ar kurām bankas varētu saskarties PF apkarošanas ietvaros. TRACFIN rīkoja vairākas tikšanās ar dažām lielākajām Francijas bankām, lai labāk izprastu noteikumu ievērošanu attiecībā uz PF un iegūtu atgriezenisko saiti par problēmām, ar kurām tās saskaras PF gadījumu atklāšanā un CPF mehānismu ieviešanā.

- **Amerikas Savienotās Valstis**: Tirdzniecības departamenta BIS, kas administrē un īsteno Eksporta administratīvos noteikumus (EAR), sadarbībā ar FinCEN un citām ASV valdības struktūrvienībām periodiski publicē vadlīnijas un ieteikumus finanšu iestādēm. Publikācijās ir iekļauti brīdinājuma signāli un riska rādītāji, kas palīdz finanšu iestādēm identificēt darījumus, kuri varētu būt saistīti ar izvairīšanos no ASV eksporta kontroles. Nesen izdotajās publikācijās galvenā uzmanība tika pievērsta attiecīgajiem PF draudiem, ko rada globāla mēroga sankciju un eksporta kontroles apiešana, ar bezpilota lidaparātiem saistītās Irānas darbības un Ukrainas-Krievijas konflikts.[67,68,69]

Avoti: Francija un Amerikas Savienotās Valstis

Publiskā sektora izaicinājumi

142. Ņemot vērā PF un sankciju apiešanas būtību, kā arī to, ka nereti ir iesaistīti valsts dalībnieki un izlūkdatu vākšana, tas bieži vien ir saistīts ar sensitīvu informāciju, kuru ir grūti atklāt publiski. Daudzas valstis ir izveidojušas PPP, bet to galvenie mērķi parasti ir uzlabot SAR/STR efektīvu izmantošanu, un ir maz tādu partnerību piemēru, kas būtu īpaši vērstas uz PF vai sankciju apiešanas jautājumiem. Aptuveni ceturtā daļa valstu ziņo, ka to informācijas sniegšana privātajam sektoram par jautājumiem, kas saistīti ar PF un sankciju apiešanu, ir saistīta ar SAR/STR saņemšanu. Tomēr Singapūra un Apvienotā Karaliste izmanto PPP, lai pārvarētu dažas valsts-privātā sektora un privātā-privātā sektora informācijas apmaiņas problēmas saistībā ar PF un/vai sankciju apiešanu.

45. ierāmējums. Jurisdikcijas piemēri: informācijas apmaiņas šķēršļu pārvarēšana saistībā ar PF un/vai sankciju apiešanu

- **Singapūra**: 2024. gada 1. aprīlī Singapūras Monetārā iestāde kopā ar sešām lielākajām Singapūras komercbankām uzsāka digitālās platformas COSMIC, kas ir saīsinājums no angļu valodas "Collaborative Sharing of Money Laundering/Terrorist Financing Information and Cases" ("Sadarbība noziedzīgi iegūtu līdzekļu legalizēšanas/teroristu finansēšanas informācijas un lietu apmaiņā"), darbību. COSMIC ļauj FI droši apmainīties ar informāciju par klientiem, kuriem ir vairāki "sarkanie karodziņi", kas var liecināt par iespējamām finanšu noziegumu problēmām, ja ir sasniegtas noteiktas robežvērtības. Tādējādi FI ir vieglāk atklāt un tādējādi novērst noziedzīgas darbības.

67 FinCEN un BIS kopīgs paziņojums, FIN-2023-NTC2, 2023. gada 6. novembris.
68 Microsoft Word – Irānas bezpilota lidaparātu nozares konsultācijas – galīgais variants publicēšanai 9. jūnijā 10:00 (003).
69 FinCEN un BIS kopīgais brīdinājums par OCC-OGC-FO.

COSMIC pašlaik pievēršas trim galvenajiem finanšu noziegumu riskiem komercbanku nozarē: juridisko personu ļaunprātīga izmantošana, tirdzniecības finansējuma ļaunprātīga izmantošana nelikumīgiem mērķiem un proliferācijas finansēšana. COSMIC mērķis ir palīdzēt FI identificēt ļaunprātīgos dalībniekus un nekavējoties rīkoties, lai apturētu nelikumīgas darbības un tīklu, kā arī atbalstīt tiesībaizsardzību un finanšu sistēmas uzraudzību.

- **Apvienotā Karaliste:** tiesībaizsardzības iestādes (TAI) regulāri izmanto kopīgo noziedzīgi iegūtu līdzekļu legalizācijas izlūkošanas darba grupu (JMLIT), lai apmainītos ar izlūkdatiem ar privātā sektora pārstāvjiem, kuri savukārt atklāj savus izlūkdatus tiesībaizsardzības iestādēm. Tas ļauj privātajam sektoram izprast stratēģiskās tipoloģijas un taktiskos draudus. Finanšu sankciju īstenošanas birojs (OFSI) nesen ir izveidojis JMLIT sankciju apiešanas vienību, kuru kopīgi vada Apvienotajā Karalistē bāzēts FI.

