12. Massihävitusrelvade leviku rahastamise riskide analüüs

12.1. Massihävitusrelvade levik ja selle rahastamine

Massihävitusrelvad (edaspidi MHR) ja nende leviku võimaldajad kujutavad endast olulist ohtu rahvusvahelisele julgeolekule. Seetõttu on rahvusvaheline üldsus leppinud kokku selliste ohtlike relvade leviku vastu ülemaailmses võitlemises. MHR vastase võitlusega seondub ka nende rahastamine. Käesoleva riskihinnangu raames vaadeldakse lähemalt MHR leviku rahastamise võimalusi Eesti finantssüsteemi või ettevõtluskeskkonda ära kasutades.

FATFi mõistes on MHR leviku rahastamine rahaliste vahendite või finantsteenuste osutamine, mida kasutatakse täielikult või osaliselt tuumarelvade, keemiliste või bioloogiliste relvade ning nende kohaletoimetamise viiside ja nendega seotud materjalide (sealhulgas nii tehnoloogiad kui ka ebaseaduslikel eesmärkidel kasutatavad kahesuguse kasutusega kaubad) tootmiseks, omandamiseks, valdamiseks, arendamiseks, ekspordiks, ümberlaadimiseks, vahendamiseks, transpordiks, ülekandmiseks, varumiseks või kasutamiseks, rikkudes siseriiklikke seaduseid või riigi rahvusvahelisi kohustusi.[1]

Käesoleva riskihindamise raames keskendutakse FATFi soovitusest nr 1 tulenevalt MHR leviku rahastamisele, mis on FATFi soovituses nr 7 viidatud finantssanktsioonide tegelik või võimalik rikkumine, kohaldamata jätmine või vältimine. Euroopa Liidus (EL), mis on FATFi soovituse nr 7 kohaselt rahvusvaheline jurisdiktsioon, külmutatakse määratletud isikute ja üksuste vara vastavalt ELi määrustele ja nende muudatustele[2]. EL avaldab sanktsioonialuste füüsiliste ja juriidiliste isikute, üksuste ja asutuste nimekirja (edaspidi ka „*määratletud isikud ja üksused*“) ka konsolideeritud ja masintöödeldaval kujul.[3] Mõiste „strateegiline kaup“ hõlmab Eesti õiguse kohaselt nii sõjalisi kaupu kui ka kahese kasutusega kaupu.[4]

FATFi soovitus nr 7 räägib kahest sanktsioonirežiimist: Korea Rahvademokraatliku Vabariigi (*KRDV,* ingl. k. *DPRK*)[5] ja Iraani[6] vastu kehtestatud meetmetest, mis nõuavad, et riigid peavad viivitamatult külmutama rahalised vahendid ja muu vara, mis kuulub mõnele isikule või üksusele, kes on määratletud ÜRO Julgeolekunõukogu poolt või volitusel vastavalt ÜRO põhikirja VII peatükile, ning samuti tagama, et rahalisi vahendeid ega muud vara ei tehta otseselt või kaudselt kättesaadavaks ühelegi sellisele isikule või üksusele.

FATFi metoodika kohaselt võib seetõttu tekkida MHR leviku rahastamise risk:

A) finantssanktsioonide rikkumisest või kohaldamata jätmisest: kui määratletud isikud või üksused omavad ligipääsu finantsteenustele, vahenditele või varale näiteks ebapiisava kommunikatsiooni, selgete kohustuste puudumise või finantsasutuste ning mittefinantsteenuseid osutavate määratletud asutuste ja isikute poolt mitteadekvaatsete protseduuride rakendamise tõttu (näiteks nõrk taustakontroll ärisuhte loomisel, või ärisuhte monitoorimisel, töötajate ebapiisav teadlikkus, riskide ebakohane juhtimine, sanktsioneeritud isikute nimekirjade jälgimise ebapiisavad süsteemid või üldine kehv vastavuskontrolli tase/kultuur).
B) finantssanktsioonide vältimisest või vältimise võimaldamisest: kui määratletud isikud või üksused teevad pingutusi finantssanktsioonide kohaldamise alt pääsemiseks (näiteks kasutavad vari- või riiulifirmasid, tankiste või seaduste rakendamisest hoiduda aitavaid vahendajaid- nõustajaid).

[1] Combating Proliferation Financing: A Status Report on Policy Development and Consultation
[2] Siin ja edaspidi on metoodiliselt lähtutud FATFi juhendmaterjalide tööpaberitest
[3] https://data.europa.eu/euodp/en/data/dataset/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions
[4] Vt strateegilise kauba seaduse § 2 lg 1.
[5] Resolutsioon 1718 (2006) ja sellele järgnevate resolutsioonide puhul Julgeolekunõukogu poolt asjaomaste resolutsioonide lisades või Julgeolekunõukogu 1718 sanktsioonide komitee poolt.
[6] resolutsiooni 1737 (2006) ja sellele järgnevate resolutsioonide puhul Julgeolekunõukogu poolt asjaomaste resolutsioonide lisades või Julgeolekunõukogu 1737 sanktsioonide komitee poolt, kui need komiteed tegutsevad ÜRO põhikirja VII peatüki alusel.

ÜRO Julgeolekunõukogu on eelnevalt nimetatud sanktsioonirežiimide rakendamiseks kehtestanud spetsiifilised kohustused seoses MHR programmidega seonduvate tegevuste rahastamisega.

1. Liikmesriigid peavad võtma vajalikud meetmed, et ennetada finantsteenuste osutamist või –abi KRDV-le või Iraanile, seonduvalt vastavate otsustega[7] keelatud esemete, materjalide, seadmete, kaupade ja tehnoloogia pakkumise, tarnimise, müümise, üleandmise, tootmise, hooldamise või kasutamisega.
2. Finantssanktsioonide kohaldamine isikute ja ühenduste suhtes[8], kes toetavad KRDV või Iraani MHR-seonduvaid tegevusi ja programme.
3. Liikmesriike kutsutakse üles takistama mis tahes muude finantsteenuste osutamist või selliste rahaliste või muude varade või ressursside ülekandmist, mis võiksid aidata kaasa KRDV ja Iraani MHR leviku suhtes tundlikele programmidele ja tegevustele[9].
4. Liikmesriike kutsutakse üles mitte võtma uusi kohustusi või andma toetusi, finantsabi või laene KRDV-le või Iraanile, välja arvatud humanitaar- ja arenguabi eesmärkidel.[10]
5. Liikmesriike kutsutakse üles mitte pakkuma rahalist toetust kaubavahetuseks KRDV-ga või, Iraani puhul, rakendama valvsust avaliku sektori rahalise toetuse andmise kohustuste täitmisel, et vältida sellist rahalist toetust, mis aitab kaasa tuumategevusele või tuumarelvade levikule või nende arendamisele.[11]

Samas on Iraani režiimi puhul oluline märkida, et resolutsioon 1737 (2006) on tunnistatud kehtetuks resolutsiooniga 2231 (2015).[12] Resolutsiooniga 2231 lõpetati varem kehtestatud tuumarelvastusega seotud sanktsioonid ja kehtestati konkreetsed piirangud:
• relvadega seotud ülekannetele Iraani ja Iraanist, mis pidid lõppema 2020. aastal;
• ballistiliste rakettidega seotud ülekannetele ning seonduvate tegevuste ja varade külmutamine, mis peaksid aeguma 2023. aastal; ja
• tuumarelvadega seotud ülekannetele ja tegevustele, mis peaksid aeguma 2025. aastal.

Vastavalt resolutsioonile 2231 sõltub nende piirangute lõppemine sellest, kas Iraan täidab Ühise Tervikliku Tegevuskava (inglisekeelne lühend *JCPOA*) kohaseid kohustusi. 2020. aasta jooksul leiti korduvaid rikkumisi, kuid ÜRO julgeolekunõukogu ei leppinud kokku ka meetmete pikendamises.[13] Seetõttu tuleb Iraani puhul lähtuda eeskätt kehtivatest piirangutest seoses ballistiliste rakettidega ning tuumarelvadega seotud ülekannete ja tegevuste piirangust, tuginedes juriidiliselt ELi kehtestatud piiravatele meetmetele[14]. Lisaks tuleks meeles pidada, et ELi kehtestatud täiendavad piiravad meetmed seoses Iraani inimõiguste olukorraga, terrorismi toetamisega ja muudel põhjustel (nt sõda Süürias) ei kuulu JCPOAsse ja jäävad kehtima. Samas ei kuulu viimatinimetatud käesoleva riskihindamise skoopi, kuivõrd tegemist ei ole Iraani sanktsioonirežiimiga FATFi soovituse nr 7 mõistes.