Avoti: Singapūra un Apvienotā Karaliste

Privātā sektora labā prakse

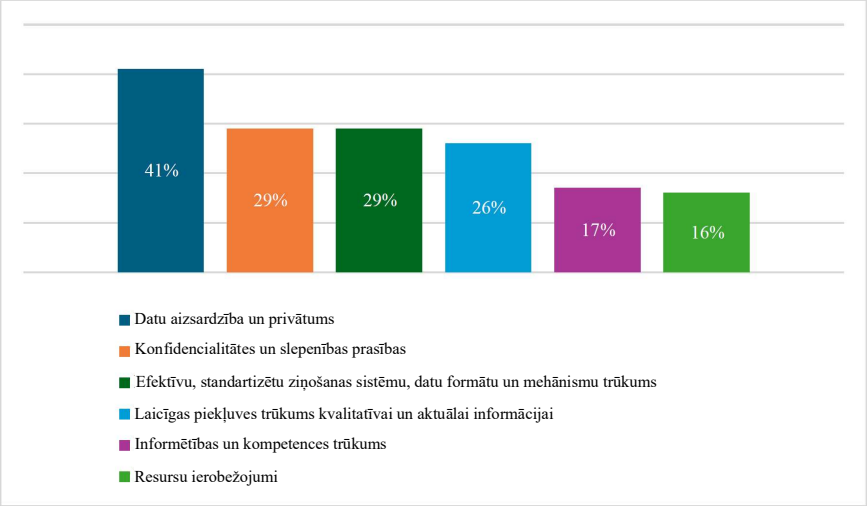
143. Daudzas privātā sektora struktūras ziņoja, ka PPP ir noderīgi rīki, lai veicinātu valsts-privātā sektora un privātā-privātā sektora informācijas apmaiņu par sankciju apiešanas un PF jautājumiem. Tomēr jāatzīmē, ka privātais sektors attiecībā uz informācijas apmaiņu minēja ievērojami vairāk problēmu nekā labās prakses piemēru (skatīt turpmāk "Privātā sektora problēmas"). Tika izteikti arī vairāki ierosinājumi valsts sektoram, kā uzlabot un paplašināt pašreizējās PPP iniciatīvas. Piemēram, privātā sektora uzņēmumi lūdza racionalizēt procesus, lai apmainītos ar informāciju ar FID un tiesībaizsardzības iestādēm; konsekventu pieeju savlaicīgai informācijas apmaiņai no valsts sektora; skaidrāku tiesisko regulējumu un/vai norādījumus, lai veicinātu valsts un privātā sektora informācijas apmaiņu papildu valstīs. Turklāt dažas privātā sektora struktūras norādīja, ka informācijas apmaiņas efektivitāti mazina tas, ka trūkst informācijas apmaiņas starp nozarēm. Tomēr vairākas privātā sektora struktūras uzskata, ka FATF varētu būt nozīmīga loma diskusiju virzīšanā un risku analīzē saistībā ar PF un izvairīšanos no sankcijām dažādās nozarēs.

Privātā sektora problēmas

144. Finanšu iestādes, DNFBP un VASP ir svarīgi dalībnieki sarežģītu PF un sankciju apiešanas shēmu novēršanā un apkarošanā. Tomēr privātā sektora struktūrām parasti ir mazāka izpratne par PF nekā par ML vai TF. Tādējādi lielākā daļa pašreizējo PPP piemēru galvenokārt ir vērsti uz to, lai valsts sektors palielinātu informētību par PF un sniegtu informāciju par SAR/STR iesniegšanu, kas var nedot iespēju privātajam sektoram apgūt, kā veikt konkrētus pasākumus, lai identificētu un atklātu sarežģītas PF un sankciju apiešanas shēmas. Lai atklātu un ziņotu par šīm sarežģītajām shēmām, privātais sektors, visticamāk, gūtu labumu no plašākām vadlīnijām par attiecīgo darbību, piemēram, tirdzniecības darījumu un liela apjoma informācijas apmaiņas starp vairākām pusēm, novērtēšanu. Attiecīgie dokumenti var tikt glabāti dažādos veidos un informācijas nesējos, kas var apgrūtināt datu salīdzināšanu ar starptautiskajiem un valstu sankciju sarakstiem.

145. Daudzas privātā sektora struktūras ziņoja par vairākām citām informācijas apmaiņas problēmām, tostarp par nevienmērīgu datu privātuma noteikumu īstenošanu, citiem regulatīviem ierobežojumiem un jurisdikcijas atšķirībām, konfidencialitātes un uzticamības problēmām, izlūkdatu izplatīšanas kavējumiem, nekonsekventiem datu formātiem un resursu ierobežojumiem (skatīt 4. attēlu). Privātais sektors jo īpaši uzsvēra, ka ir grūti rast līdzsvaru starp datu privātuma un preventīvo pasākumu pienākumiem. Tāpat arī dažas nebanku finanšu iestādes un DNFBP ziņoja, ka ir nepieciešamas nozaru vadlīnijas, jo pašreizējā informatīvā darbība ir vairāk vērsta uz lielo banku darbību.

4. attēls. Galvenie informācijas apmaiņas izaicinājumi



Starptautiskā sadarbība

146. Lai veicinātu konsekventu izpildi un mazinātu iespējas neatļautu darbību dalībniekiem izvēlēties valstis vai struktūras ar vājāku preventīvo kontroli, valsts un privātais sektors gūst labumu no saskaņotas pieejas tiesiskajam regulējumam attiecībā uz PF un sankciju apiešanu. FATF noteiktie standarti, piemēram, TFS ieviešana, un valstu pieņemtie standarti, kas var ietvert arī PF kriminalizēšanu un eksporta kontroles pastiprināšanu noteiktos gadījumos, veido kopīgu PF apkarošanas sistēmu. Piemēram, valstis, kas īsteno līdzīgus pasākumus pret finanšu iestāžu ļaunprātīgu izmantošanu, samazina vājāku saikņu iespējamību starptautiskajā finanšu sistēmā. Standartizētas eksporta kontroles un galalietotāju pārbaudes veicināšana palīdz novērst sensitīvu tehnoloģiju novirzīšanu aizliegtiem mērķiem un pārtraukt proliferācijas finansēšanu.

147. Starptautiska sadarbība ir būtiska arī, lai novērstu jaunos draudus, kas saistīti ar jaunajām finanšu tehnoloģijām, piemēram, virtuālajiem aktīviem. Šajā kontekstā, kā minēts iepriekš, FATF Virtuālo aktīvu kontaktgrupa ir intensīvi apspriedusi problēmas un paraugpraksi, lai efektīvi īstenotu AML/CFT/CPF pasākumus attiecībā uz virtuālajiem aktīviem, jo īpaši pieaugošos riskus saistībā ar virtuālo aktīvu zādzībām un ļaunprātīgu izmantošanu KTDR.

Starptautiskās sadarbības labā prakse

148. Dažas valstis ziņoja, ka efektīva starptautiskā sadarbība ir atkarīga no informācijas apmaiņas starp valdībām, finanšu iestādēm un privātā sektora dalībniekiem. Informācijas atklāšana par aizdomīgiem darījumiem, sankcijām pakļautām struktūrām un augsta riska darbībām palīdz identificēt un apturēt PF tīklus un sankciju apiešanu. Piemēram, SAR/STR atklāšana pāri robežām palīdz atklāt sarežģītas darījumu ķēdes, kas saistītas ar proliferāciju. Lielākās daļas valstu FID ziņoja, ka ir parakstījuši līgumus un saprašanās memorandus ar citiem FID, lai nodrošinātu izlūkdatu, tostarp ar PF darbībām saistītu izlūkdatu, apmaiņu. Piemēram, Egmont Group atvieglo drošu saziņu un sadarbību starp vairāk nekā 160 valstīm, ļaujot reāllaikā apmainīties ar noderīgu informāciju.

46. ierāmējums. Gadījuma izpēte: starptautiskā sadarbība kontrolētu divējāda lietojuma preču eksporta jomā

FINTRAC saņēma spontānu ziņojumu no FID, kurā bija sīki aprakstīti to jurisdikcijā esošo finanšu iestāžu iesniegtie SAR/STR, ziņojot par 90 aizdomīgiem elektroniskajiem pārskaitījumiem, kuru kopējā summa bija aptuveni 2,5 miljoni ASV dolāru. Spontānais ziņojums atklāja elektroniskos pārskaitījumus, kuros bija iesaistīti uzņēmumi, uz kuriem attiecas citas jurisdikcijas valsts sankciju režīms saistībā ar divējāda lietojuma preču nelikumīgu iegādi Krievijas aizsardzības nozarei. SAR/STR identificēja vairākus iespējamus nelikumīgi iegūtu līdzekļu legalizēšanas indikatorus un vairākus elektroniskos pārskaitījumus no FID jurisdikcijā esošajiem sarakstā iekļautiem uzņēmumiem uz uzņēmumiem Kanādā un uzņēmumiem augsta riska valstīs saistībā ar nelikumīgām iepirkuma darbībām.

FINTRAC novērtēja spontāno ziņojumu un sagatavoja informācijas atklāšanu, kurā detalizēti aprakstītas finanšu darbības, par kurām FINTRAC ziņots, izmantojot SAR/STR un elektroniskos naudas līdzekļu pārvedumu ziņojumus. Informācijas izpaušana ietvēra finanšu darījumus starp Kanādas uzņēmumu un saistītām personām/uzņēmumiem, par kuriem iepriekš tika veikta izmeklēšana saistībā ar aizdomām par nelikumīgu divējāda lietojuma/militāro preču eksportu Krievijas galalietotājiem. Turklāt SAR/STR aprakstīti darījumi, kas atbilst zināmai naudas atmazgāšanas tipoloģijai "Krievijas un Austrumeiropas noziedzīgi iegūtu līdzekļu legalizēšanas shēma", un darījumi ar Krievijas uzņēmumiem turpinājās arī pēc Kanādas sankciju piemērošanas.

Informācijas izpaušanas paketēs bija sniegts pārskats par iespējami nelikumīgu iepirkumu tīklu. Atklātā informācija tika nosūtīta vairākiem federālajiem informācijas saņēmējiem un citiem FID.

Avots: Kanāda

149. Pārrobežu sadarbība tiesībaizsardzības jomā ļauj valstīm risināt sarežģīto un starptautisko PF un sankciju apiešanas problēmu. Daudzvalstu darba grupas pastiprina valsts iestāžu resursus un zināšanas, lai izmeklētu un likvidētu tīklus. Piemēram, koordinētas operācijas var atklāt fiktīvus uzņēmumus, starpniekus un sarežģītus maršrutus, kuros iesaistītas vairākas valstis un kurus proliferācijas tīkli izmanto WMD programmu iepirkšanai un finansēšanai.

47. ierāmējums. Gadījuma izpēte: Spānijas valsts policija sadarbojas ar ES kolēģiem, lai cīnītos pret PF

Spānija nesen ir saskārusies ar vairākiem gadījumiem, kad bija nepieciešama starptautiska sadarbība ar citām ES valstīm. Visos gadījumos starpniecības uzņēmumi slēpa materiāla galamērķi. Iesaistītās struktūras bija uzņēmumu tīkli, no kuriem daži bija meitasuzņēmumi dažādās valstīs, un to vadītāji. Operācijās bija arī "koordinators" jeb starpnieks. Galvenais riska rādītājs, kas tika konstatēts dažādos gadījumos, bija neparasts pārdošanas apjoms, kā arī pēc finanšu analīzes veikšanas konstatētā pārskaitījumu izcelsme un dažādās summas.

Vienā gadījumā valsts policija izmeklēja aptuveni 5 miljonus eiro vērtu aizsardzības materiālu, jo īpaši militāro lidmašīnu detaļu, novirzīšanu uz Krieviju, izmantojot fiktīvus uzņēmumus un starpniekus. Izmeklēšanā tika atklāti attiecīgie maksājumi un maksājumu legalizēšana no fiktīvo uzņēmumu pārdošanas operācijām. Starptautiskā sadarbība ES valstu ietvaros ļāva izmeklēt sūtījumus, kas tika veikti pa sarežģītiem autoceļu un gaisa ceļu maršrutiem un šķērsoja dažādas valstis.

Citā gadījumā valsts policija izmeklēja vairāk nekā 800 000 eiro vērtu ķīmisko vielu novirzīšanu uz Krieviju, kas ir aizliegta saskaņā ar Eiropas Savienības sankcijām. Dažas no šīm vielām bija sprāgstvielu prekursori un ķīmisko ieroču prekursori. Pirms eksportēšanas ķīmiskās vielas tika uzglabātas Spānijas ostas brīvajā zonā. Spānijā valsts policija un muita veica kopīgu izmeklēšanu. Tā kā transportēšana tika veikta pa autoceļiem, bija jāsadarbojas ar citu valstu aģentūrām, lai izpētītu, kā materiāls tiek transportēts pāri Eiropas robežām.