12.2. Riskide hindamine

MHR leviku piiramiseks ja sellega seonduvate rahaliste vahendite kogumisest, hoidmisest, liigutamisest ja kasutamisest hoidumiseks on vaja hinnata sellise tegevuse riske. MHR leviku rahastamise risk on kombinatsioon ohust, haavatavusest ja selle realiseerumisel kaasnevatest tagajärgedest. Riskide hindamiseks tuleb kindlaks teha nii omane risk kui ka jääkrisk.

a. Omane risk viitab loomulikule riskitasemele, mis on enne riske maandavate meetmete rakendamist. Omane risk on riigi puhul näiteks geograafiline lähedus MHR riigile, või kahese

[7] S/RES/1874(2009); S/RES/1718(2006); S/RES/1737(2006); S/RES/1747(2007); S/RES/1929(2010)
[8] S/RES/1718(2006); S/RES/1737(2006); S/RES/1747(2007); S/RES/1929(2010).
[9] S/RES/1874(2009); S/RES/1929(2010).
[10] S/RES/1874(2009); S/RES/1747(2007).
[11] S/RES/1874(2009); S/RES/1803(2008).
[12] http://www.undocs.org/S/RES/2231(2015)
[13] Vt Eesti selgitust oma häälele: https://un.mfa.ee/estonian-explanation-of-vote-in-connection-with-agenda-item-non-proliferation/
[14] Kehtivatest sanktsioonidest ülevaate saamiseks on olemas mugav rakendus: https://www.sanctionsmap.eu/#/main

kasutusega või MHR-seonduvate kaupade tootmine riigis ja seonduv kaubavahetus, nagu ka augud ÜRO Julgeolekunõugogu resolutsioone kohaldavas õigusraamistikus.

b. Jääkrisk viitab riski tasemele, mis jääb pärast riskimaandamismeetmete kohaldamist. Jääkriski mõistmine annab tunnetuse selle kohta, kas riik (või erasektori asutus) suudab maandada MHR rahastamise riske. Kõrge tasemega jääkrisk viitab, et kontrollimeetmed on ebaadekvaatsed ja riik peaks rakendama täiendavaid meetmeid riski maandamiseks. Käesolevas peatükis on jääkriski kirjeldatud koos ettepanekutega meetmete võtmiseks.

MHR rahastamise riski hindamise spetsiifika:

a. OHT viitab määratletud isikutele ja üksustele, kes potentsiaalselt tekitavad või on minevikus tekitanud kahju vältides või rikkudes MHR või finantssanktsioone. See võib olla tegelik või potentsiaalne oht. Kõik ohud ei kujuta kõigile riikidele ja erasektori ettevõtetele ühesugust riskitaset.
b. HAAVATAVUS viitab asjaoludele, mida oht saab ära kasutada või mis võivad MHR või finantssanktsioonide rikkumist, rakendamata jätmist või sellest kõrvalehoidmist toetada või hõlbustada. Riigi jaoks võivad need haavatavused hõlmata nõrkusi seadustes või määrustes, mis hõlmavad riigi MHR rahastamise tõkestamise režiimi, või riigi kontekstilisi omadusi, mis võivad pakkuda määratletud isikutele ja üksustele võimalusi koguda või liigutada rahalisi vahendeid või muud vara. Näiteks jurisdiktsioon, millel on nõrk rahapesuvastase võitluse / terrorismi rahastamise tõkestamise regulatsioon või mis ei kogu enda riigi seaduse kohaselt asutatud äriühingute tegelike kasusaajate kohta andmeid. Erasektori ettevõtete jaoks võivad haavatavused hõlmata konkreetse sektori, finantstoote või teenuse tüübi omadusi, mis muudavad need atraktiivseks MHR rahastamise rikkumise, rakendamata jätmise või sellest kõrvalehoidmisega tegeleva isiku või üksuse jaoks. Näiteks kliendibaas, mis koosneb väikestest kaubandusettevõtetest, mis asuvad teadaolevalt MHR-ga seotud jurisdiktsioonides, kujutab endast haavatavust erasektori ettevõtja jaoks.
c. TAGAJÄRG. viitab tulemusele, kus rahalised vahendid või varad tehakse kättesaadavaks määratletud isikutele ja üksustele, et võimaldada neil hankida vajalikke materjale, esemeid või süsteeme ebaseaduslike tuuma-, keemiliste või bioloogiliste relvasüsteemide (või nende kandevahendite) arendamiseks ja hooldamiseks või kus määratletud isikute või üksuste külmutatud varasid kasutataks tuumarelva leviku rahastamiseks. Tuumarelvade leviku tõkestamise rahastamise, st massihävitusrelvade kasutamise tagajärg on raskem kui rahapesu või muude finantskuritegude puhul ning sarnaneb rohkem terrorismi rahastamise tagajärgedega seotud võimaliku inimkaotusega. Tõenäoliselt on see riikide, kanalite või allikate lõikes erinev.

12.3. Massihävitusrelvade rahastamise oht

Kuna massihävitusrelvade rahastamise toimepanemise võimalusi on mitmeid, on ohu tuvastamiseks mõistlik fokusseerida tähelepanu tõenäolisematele ja rahvusvahelistele trendidele vastavatele ohtudele viitavatele asjaoludele. ÜRO julgeolekunõukogu resolutsioonide täitmise kontrollimiseks ellu kutsutud komiteed[15] on avaldanud raporteid ja ülevaateid, mis toovad välja sanktsioneeritud isikute nimekirjadesse kantud isikute ja üksuste viimaste aastate toimimisviisid, millega on neil õnnestunud sanktsioonirežiime vältida või rikkuda.

Massihävitusrelvade rahastamise riski puhul võib eristada Eesti jaoks olulisematena kahte suunda: santsioonireziimi rikkumine läbi võimaliku MHR transiidi, kasutades Eesti territooriumi või siin asutatud ettevõtteid; sanktsioonide vältimine läbi virtuaalvääringute teenusepakkujate sektori.

[15] Reports of the Panels of Experts (PoE) UNSCR 1718 (2006); UNSCR 1874 (2009)

12.3.1. MHR transiidi rahastamise oht

Seni pole meie territooriumil esinenud teadaolevalt juhtumeid, kus kellelgi oleks tuuma-, bioloogilist, radioaktiivset või keemilist materjali õnnestunud ebaseaduslikult MHR valmistajatele tarnida.

Massihävitusrelvade komponendid – mitmesugused mürgid, keemiarelva lähteained või lõhkeained – on esitatud Euroopa Liidu sõjaliste kaupade nimekirjas. Näiteks ML7: "Keemilised toimeained, „bioltoimeained", „massirahutuste ohjamiseks mõeldud keemilised ühendid", radioaktiivsed materjalid, nendega seotud varustus, komponendid ja materjalid" ja ML8: „Kõrge siseenergiaga materjalid ja nendega seotud ained". Kahese kasutusega kaupade nimekirjast võib leida näiteks tuumamaterjalid, -rajatised ja -seadmed. Eesti massihävitusrelvi ega selleks vajaminevaid tehnoloogiaid või kaupu ei tooda.

Tulenevalt kehtivast EL ja Eesti regulatsioonidest ning Eesti paiknemisest geograafiliselt MHR transiiditeedest veidi eemal, on massihävitusrelvade transiidi Eesti kaudu rahastamise tõenäosus keskmisest madalam. Teisalt ei tähenda massihävitusrelvadega seonduva transiidi geograafia, et transiidi rahastamise oht oleks Eestis automaatselt madal, kuivõrd rahastamiseks võidakse kasutada piiriüleselt osutatavaid finants- ja finantstehnoloogia-teenuseid.

Eestil on aastatel 2017-2020 puudunud igasugune kaubavahetus Põhja-Koreaga[16].

Eesti on aastatel 2017-2020 eksportinud Iraani peamiselt puitu ja puidumaterjale, turvast ja ravimeid, vähemal määral masinaid ja seadmeid. Ekspordimahud on langustrendis (2017: 5,32M €; 2018: 3,58M €; 2019: 1,44M €).[17]

Vaadeldes rahastamise trende, on ÜRO JN KRDV sanktsioonirežiimi ekspertide komitee (panel of experts ehk *PoE*) leidnud, et Korea Rahvademokraatlik Vabariik omab jätkuvalt juurdepääsu rahvusvahelisele finantssektorile erinevate ühisettevõtete, *offshore* - kontode, varifirmade ja virtuaalsete varade kaudu. Analüüside tulemused näitavad, et KRDV kasutab seotud üksuste ja isikute kaudu jätkuvalt Ida- ja Kagu-Aasia pangandussüsteeme ja sellekaudu laiemalt rahvusvahelist korrespondentpangandust. PoE on ka liikmesriike kritiseerinud ebapiisavate pingutuste eest siseriiklike äriühingute registreerimise reeglite kehtestamisel, mis on võimaldanud jätkuvalt KRDV-l kasutada ära läbipaistmatuid ettevõtete struktuure. Lüngad ettevõtete registreerimise kontrollimehhansimides muudavad tunne-oma-klienti protsessid ja protseduurid finantsasutustes praktiliselt võimatuks.[18]

Iraani suhtes ei ole resolutsiooni 2231 suhtes samaväärselt trende ja mustreid analüüsitud, ÜRO liikmesriigid on teavitanud üksikutest võimalikest sanktsioonirežiimi rikkumistest, s.h võimalikust finantseerimistegevusest.[19] Iraaniga seonduva kaubavahetuse piiratuse tõttu, samuti Eestis tuumarelvade- ja vastava tehnoloogiasektori puudumise tõttu seonduvad sanktsioonirežiimi rikkumisega seega peamiselt ohud, millega sanktsiooninimekirjadesse kantud isikud ja üksused üritavad sooritada tehinguid Eesti ettevõtetega või nende kaasabil.