Avots: Spānija

48. ierāmējums. Gadījuma izpēte: Amerikas Savienotās Valstis un Korejas Republika piemēro sankcijas dalībniekiem, kas finansē KTDR WMD programmu[70]

2024. gada martā OFAC, koordinējot savu darbību ar Korejas Republiku (KR), sarakstā iekļāva sešas personas un divus uzņēmumus, kas atrodas Krievijā, Ķīnā un Apvienotajos Arābu Emirātos un kas gūst ieņēmumus un veicina finanšu darījumus KTDR labā. Līdzekļi, ko iegūst ar šo dalībnieku starpniecību, galu galā tiek novirzīti KTDR WMD programmu atbalstam, tādējādi pārkāpjot 1718. UNSCR prasīto TFS. KR kopīgi norādīja sešas tās pašas personas un uzņēmumus par to, ka tās ir iesaistītas nelikumīgā finansēšanā un ieņēmumu gūšanā, izmantojot ārzemēs strādājošus KTDR IT darbiniekus.

Šī darbība ir vērsta pret norādīto KTDR banku aģentiem un uzņēmumiem, kas nodarbina KTDR IT darbiniekus ārvalstīs. KTDR banku pārstāvji, IT darbinieki un uzņēmumi, kas viņus nodarbina, gūst ienākumus un piekļuvi ārvalstu valūtai, kas ir svarīga KTDR valdībai.

[70] Valsts kases departaments, "Valsts kases sankcijas pret dalībniekiem, kas finansē Ziemeļkorejas masu iznīcināšanas ieroču programmu" (2024. gada 27. marts), Valsts kases sankcijas pret dalībniekiem, kas finansē Ziemeļkorejas masu iznīcināšanas ieroču programmu | ASV Valsts kases departaments.

Šie dalībnieki, kas galvenokārt darbojas, izmantojot Krievijā un Ķīnā izvietotus tīklus, organizē shēmas, veido fiktīvus vai čaulas uzņēmumus un pārvalda slēptus bankas kontus, lai pārvietotu un slēptu nelikumīgus līdzekļus, apietu sankcijas un finansētu KTDR nelikumīgās WMD un ballistisko raķešu programmas.

Avots: Amerikas Savienotās Valstis

150. Dažas valstis un starptautiskās organizācijas, piemēram, ANO Narkotiku un noziedzības apkarošanas birojs (UNODC) un Pasaules Banka, nodrošina apmācības, tehnisko palīdzību un finansējumu, lai stiprinātu institucionālās un izpildes spējas valstīs ar ierobežotiem resursiem. Programmās galvenā uzmanība pievērsta normatīvās bāzes uzlabošanai, uzraudzības sistēmu uzlabošanai un valsts un privātā sektora informētības palielināšanai par PF riskiem. Lai efektīvi cīnītos pret proliferācijas finansēšanu, ļoti svarīgi ir sniegt speciālās zināšanas par efektīvas eksporta kontroles un galalietotāju pārbaudes īstenošanu, kā arī palīdzēt valstīm ieviest progresīvas uzraudzības sistēmas, lai atklātu ar proliferāciju saistītas finanšu darbības un ziņotu par tām.

49. ierāmējums. Jurisdikcijas piemērs: Eiropas programma EU P2P (Partner to Partner)

EU P2P (Partner to Partner) eksporta kontroles programmas mērķis ir pastiprināt divējāda lietojuma preču eksporta kontroli un ieroču tirdzniecību visā pasaulē. Programmas mērķi, ko pārvalda Eiropas Komisija un Eiropas Ārējās darbības dienests un koordinē Expertise France, ir veicināt un stiprināt starptautisko sadarbību divējāda lietojuma preču eksporta kontroles, Ieroču tirdzniecības līguma īstenošanas un ieroču eksporta kontroles jomā, stiprinot valstu un reģionālās spējas, ņemot vērā līdzsvaru starp drošības un ekonomiskajiem apsvērumiem. Programma ietver informētības palielināšanas pasākumus par PF riskiem un tehnisko palīdzību, lai izstrādātu valsts riska novērtējumu par proliferācijas finansēšanu.

Avots: Francija

Starptautiskās sadarbības izaicinājumi

151. Kā minēts citās šā ziņojuma daļās, jurisdikciju tiesiskā regulējuma un sankciju programmu atšķirības ir galvenais izaicinājums efektīvai starptautiskai sadarbībai cīņā pret sarežģītām PF un sankciju apiešanas shēmām (tostarp atšķirīgas pieejas PF kriminalizēšanai, kas ir aplūkotas sadaļās par atklāšanu, izmeklēšanu un kriminālvajāšanu). PF tīkli un sankciju apiešanas veicinātāji darbojas pāri robežām, ekspluatējot regulējuma atšķirības, izmantojot dažādas finanšu sistēmas un starptautisko tirdzniecību, tādējādi apdraudot globālo drošību. Tāpēc, lai novērstu šos riskus, ir nepieciešama cieša starptautiska sadarbība, lai stiprinātu valsts iestāžu spēju novērst, atklāt un pārtraukt nelikumīgas darbības. Tāpat ir nepieciešama sadarbība starp valstīm un starptautiskajām organizācijām, jo daudzām valstīm trūkst infrastruktūras vai pieredzes, lai efektīvi uzraudzītu un apkarotu PF un sankciju apiešanu.

6. Secinājumi un prioritārās jomas

152. Lai gan daudzas valstis pēdējos gados ir pabeigušas PF riska novērtējumu vai līdz 2025. gada beigām pabeigs savu pirmo novērtējumu, FATF Globālais tīkls ir dažādās stadijās, lai identificētu un mazinātu draudus un ievainojamību, kas saistīta ar sarežģītām PF un sankciju apiešanas shēmām. Diemžēl turpmākajos gados kopīgie centieni apkarot un novērst PF un izvairīšanos no sankcijām var kļūt arvien grūtāki. Valsts un nevalstiskie dalībnieki, kam ir labi resursi, turpinās meklēt nepilnības tiesībaizsardzības, preventīvo pasākumu un tiesiskā regulējuma jomā, kā arī izmantos jauno tehnoloģiju un notiekošo ģeopolitiskās vides pārmaiņu priekšrocības.

153. Labākais veids, kā aizsargāt starptautisko finanšu sistēmu pret šo pieaugošo PF risku, ir stiprināt esošās un topošās saiknes, kas veido CPF kontroli visā pasaulē. Pēdējo desmit gadu laikā valstis ir guvušas ievērojamus panākumus CPF tiesiskā regulējuma atjaunināšanā un PF-TFS ieviešanā, taču, iespējams, ir nepieciešama kopīga strauja virzība uz priekšu CPF režīmu efektīvā īstenošanā. Saistībā ar FATF 1. ieteikuma pārskatīšanu FATF Globālajam tīklam jau ir izstrādāts plāns, kā virzīties uz šo mērķi. Kā aprakstīts 2021. gada PF vadlīnijās, valstīm ir jānosaka, jānovērtē, jāizprot un jāsamazina PF riski. Turklāt privātā sektora uzņēmumiem ir jāīsteno procesi, lai identificētu, novērtētu, uzraudzītu, pārvaldītu un mazinātu PF riskus, taču tie to var darīt savu esošo TFS un/vai atbilstības programmu ietvaros.[71] [72] Valstīm arī jāapsver, vai var būt nepieciešami papildu pasākumi darbam ar PF riskiem, tostarp izmantojot atklāšanas un ziņošanas rīkus, iekšzemes koordināciju un sadarbību, izmeklēšanu un kriminālvajāšanu, kā arī starptautisko sadarbību. [73]

154. Šis pētījums liecina, ka PF un sankciju apiešanas dalībnieki bieži izmanto starpniekus, lai maskētu savas nelikumīgās darbības un slēptu divējāda lietojuma preču un citu preču, kas paredzētas valstīm, kurās notiek proliferācija vai kurām piemēro sankcijas, patiesos gala lietotājus. Tiek izmantotas sarežģītas shēmas, lai slēptu to personu, uzņēmumu un valstu identitāti, kuras ir iesaistītas sankciju apiešanā, tādējādi apgrūtinot nelikumīgu darbību atklāšanu. Lai veicinātu FATF Globālā tīkla kopīgu rīcību, novērstu un apkarotu sarežģītas PF un sankciju apiešanas shēmas, ir vairākas prioritāras jomas, kurām būtu jāpievērš uzmanība.

---

71 Vadlīnijas par proliferācijas finansēšanas riska novērtēšanu un mazināšanu.

72 PF riska kontekstā uz risku balstīti finanšu iestāžu un DNFBP pasākumi ir vērsti uz to, lai pastiprinātu un papildinātu 7. ieteikuma stingro prasību pilnīgu īstenošanu, atklājot un novēršot mērķtiecīgu finanšu sankciju neizpildi, iespējamu pārkāpumu vai izvairīšanos no to izpildes. Nosakot pasākumus PF risku mazināšanai kādā nozarē, valstīm jāņem vērā ar attiecīgo nozari saistītie PF riski. Pieņemot uz risku balstītus pasākumus, kompetentajām iestādēm, finanšu iestādēm un DNFBP būtu jāspēj nodrošināt, ka šie pasākumi ir samērīgi ar identificētajiem riskiem, un tas ļautu tām pieņemt lēmumus par to, kā visefektīvāk sadalīt savus resursus.

73 Saskaņā ar 2. ieteikumu un tā skaidrojošo piezīmi valstīm būtu jāievieš starpaģentūru sistēma, lai efektīvāk mazinātu proliferācijas finansēšanas riskus.

Ieteikumi turpmākajam FATF darbam saistībā ar CPF

a) **Periodiski atjaunināta informācija par PF:** apsveriet iespēju regulāri atjaunināt šā ziņojuma sadaļas par pašreizējo situāciju, tendencēm un metodēm. PF un sankciju apiešanas risks tuvākajā nākotnē joprojām būs būtisks izaicinājums, ar ko FATF Globālajam tīklam būs jātiek galā. Tomēr draudi, ievainojamības un tipoloģijas, kas ir mūsu kolektīvās izpratnes par šo jautājumu pamatā, noteikti pastāvīgi attīstīsies un mainīsies. Ņemot vērā PF riska novērtēšanas būtību, valstīm un privātajam sektoram ir svarīgi saglabāt izpratni par pašreizējo situāciju. Bez 1718. UNSCR POE ziņojumiem FATF būtu jāpalīdz galvenajām ieinteresētajām personām uzraudzīt riska situāciju.

b) **Veicināt valsts un privātā sektora sadarbību**: apsveriet iespēju izmantot šo ziņojumu un publiskās apspriešanas laikā gūtās atziņas, lai FATF pasākuma ietvaros strukturētu informācijas sniegšanu privātajam sektoram un pēc tam izmantotu viņu atsauksmes, lai izstrādātu turpmāku vadlīniju ziņojumu, kas būtu vairāk vērsts uz pasākumiem, kurus var veikt sadarbībā ar finanšu iestādēm, DNFBP un VASP, lai stiprinātu CPF novēršanas pasākumus. Piemēram, 2026. gada privātā sektora konsultatīvajam forumam varētu organizēt attiecīgu sesiju vai sesiju sēriju. Tā kā FATF Globālais tīkls ziņoja, ka PF un sankciju izmeklēšanas uzsākšanā lielā mērā paļaujas uz SAR/STR, var izmantot koordinētāku informēšanu un norādījumus, lai stiprinātu valsts un privātā sektora informācijas apmaiņu attiecīgajās nozarēs.

c) **WMD PF definīcija**: piecu gadu laikā apsveriet iespēju FATF vispārīgo glosāriju papildināt ar oficiālu WMD PF definīciju, ņemot vērā FATF Globālā tīkla PF riska novērtējumu horizontālā pārskata rezultātus. Kā izklāstīts šajā ziņojumā, jurisdikciju atšķirības pieejā attiecībā uz PF un sankciju apiešanu var apdraudēt vai sarežģīt atklāšanu, izmeklēšanu un starptautisko sadarbību šajā jomā. Vienota un vispārpieņemta definīcija mazinātu neapmierinātību ar PF un sankciju apiešanas novēršanu un apkarošanu.

d) **Horizontālā pārskatīšana attiecībā uz PF NRA:** trīs gadu laikā apsveriet iespēju veikt FATF Globālā tīkla PF riska novērtējumu horizontālo pārskatīšanu. Kā aprakstīts šajā ziņojumā, valstis ir dažādās PF riska identificēšanas, novērtēšanas, izpratnes un mazināšanas stadijās un izmanto virkni jaunu metožu, lai to izdarītu. Turklāt šķiet, ka ir nesabalansēta izpratne par ievainojamībām saistībā ar PF un sankciju apiešanu. Ņemot vērā svarīgo uzdevumu, kas gan valsts, gan privātajam sektoram ir jāveic, lai labāk izprastu PF risku saskaņā ar FATF standartiem, horizontālā pārskatīšana var palīdzēt identificēt labo praksi pēc tam, kad FATF Globālajam tīklam būs bijis vairāk laika PF riska novērtēšanai.