12.3.2. MHR rahastamise oht läbi virtuaalvääringute teenusepakkujate sektori

KRDV on viimastel aastatel pööranud suurt tähelepanu virtuaalse vara (krüptovara) pakkujate, näiteks virtuaalvääringu vahetamise teenusepakkujate ärakasutamisele ÜRO JN sanktsioonidest kõrvalehoidmiseks. PoE tõstis oma 2019.[20] ja 2020. aasta aruannetes[21] esile mitmeid taktikaid ja tehnikaid, mida KRDV kasutab, mille sihiks on ebaseaduslik virtuaalvääringute kogumine, kaevandamistegevused, sealhulgas keerukaid tehnoloogilisi toiminguid ja pahavara rakendades. Selge vastuseta on küsimus, kuidas KRDV seejärel oma virtuaalse vara tavavaluutaks konverteerib.

[16] https://valiskaubandus.stat.ee/profile/country/ee/
[17] https://valiskaubandus.stat.ee/visualize/tree_map/export/ir/all/2019/?locale=et
[18] https://undocs.org/S/2020/840
[19] https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2020_531.pdf
[20] https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_691.pdf
[21] https://undocs.org/S/2020/840

KRDV on alates 2019. aasta maist suurendanud oma Monero kaevandustegevust vähemalt kümnekordseks (võrreldes bitcoini kaevandamisele samal perioodil). Monero on virtuaalne valuuta, mis sarnaneb bitcoiniga, kuid pakub täiendavat anonüümsust ja ei vaja kaevandamiseks tingimata sama suure jõudlusega arvuteid.[22]

PoE-le on teatatud 2019. aastaks vähemalt 35 juhtumist, kus KRDV päritolu isikud on toime pannud küberrünnakuid finantsasutuste, virtuaalvääringu vahetajate ja kaevandajate vastu, eesmärgiga varastada virtuaalvääringuid tulu saamiseks. Selleks, et tehingute jälgitavust piirata, kasutab KRDV sarnaselt rahapesijatega erinevaid digitaalseid vara kihistamismeetodeid, näiteks loovad tuhandeid virtuaalvääringu rahakotte erinevate teenusepakkujate juures. 2019. a jooksul suundus KRDV rünnete teravik veelgi enam virtuaalvääringu vahetusplatvormide vastu, seejuures on mõned virtuaalvääringu vahetusplatvormid olnud rünnaku ohvriteks korduvalt ning pidanud seetõttu ka tegevuse lõpetama[23].

12.4. MHR rahastamise haavatavus

12.4.1. MHR rahastamise üldine haavatavus

Eestis on toimiv ja rahvusvahelistele nõuetele vastav regulatsioon ja määratud vastutavad asutused. Kaitsepolitseiameti ülesanne on massihävitusrelvade ja nende komponentide ebaseadusliku käitlemise avastamine ning tõkestamine. Sõjaliste ja kahese kasutusega kaupade eksportkontrolli tehakse koostöös Välisministeeriumi juures tegutseva Strateegilise Kauba Komisjoni ning Maksu- ja Tolliametiga. Oluline on prioritiseerida strateegilise kauba komisjoni ja selle liikmete aktiivset koostööd RAB-ga ja Eestis tegutsevate pankadega, et massihävitusrelvade rahastamise kahtluse korral tõhustada informatsiooni vahetamist litsentse taotlevate või potentsiaalselt ebaseaduslikke vedusid teostavate isikute ja firmade finantstehingute kohta.

Rahvusvaheliselt on Eesti kaasatud erinevatesse massihävitusrelvade vastu võitlevatesse organisatsioonidesse: NATO ja ELi vastavad formaadid, IAEA (International Atomic Energy Agency), OPCW (Organisation for the Prohibition of Chemical Weapons), Austraalia Grupp (The Australia Group), NSG (Nuclear Supplies Group), Wassenaari kokkulepe (Wassenaar Agreement) jne. Eesti on aastatel 2020-2021 ÜRO Julgeolekunõukogu valitud liige, olles sel ajal kahel korral ka Julgeolekunõukogu eesistuja: 2020. aastal (kevadel) ja 2021. aastal (suvel).

Eestis rakendatakse rahvusvahelisi sanktsioone läbi Euroopa Liidu õigusaktide. Euroopa Liidu Nõukogu on Euroopa Liidu üks peamisi otsustusõiguslikke kehandeid, mis võtab vastu õigusakte, sõlmib lepinguid ning kujundab EL ühist välis- ja julgeolekupoliitikat. Nõukogu istungitel kohtuvad ELi liikmesriikide ministrid, kel on õigus oma riigi valitsuse nimel kohustusi võtta ja vajadusel hääletada.

Osana EL ühisest välis- ja julgeolekupoliitikast kehtestab nõukogu ka sanktsioone ehk piiravaid meetmeid. Ühise välis- ja julgeolekupoliitika teostamiseks võtab Euroopa Liidu Nõukogu vastu otsuseid, tuginedes Euroopa Liidu lepingu artiklile 29. Nimetatud otsusega kehtestatakse kohustusi, keelde ja piiranguid kas ELi liikmesriikidele või ELi füüsilistele ja juriidilistele isikutele. Liikmesriigid rakendavad näiteks selliseid levinud sanktsioonitüüpe nagu sissesõidukeeld ja relvaembargo – Eestis vastavalt väljasõidukohustuse ja sissesõidukeelu seaduse ning relvaseaduse alusel.

Ülaltoodud otsusega kehtestatud keelud ja piirangud, mis kohustavad ELi füüsilisi ja juriidilisi isikuid, on reguleeritud ELi Nõukogu otsekohalduvates määrustes, millel on liikmesriikide riigisiseste õigusaktidega sarnane mõju. Seega võetakse ELi sanktsioonirežiimides vastu kaks ühise välis- ja julgeolekupoliitika õigusakti – otsus, kus sisalduvad kõik kehtestatud meetmed ning määrus, mis reguleerib füüsiliste ja juriidiliste isikute kohustusi.

[22] Näiteks WannaCry ohvrite tehtud Bitcoini lunaraha maksed kanti üle Bitcoini rahakottidesse ja lõpuks konverteeriti Monero'ks, kasutades Šveitsi virtuaalvääringuvahetusplatvormi ShapeShift.
[23] Youbit (endine Yapizon) langes 2017. a aprillis korduvate küberrünnete alla, kaotades $4.8 M, ja täiendavalt detsembris 2017 kogu varadest 17%, olles sellega sunnitud oma tegevuse lõpetama.

Nagu ülal viidatud, on ELi Nõukogu otsekohalduvates määrustes toodud kohustustel, keeldudel ja piirangutel riigisiseste õigusaktidega sarnane mõju. Rahvusvahelise sanktsiooni kohaldamist Eestis reguleerib rahvusvahelise sanktsiooni seadus (edaspidi RSanS) ning sanktsioonirikkumine on reguleeritud karistusseadustiku §-s 93[1], mille kohaselt karistatakse sanktsioonikohustuse täitmata jätmise või keelu rikkumise eest rahalise karistuse või kuni viieaastase vangistusega.

Ülevaatlik info kehtivate sanktsioonide kohta koos linkidega vastavatele õigusaktidele on kättesaadav Eesti Euroopa Liidu Nõukogu eesistumise raames arendatud ELi sanktsiooniveebist.[24]

Vastavalt rahvusvahelise sanktsiooni seadusele teostab seaduse nõuete täitmise üle järelevalvet ja on pädevaks asutuseks Rahapesu Andmebüroo, kelle kodulehel[25] on kättesaadav nii ülevaade sanktsioonidest kui ka sanktsioneeritud isikute kohta otsingu teostamise võimalus. Alates 1. jaanuarist 2021 teostab Finantsinspektsioon finantssanktsioonide kohaldamise järelevalvet nende krediidiasutuste ning finantseerimisasutuste poolt, kes kuuluvad tema järelevalve alla.