A pielikums: Riska rādītāji

1. Turpmāk sniegtie rādītāji ir neizsmeļošs saraksts, kas iegūts no FATF šā projekta gaitā saņemtās informācijas. Rādītāji ir izstrādāti, lai uzlabotu valsts un privātā sektora struktūru spēju identificēt aizdomīgus darījumus un/vai darbības, kas saistītas ar attiecīgajām PF un sankciju apiešanas shēmām. Lai gan vairāki identificētie rādītāji var nebūt tieši vai ekskluzīvi saistīti ar PF vai sankciju apiešanu un var liecināt par citiem nelikumīgas darbības veidiem, tie tomēr var būt svarīgi, mēģinot identificēt PF un sankciju apiešanas shēmas.

Kā izmantot šos rādītājus

2. Rādītājs var palielināt neparastas vai aizdomīgas darbības rašanās iespējamību. Viena rādītāja esamība saistībā ar klientu vai darījumu pati par sevi nevar būt pamats aizdomām par PF darījumu vai izvairīšanos no sankcijām, un rādītājs ne vienmēr skaidri norāda uz šādu darbību, taču tas var rosināt turpmāku uzraudzību un pārbaudi, ja nepieciešams. Tāpat arī vairāku rādītāju parādīšanās varētu būt iemesls rūpīgākai izpētei. Tas, vai viens vai vairāki rādītāji liecina par aizdomīgu darījumu vai darbību, ir atkarīgs arī no iestādes vai tirgus dalībnieka piedāvātā biznesa, produkta vai pakalpojuma, kā arī no tā, kā tas mijiedarbojas ar saviem klientiem.

3. Turpmāk uzskaitītie rādītāji attiecas gan uz valsts, gan privāto sektoru. Attiecībā uz privāto sektoru rādītāji ir svarīgi finanšu iestādēm, tostarp bankām un naudas vērtības pārvedumu pakalpojumiem, izraudzītiem nefinanšu uzņēmumiem un profesijām, virtuālo aktīvu pakalpojumu sniedzējiem, kā arī maziem un vidējiem uzņēmumiem un lieliem konglomerātiem, kas darbojas divējāda lietojuma preču jomā vai citās attiecīgajās nozarēs, vai kuriem ir saskarsmes punkti ar tām. Privātajā sektorā šos rādītājus ir paredzēts izmantot personālam, kas atbild par atbilstību, darījumu uzraudzību, izmeklēšanas analīzi, klientu uzņemšanu un attiecību pārvaldību, kā arī citām jomām, kas strādā, lai novērstu PF, izvairīšanos no sankcijām un predikatīvos noziegumus.

4. Dažiem riska rādītājiem nepieciešams savstarpēji salīdzināt dažādus datu elementus (piemēram, finanšu darījumus, muitas datus), kas bieži vien ir ārējos avotos. Ņemot vērā atkarību no ārējiem datiem, privātais sektors var neievērot visus turpmāk norādītos rādītājus. Attiecībā uz dažiem riska rādītājiem privātajam sektoram būs nepieciešama papildu kontekstuāla informācija no kompetentajām iestādēm, piemēram, sadarbojoties ar tiesībaizsardzības iestādēm vai FID. Izmantojot šos rādītājus, privātā sektora struktūrām būtu jāņem vērā arī klienta profila kopums, tostarp informācija, kas iegūta klienta uzticamības pārbaudes procesā, darījumos iesaistītās tirdzniecības finansēšanas metodes, ja piemērojams, un citi būtiski konteksta riska faktori.

5. Turpmākajā tabulā norādīti riska rādītāji, kas sagrupēti trīs plašās kategorijās: 1) klientu informācija/uzvedība; 2) darījumi; un 3) tirdzniecības darbības. Klientu informācijas/uzvedības rādītājus var izmantot, veicot CDD, savukārt darījumu rādītājus var izmantot darījumu, tostarp eksporta darījumu, uzraudzībai. Tirdzniecības darbības var sniegt papildu kontekstu, kas jāņem vērā plašākos riska pārvaldības procesos. Lai gan daži riska rādītāji katrā kategorijā pārklājas, FATF Globālais tīkls centās piešķirt prioritāti pēc iespējas plašākas informācijas sniegšanai, lai atbalstītu valsts un privāto sektoru.