KRDV suhtes on EL-s kehtestatud nõukogu otsus (ÜVJP) 2016/849[26] ja nõukogu määrus (EL) 2017/1509[27]. Alates 2016. aastast on EL otsustanud lisaks ÜRO Julgeolekunõukogu resolutsioonidest tulenevatele meetmetele rakendada täiendavaid lisameetmeid KRDV suhtes, kuna viimatinimetatu tegevus kujutab tõsist ohtu rahvusvahelisele rahule ja julgeolekule piirkonnas ja mujal. Täiendavaid piiravaid meetmeid peeti vajalikuks, et veelgi suurendada KRDV-le survet oma rahvusvaheliste kohustuste täitmiseks. EL on otsustanud võidelda massihävitusrelvade leviku tõkestamise vastu ning on pühendunud Korea poolsaare tuumarelva-vabaks muutmisele, sealhulgas uute piiravate meetmete kaalumise kaudu.

16. jaanuaril 2016 tühistas EL kõik Iraani tuumaprogrammiga seoses kehtestatud majanduslikud ja rahalised piiravad meetmed. Seetõttu on alates sellest päevast taas lubatud järgmised tegevused, sealhulgas nendega seotud teenused: finants-, pangandus- ja kindlustusmeetmed; kaubandus nafta-, gaasi- ja naftakeemiasektoris; tegevus laevanduses, laevaehituses ja transpordisektoris. Lisaks eemaldati isikuid, üksusi ja asutusi sanktsiooninimekirjadest ning seetõttu ei pea enam kohaldama nende varade külmutamist, rahaliste vahendite kättesaadavaks tegemise keeldu ja viisakeelde[28]. Mitmed massihävitusrelvade levitamisega seotud meetmed ja piirangud jäid edasi kehtima. Need käsitlevad muu hulgas relvaembargot, raketitehnoloogiaga seotud piiravaid meetmeid, teatavate tuumarelvadega seotud ülekannete ja tegevuste piiranguid ning sätteid, mis käsitlevad teatavaid metalle ja tarkvara, mille suhtes kehtib autoriseerimiskord. Kehtivate meetmete õiguslikuks aluseks on nõukogu otsus 2010/413/ÜVJP[29] ning nõukogu määrus (EL) nr 267/2012[30].

On kindlaks tehtud, et määratletud isikud ja üksused kasutavad oma skeemide elluviimiseks varifirmade võrgustikke. Hoolsusmeetmete rakendamata jätmine (nt ärisuhtest arusaamise kohustus ja ettevõtete tegelike kasusaajate väljaselgitamise kohustus), võib viia selliste üksuste või isikute tehingutes osalemise avastamata jätmiseni, mis toob kaasa sanktsioonirežiimi rikkumise. Varifirmade ning määratletud isikute ja üksuste nimel tegutsevate vahendajate kasutamine muudab tehingute jälgimise keerukaks. Eesti juriidiliste isikute haavatavused[31] on asjakohased ka massihävitusrelvade leviku rahastamise aspektist, eriti asjaolu, et juriidiliste isikute tegelike kasusaajate üle teostatav kontroll on praktikas puudulik.

Rahvusvahelise sanktsiooni seaduses on kehtestatud, et finantssanktsiooni kohaldavad muu hulgas ka:

[24] https://vm.ee/et/rahvusvahelised-sanktsioonid
[25] https://www.fiu.ee/rahvusvahelised-sanktsioonid/rahvusvahelised-finantssanktsioonid
[26] Nõukogu otsus (ÜVJP) 2016/849, 27. mai 2016, mis käsitleb Korea Rahvademokraatliku Vabariigi vastu suunatud piiravaid meetmeid ja millega tunnistatakse kehtetuks otsus 2013/183/ÜVJP, ELT L 141 28.5.2016, lk 79.
[27] Nõukogu määrus (EL) 2017/1509, 30. august 2017, mis käsitleb Korea Rahvademokraatliku Vabariigi vastu suunatud piiravaid meetmeid ja millega tunnistatakse kehtetuks määrus (EÜ) nr 329/2007, ELT L 224 31.8.2017, lk 1.
[28] https://eeas.europa.eu/delegations/iran/32286/nuclear-agreement_en#JCPOA+Information+Note
[29] Nõukogu otsus 2010/413/ÜVJP, 26. juuli 2010, mis käsitleb Iraani vastu suunatud piiravaid meetmeid ning millega tunnistatakse kehtetuks ühine seisukoht 2007/140/ÜVJP, ELT L 195 27.7.2010, lk 39.
[30] Nõukogu määrus (EL) nr 267/2012, 23. märts 2012, milles käsitletakse Iraani vastu suunatud piiravaid meetmeid ja millega tunnistatakse kehtetuks määrus (EL) nr 961/2010, ELT L 088 24.3.2012, lk 1.
[31] vt käesoleva NRA riiklike haavatavuste peatüki jaotist 2 Juriidiliste isikute ärakasutamise analüüs

- Eestis kehtivate Euroopa patentide register[32];
- kasulike mudelite register[33];
- kauba- ja teenindusmärkide register[34];
- kinnistusraamat[35];
- laevakinnistusraamat[36];
- mittetulundusühingute ja sihtasutuste register[37];
- patendiregister[38];
- riiklik liiklusregister[39];
- tööstusdisainilahenduste register[40];
- Eesti väärtpaberite register[41];
- õhusõidukite register[42];
- äriregister[43].

Registripidaja keeldub tegemast finantssanktsiooni rikkuvat kannet ning määrab isiku, kes korraldab oma pädevuse piires finantssanktsiooni rakendamist, ja edastab tema kontaktandmed Rahapesu Andmebüroole. Arvestades, et tulevikus ei ole tegelike kasusaajate register äriregistri osa, vaid muutub eraldi andmekoguks, mille vastutav töötleja on Rahandusministeerium ning volitatud töötlejateks Tartu Maakohtu Registriosakond ning Riigi Infosüsteemide Keskus, siis tuleks rahvusvahelise sanktsiooni seadust täiendada nii, et ka tegelike kasusaajate registripidajal oleks kohustus finantssanktsioone kontrollida ja neid rikkuvate kannete korral tagada Rahapesu Andmebüroo kohene teavitamine. Tegeliku kasusaaja kanne ei loo küll automaatselt õigusi ega too kohustusi, kuid määratletud isikute ja üksuste kandmine tegelike kasusaajatena (seal hulgas tegelike kontrollijatena) Eesti juriidiliste isikute andmetesse viitab sanktsioonirežiimi rikkumisele.

Kooskõlas asjakohaste ÜRO Julgeolekunõukogu resolutsioonidega tõkestatakse riiklikul tasandil raha kogumist, liigutamist ja kasutamist isikute ja üksuste poolt, kes on seotud massihävitusrelvade levitamisega. Kuigi koordineerimistegevused antud valdkonnas on viimastel aastatel olnud hinnatud ebapiisavateks, on 2020. a lõpu seisuga nii sanktsioonide kui massihävitusrelvade rahastamisega seonduvate ÜRO resolutsioonide riigisisese rakendamise hõlbustamiseks ellu kutsutud Välisministeeriumi juures tegutsev töörühm. Teisalt on haavatavust suurendavaks aspektiks juriidiliste isikute võimalik ärakasutamine sanktsioneeritud isikute poolt, kuivõrd juriidiliste isikute tegelikke kasusaajaid sanktsioneeritud isikute nimekirjade osas ei kontrollita. Kui juriidiline isik ei ole kliendisuhtes kohustatud isikuga, kellel on kohustus ka iseseisvalt kliendi tegelikke kasusaajaid (s.h sanktsioonide osas) hoolsusmeetmete rakendamisel kontrollida, võib juhtuda, et sanktsioneeritud isikute nimekirja kuuluva tegeliku kasusaajaga juriidilist isikut ei tuvastata õigeaegselt.

Hinnang haavatavusele on seega kokkuvõttes **madal-keskmine**.

[32] https://www.epa.ee/et/patendid/eestis-kehtivate-euroopa-patentide-register
[33] https://www.epa.ee/et/kasulikud-mudelid/registreerimine
[34] https://www.epa.ee/et/kaubamargid/kaubamargi-registreerimine
[35] https://www.rik.ee/et/e-kinnistusraamat
[36] https://laevakinnistusraamat.rik.ee/
[37] https://www.just.ee/et/eesmargid-tegevused/ari-ja-uhinguregister
[38] https://www.epa.ee/et/patendid/toimingud-eesti-patendiregistris
[39] https://eteenindus.mnt.ee/main.jsf?lang=et
[40] https://www.epa.ee/et/toostusdisainilahendused/toimingud-toostusdisainilahenduste-registris
[41] https://nasdaqcsd.com/et/teenused/teenused-emitendile/vaartpaberiomanike-nimekiri/
[42] https://www.ecaa.ee/et/lennundustehnika-ja-lennutegevus/ohusoidukite-register
[43] https://www.just.ee/et/eesmargid-tegevused/ari-ja-uhinguregister

12.4.2 Sektroriaalsed haavatavused

12.4.2.1. Finantssektor

Peamisteks ohuallikateks on finantssektori kaudu finantseeritavad ja/või arveldavad majandussubjektid, keda võidakse suhteliselt madala teadlikkuse tõttu nende endi teadmata ära kasutada massihävitusrelvade transiidi rahastamiseks. Finantssektori-spetsiifiline oht esineb eelkõige vahendustehingutes, kus kaup ei pruugi läbi Eesti liikuda, aga finantseerimine toimub krediidiasutuste poolt või teostatakse makseid, kasutades Eesti finantsasutusi.

Lähiminevikus on kogu fookus teadlikkuse tõstmisel olnud rahapesul ja terrorismi rahastamisel. Seetõttu on massihävitusrelvade ja kahesuguse kasutusega kauba temaatika saanud oluliselt vähem avalikkuse tähelepanu ning teavitustegevus finantssektorile on olnud tagasihoidlikum. Samas massihävitusrelvade levitamise rahastamise tõenäosust Eesti kaudu võib pidada väga madalaks, kuivõrd peamiselt on meie finantssektor suunatud Eesti klientide teenindamisele ja Eestis massihävitusrelvi ega selleks vajaminevaid tehnoloogiaid/kaupu ei toodeta.

Finantssektori kaudu on võimalik läbi viia strateegilise (sõjalise, kahesuguse kasutusega) kauba ostu-müügitehinguid kaubanduse finantseerimisega seotud tehingute kaudu[44]. Antud risk eksisteerib, kuid rahvusvaheliste standardite järgi ei eeldata, et finantsasutused iseseisvalt tuvastavad kahesuguse kasutusega kaupu, kuna tegemist on finantsasutuste jaoks keerulise teemaga. Finantsasutuste peamine tegevus on massihävitusrelvade leviku rahastamise tõkestamisel jälgida, et nad külmutaks ja ei teeks vahendeid kättesaadavaks ning ei pakuks finantsteenuseid määratletud isikutele ja asutustele ning tegevuspõhiselt ei rahastaks massihävitusrelvade levikut: andesklientidele omavahendeid sellisteks tehinguteks. Juhul kui finantsasutus tuvastab hoolsusmeetmete kohaldamise käigus, et tehing on seotud või tekib kahtlus, et tehing on seotud keelatud kaubaga, siis ta ei teosta tehingut ja teavitab sellest kahtlasest tehingust Rahapesu Andmebürood.

Teadlikkus antud valdkonnas on tagasihoidlik ja avalikest allikatest ei ole võimalik väga palju praktikas kasutatavat informatsiooni ka kätte saada. KAPO kodulehelt saab lugeda massihävitusrelvade leviku tõkestamise kohta[45] ja Välisministeeriumi lehel on ülevaade strateegilise kaubaga seotud õigusaktidest, kus massihävitusrelvadele eraldiseisvalt tähelepanu ei ole pööratud. Eestis kehtiv „Strateegilise kauba seadus“ käsitleb massihävitusrelvi ja nende sihtmärgi tabamise süsteeme sõjalise kaubana. Kogu tegevus seoses strateegilise kaubaga vajab eriluba. Samuti on Välisministeeriumi lehelt kättesaadavad juhendid ja ohuindikaatorid, mis annavad üldise pildi seonduvalt „Strateegiliste kaupadega“ aga ei too eraldiseisvalt välja massihävitusrelvade temaatikat.

Maksu- ja Tolliameti kodulehelt[46] on võimalik kontrollida, kas konkreetse kaubakoodiga kauba osas on kehtestatud piiranguid.

Finantsasutused kasutavad oma seiresüsteemides ja hoolsusmeetmete rakendamisel riskipõhist lähenemist. Massihävitusrelvade rahastamist puudutavate finantssanktsioonide ja muude hoolsusmeetmete kehtestamise üle teostab finantsasutuste üle järelevalvet kuni 01.01.2021 Rahapesu andmebüroo, kes ei ole selle teemaga jõudnud väga süvitsi tegeleda ressursside nappuse tõttu. Alates 01.01.2021 teostab Finantsinspektsioon finantssanktsioonide sh massihävitusrelvade leviku rahastamisega seotud finantssanktsioonide (sihipäraste) järelevalvet finantssektoris.

Turuosaliste vastavuskontrollisüsteemide tõhusust võib hinnata küsitlustest saadud tulemuste põhjal järgmiselt:

[44] Näiteks: akreditiivid, faktooring, escrow, erinevad garantiid, laenud, krediidikindlustus jmt.
[45] lingilt https://www.kapo.ee/et/content/massihävitusrelvade-leviku-tõkestamine.html
[46] https://apps.emta.ee/arctictariff-public-web/#!/taric/nomenclature/sbn?sd=11.01.2021&d=I&cc=&l=et&ql=et&ea=false

- Vastavusekontrollisüsteemide piisavust hinnatakse regulaarsel alusel[47];
- Suurima mõjuga turuosaliste seiresüsteemid on automatiseeritud[48], reeglina on ka teiste turuosaliste seiresüsteemide automatiseerimine vastav teenuste mahtudele;
- Sanktsioonide nimekirju uuendatakse regulaarselt ja automatiseeritult[49];
- Tehingute seire stsenaariumide valik ja kalibreerimine on reeglina kooskõlas üksuse profiili ning sellest tulenevate riskidega[50], samas on teatud turuosalistel selles osas arenguruumi, et muuta nende võimekus veelgi kõrgematasemelisemaks, võimaldades reaalajas tehingute jälgimist ja peatamist ning olles senisest enam riskitundlikumad[51];
- Suurima mõjuga turuosaliste tehingute seiresüsteemid võimaldavad tuvastada teatuid keerukaid või ebatavalisi tehinguid, kuid peaksid olema senisest enam riskitundlikud[52];
- Enamuse turuosaliste puhul on kasutusel kliendi riskitaseme riskipõhist arvutamist võimaldav süsteem[53];
- Enamus turuosalisi investeerib riskijuhtimise tehnilistesse lahendustesse ja peamiselt panustatakse programmidesse ja tarkvarasse[54].

Rahapesu Andmebüroole edastatud rahvusvahelise sanktsiooni teadete põhjal saab väita, et finantsasutuste vastavuskontrollisüsteemid on tõhusad ja on võimelised tuvastama sanktsiooni nimekirja kantud isikuid ja üksusi.

Kliendikontrolli raamistiku kvaliteedi osas läbiviidud küsitluse käigus leiti järgmised haavatavused:

- Riigi registrites sisalduv tegelikke kasusaajaid käsitlev teave ei ole alati usaldusväärne;
- Raskendatud on juurdepääs teabele, mis on vajalik tegelike kasusaajate kindlakstegemiseks;
- Raskendatud on juurdepääs teabele, mis on vajalik teiste suure riskiga klientide (nt saatkonnad, virtuaalvääringute pakkujad, rahateenuseid pakkuvad ettevõtjad, mittetulundusühendused jms) kindlakstegemiseks ja kontrollimiseks.

Hoolsusmeetmete raamistiku kvaliteet on reeglina kõrge. Kliendikontrolli seisukohalt on suurematekseks probleemideks tegeliku kasusaaja tuvastamise protsessi keerukus ning usaldusväärse allika puudumine tegeliku kasusaaja andmete kontrollimiseks. Lisaks tekitab raskusi kauba finantseerimisega seotud tehingutes kõikide osapoolte tuvastamine, kuna finantsasutused ei pruugi näha tervet tehingu ahelat.

Reeglina on rahvusvaheliste sanktsioonide kindlakstegemise kvaliteet kõrge. Kuigi kahesuguse kasutusega kaupade temaatika on väga spetsiifiline ja nõuab finantssektorilt väga laialdasi teadmisi, ei eeldata, et finantsasutused iseseisvalt tuvastavad kahesuguseid kaupu, kuna tegemist on finantsasutuste jaoks keerulise teemaga. Eelkõige tuleks finantssektoril tähelepanu pöörata kõrge riskiga riikidega seotud tehingutele, mille puhul toimub kauba vahendamine ja/või tehingu rahastamine, kus kaup ei pruugi üldse ületada Eesti tollipiiri.