1. Klientu informācija/uzvedība

1. Korporatīvo struktūru (piemēram, čaulas uzņēmumu) izmantošana, lai slēptu īpašumtiesības, līdzekļu avotu vai iesaistītās valstis/subjektus, jo īpaši valstīs, uz kurām attiecas sankcijas.
2. Galalietotāja slēpšana, izmantojot darījumu slāņošanu, kad iepirkuma aģenti novirza sūtījumus, saziņu un finanses, izmantojot vairākus uzņēmumu, brokeru un starpnieku slāņus.
3. Ja klients izmanto sarežģītas struktūras, lai slēptu importēto/eksportēto preču saistību, piemēram, izmanto daudzslāņainus akreditīvus, fiktīvus uzņēmumus, starpniekus un brokerus.
4. Izmaiņas standarta uzņēmējdarbības dokumentos, lai slēptu galīgo klientu.
5. Sīkāka informācija par pusēm ir līdzīga WMD sankcijās vai tirdzniecības kontrolē iekļautajām pusēm (piemēram, nosaukumi, adreses vai tālruņa numuri)
6. Konti pieder uzņēmumiem ar neskaidru īpašumtiesību struktūru, čaulas uzņēmumiem vai vienas dienas uzņēmumiem, vai arī darījumus veic uzņēmumi ar šādu struktūru.
7. Klients ir iesaistīts ierobežotu vai augsta riska preču un/vai tehnoloģiju apgādē, pārdošanā vai piegādē.
8. Klients iepriekš ir sadarbojies vai uztur attiecības ar personām vai uzņēmumiem, uz kuriem tagad attiecas sankcijas.
9. Puses fiziski atrodas valstīs, kas rada bažas par novirzīšanu (valstis, kas atļauj proliferācijas preču piegādi vai to finansēšanu caur savu teritoriju).
10. Klients vai klienta darījuma partneris veic darījumus ar iekšzemes sankciju režīmā iekļautām juridiskām un fiziskām personām vai darījumus, kas ir saistīti ar iekšzemes sankciju režīmā iekļautām juridiskām un fiziskām personām, piemēram, e-pasta adresēm, fiziskām adresēm, tālruņa numuriem, pases numuriem vai konvertējamas virtuālās valūtas (CVC) adresēm, norādītajiem identifikatoriem.
11. Klienti, kas saistīti ar universitātēm un pētniecības iestādēm, kuras strādā ar divējāda lietojuma precēm vai produktiem, uz kuriem attiecas eksporta kontrole.
12. Darījumi ir saistīti ar šķietamu civilo galalietotāju, bet pamata pētījumi liecina, ka adrese ir militārs objekts vai atrodas kopā ar militārajiem objektiem problemātiskā valstī.
13. Klients iegādājas jaunus kuģus bez acīmredzama ekonomiska vai uzņēmējdarbības mērķa.
14. Uzņēmējdarbības modelis ir pilnībā orientēts uz eksportu, darbojoties kā caurlaides vienība.
15. Uzņēmums darbojas kuģniecības, importa/eksporta, tekstilizstrādājumu, apģērbu, zvejniecības un/vai jūras produktu nozarē.
16. Klients uzstāj uz konfidencialitāti attiecībā uz darījumiem vai izrāda nepietiekamas rūpes par normatīvo aktu ievērošanu saistībā ar sankcijām un PF.
17. Darījumi ir saistīti ar uzņēmumiem, kuru uzņēmējdarbības reģistrācijā norādīts darbs pie "īpašiem mērķiem" paredzētiem projektiem.
18. Klientu pieprasījumi aizņemties personisko informāciju no kolēģiem līgumu noslēgšanai.
19. Klients veic darījumus ar precēm, kas nav saistītas ar tā parasto uzņēmējdarbību un var būt saistītas ar divējāda lietojuma iekārtām vai tehnoloģijām (piemēram, ķīmiskie reaktori, darbgaldi, raķešu sistēmu sastāvdaļas).

20. Klienta kontaktinformācija, piemēram, tālruņa numuri, neatbilst galamērķa valstij.
21. Klients atsakās sniegt bankām, nosūtītājiem vai trešajām personām sīkāku informāciju, tostarp informāciju par galalietotājiem, paredzēto galapatēriņu(-iem) vai uzņēmuma īpašumtiesībām.
22. Uzņēmumiem, kas kalpo kā nelikumīgu darbību aizsegs, trūkst klātbūtnes tiešsaistē, lai gan tie veic nozīmīgus darījumus.
23. E-pasta vai tīmekļa adrešu kiberizdomāšana, lai nelikumīgi pieprasījumi izskatītos kā no likumīgiem uzņēmumiem, bieži vien izmantojot zināmas darījumu attiecības.
24. IP adrese neatbilst klienta norādītajai atrašanās vietai.
25. Uzņēmuma nosaukums, kas ir pārāk vispārīgs, nav aprakstošs vai ir viegli sajaucams ar citas pazīstamākas juridiskās personas nosaukumu. Turklāt uzņēmuma nosaukumu var regulāri rakstīt dažādi.

2. Darījumi

1. Darījumi ietver mazāka apjoma maksājumus no viena un tā paša gala lietotāja ārvalstu bankas konta vairākiem līdzīgiem piegādātājiem.
2. Darījumi ietver pēdējā brīdī veiktas izmaiņas maksājumu maršrutā, kas iepriekš bija plānoti no attiecīgās valsts, bet tagad tiek novirzīti caur citu valsti vai uzņēmumu.
3. Aizliegta darījuma novirzīšana caur finanšu sistēmu, liekot finanšu iestādei apstrādāt maksājumus, pārkāpjot iekšzemes sankciju režīmu.
4. Līdzekļu plūsma starp uzņēmumiem var būt cikliska, vienam pārtraucot maksājumu, bet otram uzsākot maksājumu tam pašam saņēmējam.
5. Klients izmanto finanšu pakalpojumus un/vai veic darījumus, kas ir fiziski attālināti no faktiskās preču tirdzniecības.
6. Finanšu darījumu dokumentācijā ir izlaistas atsauces uz personām vai valstīm, uz kurām attiecas sankcijas.
7. Darījumi notiek caur valstīm vai finanšu centriem, par kuriem ir zināms, ka tiem ir vāja sankciju izpilde vai tie iesaistās nelikumīgās tirdzniecības shēmās.
8. Sarežģītu vai neparastu maksājumu ceļu izmantošana, tostarp vairāku finanšu iestāžu ķēdes, jo īpaši, ja tās šķērso valstis ar nepietiekamu PF kontroli vai sankcijām.
9. Darījumi, kuros maksājumiem izmanto atvērtus kontus/atvērtas kredītlīnijas saistībā ar zināmām pārkraušanas valstīm.
10. Pirkumi saskaņā ar akreditīvu, kas tiek nosūtīti izsniedzējai bankai, nevis faktiskajam galalietotājam.
11. Klienta pieprasījums izsniegt akreditīvu saistībā ar divējāda lietojuma precēm vai produktiem, uz kuriem attiecas eksporta kontrole, pirms tiek saņemts apstiprinājums konta atvēršanai.
12. Strauji pieaug noguldījumu atlikumi viņu noguldījumu kontos, kam seko skaidras naudas izņemšana, kas liecina par šādu darījumu veikšanas iespēju.
13. Klients uz ārzemēm pārskaita līdzekļus, kuru vērtība ir līdzīga nesen veiktajiem skaidras naudas noguldījumiem