[47] Krediidiasutuste, makseasutuste, investeerimisühingute, elukindlustusseltside küsitluste tulemuste põhjal

[48] Krediidiasutuste, makseasutuste, investeerimisühingute küsitluste tulemuste põhjal

[49] Krediidiasutuste, makseasutuste, elukindlustusseltside küsitluste tulemuste põhjal

[50] Krediidiasutuste küsitluste tulemuste põhjal

[51] Fondivalitsejate, makseasutuste. investeerimisühingute küsitluste tulemuste põhjal

[52] Krediidiasutuste, makseasutuste, elukindlustusseltside küsitluste tulemuste põhjal

[53] Krediidiasutuste, fondivalitsejate, makseasutuste, investeerimisühingute, elukindlustusseltside küsitluste tulemuste põhjal

[54] Krediidiasutuste, makseasutuste, investeerimisühingute, eluskindlustusseltside küsitluste tulemuste põhjal

Skaalal 1-5 on finantssektori haavatavuse hinne massihävitusrelvade leviku rahastamise osas 2,75 ehk **keskmiselt madal.**

Finantssektori MHR leviku rahastamise jääkriskide maandamiseks nähakse ette järgmised leevendavad meetmed:

1) pädevate asutuste koostöös näidisstsenaariumite loomine, mis aitaks turuosalistel oma tegevusega seotud riske tuvastada ja analüüsida.
2) teadlikkuse suurendamise ja vabalt kättesaadavate juhendite täiendamisega peatükiga „Massihävitusrelvadega seonduv", kus oleks praktiliselt kasutatavad meetmed ja võimalikud ohukohad selgelt kirjeldatud.
3) kindlasti on oluline ka finantssektorist väljapoole jäävate majandussubjektide informeerimine temaatikast.
4) julgustada kohustatud isikuid teavitama Rahapesu Andmebürood ka sellistest tehingutest, kus tuvastatakse või tekkib kahtlus, et tegemist on massihävitusrelvade leviku rahastamisega.

12.4.2.2. Fintech sektor

Kirjanduse põhjal kasutavad MHR levitajad ametlikke finantsteenuse osutajaid kahel peamisel eesmärgil:

1) massihävitusrelvadega seotud kaupade hankimise eest tasumiseks;
2) tuumarelva (või bioloogilise- või keemiarelva) levitamisega seotud raha kogumiseks, pesemiseks ja liigutamiseks (nt raha, millega makstakse lõpuks massihävitusrelvade eest, või kasum, mis tekib massihävitusrelvade levitamise tagajärjel).[55] Seeläbi muudavad nad finantstehnoloogia sektori osaks oma levitamiskavast.

Fintech sektori haavatavust võib eeskätt suurendada ebapiisav teadlikkus rahvusvaheliste sanktsioonide rakendamise, massihävitusrelvade ja kahesuguse kasutusega kauba temaatikal. Teadmiste puudujääke võib esineda ka regulaatorite hulgas, mis võib omakorda põhjustada selle, et regulatsioonid ei vasta alati tegelikele vajadustele või puuduvad sektorispetsiifilised suunised ohtudega võitlemiseks.

Massihävitusrelvade ja kahesuguse kauba temaatika on saanud oluliselt vähem avalikkuse tähelepanu kui näiteks rahapesu ja terrorismi rahastamise valdkond ning teavitustegevus finantstehnoloogia sektorile on olnud tagasihoidlik.

Virtuaalvääringutest tulenevad ohud seisnevad peamiselt nende omadustes: suhtelist anonüümsust võimaldav tehnoloogia, mille lihtne kasutatavus ning puudulik kliendi tundmise (KYC) reeglite rakendamine teenusepakkujate poolt võimaldab virtuaalvääringute valdkonna ärakasutamist kuritegelikul eesmärgil. KRDV on viimastel aastatel pööranud suurt tähelepanu virtuaalse vara (krüptovara) pakkujate, näiteks virtuaalvääringu vahetamise teenusepakkujate ärakasutamisele ÜRO JN sanktsioonidest kõrvalehoidmiseks. PoE tõstis oma 2019.[56] ja 2020. aasta aruannetes[57] esile mitmeid taktikaid ja tehnikaid, mida KRDV kasutab, mille sihiks on ebaseaduslik virtuaalvääringute kogumine, kaevandamistegevused, sealhulgas keerukaid tehnoloogilisi toiminguid ja pahavara rakendades. Selge vastuseta on küsimus, kuidas KRDV seejärel oma virtuaalse vara tavavaluutaks konverteerib.

KRDV on alates 2019. aasta maist suurendanud oma Monero kaevandustegevust vähemalt kümnekordseks (võrreldes bitcoini kaevandamisele samal perioodil). Monero on virtuaalne valuuta, mis sarnaneb bitcoiniga, kuid pakub täiendavat anonüümsust ja ei vaja kaevandamiseks tingimata sama suure jõudlusega arvuteid.[58]

[55] Kassenova, T., The Exploitation of the Global Financial Systems for Weapons of Mass Destruction (WMD) Proliferation, https://carnegieendowment.org/2020/03/04/exploitation-of-global-financial-systems-for-weapons-of-mass-destruction-wmd-proliferation-pub-81221.

[56] https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_691.pdf

[57] https://undocs.org/S/2020/840

[58] Näiteks WannaCry ohvrite tehtud Bitcoini lunaraha maksed kanti üle Bitcoini rahakottidesse ja lõpuks konverteeriti Monero'ks, kasutades Šveitsi virtuaalvääringuvahetusplatvormi ShapeShift.

PoE-le on teatatud 2019. aastaks vähemalt 35 juhtumist, kus KRDV päritolu isikud on toime pannud küberrünnakuid finantsasutuste, virtuaalvääringu vahetajate ja kaevandajate vastu, eesmärgiga varastada virtuaalvääringuid tulu saamiseks. Selleks, et tehingute jälgitavust piirata, kasutab KRDV sarnaselt rahapesijatega erinevaid digitaalseid vara kihistamismeetodeid, näiteks loovad tuhandeid virtuaalvääringu rahakotte erinevate teenusepakkujate juures. 2019. a jooksul suundus KRDV rünnete teravik veelgi enam virtuaalvääringu vahetusplatvormide vastu, seejuures on mõned virtuaalvääringu vahetusplatvormid olnud rünnaku ohvriteks korduvalt ning pidanud seetõttu ka tegevuse lõpetama[59].

Ühisrahastuse puhul on peamiseks ohuks sektori alareguleeritus ja sektorispetsiifiliste juhendmaterjalide, mis puudutavad massihävitusrelvade leviku või rahastamise tõkestamist, puudus.

Ohuallikateks on ka finantstehnoloogia sektori kaudu finantseeritavad ja/või arveldavad majandussubjektid, keda võidakse suhteliselt madala teadlikkuse tõttu nende endi teadmata ära kasutada. Oht võib, sarnaselt finantssektorile, esineda erinevates vahendustehingutes, kus kaup ei pruugi läbi Eesti liikuda, aga finantseerimine toimub Eesti finantstehnoloogia teenuseosutaja poolt. Tegelike kasusaajate kontrolli ebaühtlane rakendamine rahvusvaheliselt võib samuti kujutada ohtu.

Finantstehnoloogia sektori puhul tuleb eraldi esile tõsta küber- ja krüptodomeenist tulenevaid ohte. Näiteks tumeveebis tehingute tegemine, organiseeritud küberkuritegevus, suurem sõltuvus infotehnoloogiast ja kriitilise tähtsusega teenuste liikumine küberkeskkonda[60]. Küber- ja krüptodomeeni saab kasutada ebaseaduslikel eesmärkidel, sealhulgas massihävitusrelvadega seotud programmide jaoks või vahendite saamiseks.[61]

KRDV suhtes kehtestatud sanktsioonide vältimise oht on virtuaalvääringu teenusepakkujate sektori puhul **kõrge**.

Haavatavust suurendab see, et info sanktsioonirežiimide kohta, samuti KRDV või Iraani tegevuse kohta ei tule sageli ametlikest kanalitest, vaid on kättesaadav pigem ajakirjanduse kaudu, millele teenusepakkujad ei pruugi osata õigeaegselt tähelepanu pöörata. Virtuaalvääringu teenusepakkujad on rahvusvahelise sanktsiooni seaduse mõistes erikohustusega isikud, seega peavad nende siseprotseduurid sisaldama muu hulgas asjakohaseid meetmeid sanktsioneeritud isikute või tehingute kahtluse korral toimimiseks.

Massihävitusrelvade rahastamist puudutavate finantssanktsioonide rakendamise üle teostab finantstehnoloogia sektoris järelevalvet Rahapesu Andmebüroo, kes ei ole selle teemaga jõudnud väga süvitsi tegeleda ressursside nappuse tõttu.

Ligikaudu 50% ettevõtetest ei ole kasutusele võetud erinevaid mehhanisme (näiteks sanktsioonidest kõrvalehoidmise, terrorismi rahastamine (see küll vaid 25%), radikaalsete liikumiste, kahesuguse kasutusega kaupadega seonduvad rahavood jne tuvastamiseks või vältimiseks). Samuti vastasid „ei“ või „ei oska öelda“ ligikaudu 40% ettevõtetest varade külmutamise protseduuri dokumenteerimise kohta.

Virtuaalvääringute sektori risk massihävitusrelvade teemas on samasugune nagu muudes teemades. Suhtelist anonüümsust võimaldav tehnoloogia, lihtne kasutatavus ning puudulik kliendi tundmise (KYC) reeglite rakendamine tähendab kõrgeimat võimalikku riski virtuaalvääringute valdkonna ära kasutamiseks kuritegelikul eesmärgil. Ohuga kokkupuutumise tõenäosus on virtuaalvääringute vahetajatel suur, seoses KRDV aktiivsusega ja erinevate taktikatega kasutada illegaalse tulu teenimiseks ära just virtuaalvääringu

[59] Youbit (endine Yapizon) langes 2017. a aprillis korduvate küberrünnete alla, kaotades $4.8 M, ja täiendavalt detsembris 2017 kogu varadest 17%, olles sellega sunnitud oma tegevuse lõpetama.

[60] Arengud Läänemere piirkonna julgeolekukeskkonnas kuni 2020. aastani, https://www.riigikogu.ee/wpcms/wp-content/uploads/2014/11/RIIGIKOGU_RAPORT-2.pdf, lk 35.

[61] Vt nt Põhja-Korea kohta kirjutatut, Kassenova, T., The Exploitation of the Global Financial Systems for Weapons of Mass Destruction (WMD) Proliferation, https://carnegieendowment.org/2020/03/04/exploitation-of-global-financial-systems-for-weapons-of-mass-destruction-wmd-proliferation-pub-81221.

sektorit. Ühisrahastuse valdkond eraldivõetuna massihävitusrelvade rahastamise kontekstis probleemi ei kujuta.

Eriti haavatavad on virtuaalvääringu teenuse pakkujad KRDV suhtes kehtestatud sanktsioonide rikkumise ohu tõttu, kuivõrd on teada et KRDV kasutab just viimasel ajal virtuaalvääringuid ebaseadusliku tulu teenimiseks ja kehtestatud sanktsioonide vältimiseks. Lähtudes eeltoodust võib virtuaalvääringu teenuse osutajatega seotud haavatavust massihävitusrelvade rahastamise osas pidada **keskmiseks/kõrgeks.**

Ühisrahastusteenuse osutajatega seotud haavatavust massihävitusrelvade leviku rahastamise osas hinnati „madalaks".
Eeltoodud põhjustel ei ole tuvastatud MHR leviku rahastamise jääkriskid finantstehnoloogia sektoris piisavalt maandatud ja rakendada tuleks järgnevaid meetmeid:

1) järelevalveasutustel koostada sektorispetsiifilisi suuniseid ja juhendmaterjale.
2) pädevad asutused peaksid korraldama sektorispetsiifilisi koolitusi just massihävitusrelvade leviku rahastamise tõkestamise kontekstis.
3) pädevate asutuste koostöös näidisstsenaariumite loomine, mis aitaks turuosalistel oma tegevusega seotud riske tuvastada ja analüüsida.
4) Virtuaalvääringu teenusepakkujad peaksid pöörama erilist tähelepanu KRDV-ga seonduvatele tegevustele, üksustele ja isikutele ning kasutama tõhusaid meetmeid klientide hulgast KRDV päritolule viitavate indikaatorite väljatöötamisek
5) Tugevdatud hoolsusmeetmeid tuleb kohaldada olukorras, kus kliendil on huvi levinuma virtuaalvääringu (bitcoin) vahetamisel lisa-anonüümust pakkuvate virtuaalvääringute vastu (nagu Monero) ja eriti sellise virtuaalvääringu vahetamisel tavavaluutaks.
6) rahakotiteenuse pakkujatel tuleb vastavalt RahaPTS §-le 25 tagada kõigi klientide isikusamasuse tuvastamine, ning täiendava hoolsusmeetmena rakendada KRDV päritolu isikute tuvastamiseks lisameetmeid.

12.4.2.3. Kauplejate sektor

Käesoleva NRA käigus läbi viidud uuringu valimisse kaasatud erinevad kauplejate sektorid ei kujuta endast sellistes valdkondades tegutsevaid isikuid, kes võiksid olla seotud massihävitusrelvade tootmise, transiidi või rahastamisega. Massihävitusrelvade levitamine ja seonduv kaubandus on kauplejate sektoris väga vähe tõenäoline, sest hõlmatud tegevusalade puhul oleks selliste tegevus ilmselgelt eristuv ettevõtete tavapärasest äritegevusest.

Eesti kontrollib üle oma piiri veetavaid kaubavoogusid, pöörates kontrolli käigus tähelepanu strateegilistele kaupadele ja massihävitusrelvadega seotud riskidele. Massihävitusrelvade leviku rahastamist võib Eesti kauplejate sektori kontekstis pidada mitteaktuaalseks teemaks.

Juhtkonna teadlikkus massihävitusrelvade leviku ja selle rahastamise ohtude osas on pigem madal, kuna sektorite kokkupuude sellise teemaga on väga ebatõenäoline: Eestis ei toodeta massihävitusrelvi ega nende komponente. Sektorite osas on teadlikkus erinev. Teadlikkus on eeldatavasti kõrgem autode ja väärismetalli sektoris, kuna nende seas on kohustatud isikuid rohkem ning seetõttu ka teadlikkus suurem. Järelevalve seisukohast on suurimaks probleemiks inim- ja tehnoloogiliste ressursside ebapiisavus või vähene oskus ja teadlikkus olemasolevaid ressursse kasutada. Kuna sektor on lai, siis ka sektori siseselt suured erinevused järelevalve teostamise kvaliteedis. Alamsektoreid, kus teadlikkus ja oskused piisavad, on vähe.

Massihävitusrelvade rahastamise tuvastamine on kauplejatele kindlasti raske ülesanne, kuna rahastamine võib toimuda ka nö „mitte sanktsioneeritud" isikute poolt kas teadlikult või mitte. Indikaatoreid, millele tähelepanu pöörata, ei ole kauplejatele järelevalveasutuste poolt kättesaadavaks tehtud. Info sanktsioonide rakendamisega, kahese kasutusega kaupade ja sõjalise kasutusega kaupade regulatsioonide ja protseduuride kohta on asutuste veebilehtedel kättesaadav kõigile, kellel nende teemadega puutumust on. Kauplejad on üldiselt teadlikud järelevalveasutusele teatamise kohustusest juhul, kui kliendiga tehingu

sõlmimisel tekib terrorismi rahastamise kahtlus või juhul kui ebaharilik tehing on seotud kõrgendatud terrorismiohuga piirkondadega ehk riskiriikidega. Samas reaalselt ei ole teateid esitatud kas probleemi puudumise või tuvastamise ebaefektiivsuse tõttu. Kõrge riskiga klientide tuvastamiseks ja kliendiandmete kontrollimiseks kasutatavaid infosüsteeme ei osatud hinnata vähese kogemuse ja teadlikkusse tõttu. Teadlikkus sanktsioonide nimekirjade olemasolust on üldiselt madal ning ettevõtte sisese töökorraldusega ei ole nimekirjade, toodete ja isikute võrdlemine täpselt paika pandud.

Kauplejate sektori haavatavust massihävitusrelvade leviku rahastamisega seonduvalt on vaja vaadelda tervikuna koos kogu strateegilise kaubaga, mis katab nii massihävitusrelvad, kogu sõjalise kauba ja ka kahesuguse kasutusega kauba. Vaatamata asjaolule, et oht on väike, on temaatika väga spetsiifiline ja nõuab väga laialdasi teadmisi.

Peamiseks haavatavuseks on kauplejate üldine (va need kauplejad, kes teadlikult tegelevad strateegiliste kaupadega ja on selleks omandanud vastava loa) vähene teadlikkus teemast, mistõttu võib eksisteerida võimalus, et kaupleja tegeleb enesele teadmata (või ka teadlikult) toodete või teenuste vahendamisega, mis võivad olla kantud strateegilise kauba nimekirja või sisaldavad osi, materjale või detaile, mis on nimekirjas. Strateegilise kauba nimekiri eksisteerib ja on vabalt kättesaadav Välisministeeriumi lehelt. Suuremat riski võivad kujutada sanktsioneeritud (embargoalused) kaubad kuna nende puhul on piirangud sõltuvad konkreetsest riigist ja isikust. Ka hõlmavad embargopiirangud sageli lisaks strateegilistele kaupadele ka muid kaupu. Nimekirjad sanktsioonidest on samuti kättesaadavad Välisministeeriumi lehel.

Spetsiifiliselt Iraaniga kaubandussuhteid omavaid kauplejaid on vähe ja KRDV-ga Eestil kaubandussuhted puuduvad, mistõttu võib nende sanktsioonirežiimide rikkumise tõenäosust kauplejate sektoris pidada **väga madalaks**.