14. Klienti norēķiniem par precēm izmanto privātpersonu kontus.
15. Daudzu bankas kontu izmantošana.
16. Skaidra pamatojuma trūkums tirdzniecības darījumam vai lielas summas samaksas iemeslam, jo īpaši, ja tas neatbilst klienta parastajai uzņēmējdarbībai.
17. Preču apjoms un vērtība neatbilst maksājumu apjomam.
18. Klients pieprasa maksājumu virtuālajos aktīvos, lai izvairītos no KYC/AML pasākumiem.
19. Pārskaitījumi, izmantojot virtuālo aktīvu pakalpojumu sniedzējus, jo īpaši, ja tie ir saistīti ar vāji regulētām valstīm vai ja tiek izmantotas decentralizētas biržas bez pienācīgas uzticamības pārbaudes.
20. Neoficiālu vai alternatīvu kanālu, piemēram, naudas pārvedumu sistēmu (hawala) izmantošana, ko var izmantot, lai apietu sankciju ierobežojumus.
21. Jaunu adrešu izveide virtuālajiem aktīviem, lai radītu "šķietamību", ka tie nav iesaistīti sankcijām pakļautās kriptovalūtu biržās.
22. Darījumi, kas saistīti ar maksājumiem par aizsardzības vai divējāda lietojuma precēm no uzņēmuma, kas reģistrēts pēc 2022. gada 24. februāra un atrodas valstī, kura nav Globālās eksporta kontroles koalīcijas (GECC) dalībvalsts.

3. Tirdzniecības darbības

1. Preces nosūtīšanas instrukciju maiņa, kad prece nonāk pie ekspeditora, bez eksportētāja ziņas.
2. Pēdējā brīža izmaiņas nosūtīšanas instrukcijās, kas ir pretrunā ar klientu vēsturi vai uzņēmējdarbības praksi.
3. Izmaiņas galīgā saņēmēja nosūtīšanas dokumentos vai galamērķa atrašanās vietā pirms nosūtīšanas vai tās laikā.
4. Klients pieprasa sūtījumu uz adresi, kas nav norādīta viņa identifikācijas dokumentos.
5. Eksportē produktu, kura kvalitāte neatbilst galamērķa valsts tehnoloģiskajam līmenim.
6. Darījums(-i) ietver preču sūtījumus, kas neatbilst parastajiem ģeogrāfiskās tirdzniecības modeļiem, t. i., ja iesaistītā valsts parasti neeksportē vai neimportē vai parasti nepatērē attiecīgo preču veidus.
7. Tirdzniecības darījumi, kas saistīti ar iekārtām vai materiāliem, kurus var izmantot militārās vai kodolprogrammās (piemēram, augstas stiprības sakausējumi, centrifūgas).
8. Kravas ekspeditora vai čarterlidmašīnas operatora kā tiešā lietotāja norādīšana.
9. Produkti tiek transportēti ar apvedceļu līdzekļiem, tostarp izmantojot mazu vai novecojušu kuģi.
10. Preces tiek piegādātas nelielos, biežos sūtījumos uz centrālo atrašanās vietu pirms to apvienošanas.

11. Darījumi ietver ekspeditoru uzņēmumus, kas darbojas augsta riska pārkraušanas zonās.
12. Iepirkumu novirzīšana caur pārkraušanas punktiem, ko parasti izmanto, lai novirzītu ierobežotas aprites preces uz galamērķiem, uz kuriem attiecas embargo.
13. Darījumi, kas saistīti ar netipiskiem produkta un galamērķa nosūtīšanas maršrutiem.
14. Ja ekspeditoru/muitošanas uzņēmums tirdzniecības dokumentos ir norādīts kā produkta galamērķis.
15. Ja preču galamērķa/nosūtīšanas valsts atšķiras no valsts, no kuras tiek nosūtīti/saņemti ieņēmumi, bez jebkāda ticama iemesla.
16. Kuģošanas dokumentu, piemēram, konosamentu un rēķinu, viltošana, lai slēptu kuģošanas maršrutus, uzkraušanas ostas, saņēmējus vai kuģniecības aģentus.
17. Preču, uz kurām attiecas sankcijas vai eksporta kontrole, nosaukumu aizstāšana, kā arī viltotu līgumu izmantošana, lai slēptu galalietotāju.
18. Pamatojošajos dokumentos, piemēram, faktūrrēķinā, nav norādīts faktiskais galalietotājs.
19. Nepareiza preču klasifikācija dokumentācijā, lai izvairītos no atklāšanas, piemēram, ierobežotas pieejamības preču apraksti, kas nav sensitīvi.
20. Neatbilstības starp informāciju tirdzniecības, transporta un finanšu dokumentos. Piemēram, neatbilstības starp rēķiniem un informāciju par sūtījumu (preču veids, svars, vērtība, galamērķis).
21. KTDR eksportētāji slēpj KTDR ražoto preču izcelsmi, piestiprinot izcelsmes valsts marķējumu, kurā norāda trešo valsti.
22. Trešo valstu piegādātāji pārvieto ražošanu vai apakšuzņēmuma darbu uz KTDR rūpnīcu, neinformējot par to klientu vai citas attiecīgās personas.
23. Tirdzniecības kuģi, kas kuģo ar KTDR karogu, ir fiziski pārveidoti, lai slēptu to identitāti un izliktos par citiem kuģiem.
24. Luksusa preces bieži tiek sūtītas uz centrālajām noliktavām trešajās valstīs.
25. Strauja pāreja pie jauniem pircējiem darījumos, kas saistīti ar ierobežotas pieejamības luksusa precēm.
26. Būvmateriālu iegāde un piegāde.
27. Būtiska finansiāla darbība, kas nav saistīta ar norādīto uzņēmējdarbības mērķi, piemēram, maksājumi, kas nav saistīti ar tekstilrūpniecību, zivsaimniecību vai ogļu eksportu.
28. Klienti, kas ir ražošanas vai tirdzniecības uzņēmumi, izmanto skaidru naudu darījumos, kas saistīti ar rūpniecības produktiem vai citiem tirdzniecības darījumiem.
29. Vai deklarētā kravas cena ir zema salīdzinājumā ar transportēšanas izmaksām.
30. Kuģa reģistrācijas karogs tiek bieži mainīts.
31. FTZ iesaistīšana, ko var izmantot, lai slēptu sensitīvu preču izcelsmi un apriti.