Eeltoodud põhjustel on madala jääkriski maandamiseks võimalik soovitada järgmiseid meetmeid:

1) riiklikul tasemel saab riske maandada pädevate asutuste koostöös näidisstsenaariumide loomisega, mis aitaks turuosalistel oma tegevusega seotud riske tuvastada ja analüüsida;
2) sektorisiseselt saab riske maandada eelkõige läbi teadlikkuse suurendamise ja vabalt kättesaadavate juhendite täiendamisega peatükiga „Massihävitusrelvade leviku rahastamisega seonduv“, kus oleks praktiliselt kasutatavad meetmed ja võimalikud ohukohad selgelt kirjeldatud.

12.4.2.4. Kinnisvarasektor

Sektoril ei ole tõenäolisi kokkupuuteid massihävitusrelvade leviku rahastamisega. KRDV ja Iraani sanktsioonide nimekirjade rakendamist kinnisvara soetamisel jälgib kinnistusraamatu pidaja, kelle spetsiifiline erikohustus tuleneb rahvusvahelise sanktsiooni seaduse § 25 lg 1 p 4 ja kes teavitab Rahapesu Andmebürood finantssanktsiooni subjekti või finantssanktsiooni rikkuva tehingu või toimingu tuvastamisest.

12.4.2.5. Mittetulundussektor

Massihävitusrelvade leviku ja selle rahastamise tõkestamisel on heategevuslikul, usulisel, kultuurilisel, hariduslikul, sotsiaalsel või perekondlikul eesmärgil tegutsevate organisatsioonide puhul haavatavusi väga raske välja tuua, kuna kokkupuutemoment on minimaalne. Kaasused siinkohal Eestis puuduvad. Teatav tõenäosus on sellistel sanktsioonirežiime potentsiaalselt rikkuvatel tegevustel, kus oskusteave või laborivahendite liikumine suundub kurjategijate kätte haridussektoris, seda just Iraani sanktsioonirežiimi rikkumise ohu vaatenurgast.

Julgeolekuasutuste vaates on eristatav kahese kasutusega kaup ning massihävitusrelvadega seonduv. Eestis on massihävitusrelvade leviku oht madal, Eesti massihävitusrelvi ega selleks vajaminevaid tehnoloogiaid/kaupu ei tooda. Seni pole meie territooriumil esinenud juhtumeid, kus keegi oleks proovinud tuuma-, bioloogilist-, radioaktiivset või keemilist materjali rünnakuks kasutada või seda rahastada.

Suurimaks massihävitusrelvadega seotud ohuks peetakse piiriülest levikut, mille puhul võidakse Eestit kasutada transiitriigina.

Heategevuslikul, usulisel, kultuurilisel, hariduslikul, sotsiaalsel või perekondlikul eesmärgil tegutsevate organisatsioonide puhul võivad teatud spetsiifilised ohud tekkida seoses nende asutuste sooviga toetada KRDV-s hädasolevaid inimesi või Iraani puhul sooviga teha hariduslikku koostööd, mis võib olla tegelikkuses seotud tuumarelva arendamisega seonduva teadustegevusega. Humanitaarsetel eesmärkidel on sanktsioonidest lubatud ka teatud juhtudel erandeid teha. See toob aga omakorda kaasa täiendavad riskid. Teadaolevalt ei tegutse Eesti mittetulundussektor hetkel siiski nendesse riikidesse abi või suhete vahendamisega.

Toetudes eksperthinnangule on sektori haavatavuse tase massihävitusrelvade leviku rahastamise tõkestamisel **madal**.

Jääkriskide maandamiseks tuleks rakendada järgnevaid meetmeid:

1) pädevate asutuste koostöös näidisstsenaariumide loomisega, mis aitaks turuosalistel oma tegevusega seotud riske tuvastada ja analüüsida.
2) sektorisiseselt saab riske maandada eelkõige läbi teadlikkuse suurendamise ja vabalt kättesaadavate juhendite täiendamisega, kus oleks kirjeldatud praktiliselt kasutatavad meetmed ja võimalikud ohukohad.

12.4.2.6. Äriühingute teenusepakkujate sektor

Vaadeldes massihävitusrelvade rahastamise trende, on ÜRO JN KRDV sanktsioonirežiimi ekspertide komitee (panel of experts ehk PoE) leidnud, et Korea Rahvademokraatlik Vabariik omab jätkuvalt juurdepääsu rahvusvahelisele finantssektorile erinevate ühisettevõtete, offshore - kontode, varifirmade ja virtuaalsete varade kaudu. Analüüside tulemused näitavad, et KRDV kasutab seotud üksuste ja isikute kaudu jätkuvalt Ida- ja Kagu-Aasia pangandussüsteeme ja sellekaudu laiemalt rahvusvahelist korrespondentpangandust. PoE on ka liikmesriike kritiseerinud ebapiisavate pingutuste eest siseriiklike äriühingute registreerimise reeglite kehtestamisel, mis on võimaldanud jätkuvalt KRDV-l kasutada ära läbipaistmatuid ettevõtete struktuure. Lüngad ettevõtete registreerimise kontrollimehhansimides muudavad tunne-oma-klienti protsessid ja protseduurid finantsasutustes praktiliselt võimatuks.

Iraani suhtes ei ole resolutsiooni 2231 suhtes samaväärselt trende ja mustreid analüüsitud, ÜRO liikmesriigid on teavitanud üksikutest võimalikest sanktsioonirežiimi rikkumistest, s.h võimalikust finantseerimistegevusest. Iraaniga seonduva kaubavahetuse piiratuse tõttu, samuti Eestis tuumarelvade- ja vastava tehnoloogiasektori puudumise tõttu seonduvad sanktsioonirežiimi rikkumisega seega peamiselt ohud, millega sanktsiooninimekirjadesse kantud isikud ja üksused üritavad sooritada tehinguid Eesti ettevõtetega või nende kaasabil.

Äriühingute teenusepakkujad ei ole erikohustusega isikuteks rahvusvahelise sanktsiooni seaduse mõistes, teisalt on nad EL otsekohalduvate määruste kohaselt kohustatud nii KRDV kui ka Iraani sanktsioneeritud isikute nimekirjadesse kantud isikute vara külmutama.

Sektori jääkrisk on eeltoodud põhjustel **kõrge** ning võib juhtuda, et äriühingute teenusepakkujaid kasutatakse ära ettevõtete loomise eesmärgil sanktsioneeritud isikute poolt. Kuna põhiliselt kohaldatakse sektoris RahaPTS sätteid üldises korras, mille rakendamisel tuleb arvestada Rahapesu Andmebüroo juhenditega, ei saa sektori hoolsusmeetmete kohaldamise taset lugeda kohaseks ka seoses massihävitusrelvade rahastamisega – rahvusvaheliste sanktsioonide kohaldamisega- kaasnevate riskidega. Kuna tegemist ei ole finantseerimisasutusega, ei kohaldu rangemad nõuded isikusamasuse tuvastamiseks, ehk teenuseid võib teatud juhul osutada ka ilma isikusamasust tuvastamata. Näiteks ärisuhte puudumisel tehingute osas, mis jäävad alla 15 000 -eurose piirmäära ning ei esine teisi seadusest tulenevaid tingimusi.

Riskide maandamiseks:

- tuleks tõsta regulatsiooni taset, et ei oleks lubatav sektori teenuste kasutamine ilma isikusamasuse tuvastamiseta, ning oleks tagatud, et sanktsioneeritud isikute nimekirja kantud isikud ei omaks ligipääsu äriühingute teenusepakkujate teenustele.

12.4.2.7. Advokaadid, audiitorid, kohtutäiturid, muud õigusteenuse osutajad, notarid, pandimajapidajad, raamatupidajad, hasartmängukorraldajad

Sektori ärakasutamist massihävitusrelvade leviku rahastamiseks KRDV või Iraani sanktsioonirežiimide rikkumise läbi võib pidada ebatõenäoliseks ja seetõttu ei ole asjakohane käesoleva sektori haavatavust antud aspektist eraldi analüüsida.

Kohaldub üldine regulatsioon rahvusvaheliste sanktsioonide rakendamiseks.

12.5. Massihävitusrelvade leviku rahastamise tagajärjed

Eestis tuleb riiklikul tasandil massihävitusrelvade leviku rahastamise tagajärgi hinnata läbi teostunud sanktsioonirežiimi rikkumisega kaasneva potentsiaalse mõju:

a) riigi julgeolekule,
b) majandusele,
c) poliitilisele olukorrale (s.h riigi maine) ja
d) ühiskonnale

Tuumarelvade leviku tõkestamise rahastamise, st massihävitusrelvade kasutamise tagajärg on raskem kui rahapesu või muude finantskuritegude puhul ning sarnaneb rohkem terrorismi rahastamise tagajärgedega seotud võimaliku inimkaotusega. Sellise tegevuse rahastamise võimalikkus läbi Eesti omab riigi julgeolekule suurt mõju. Kaasnevateks negatiivseteks tagajärgedeks oleks usalduse kaotus meie julgeolekupartnerites ning rahvusvahelise rahu ja julgeoleku ulatuslik kahjustumine.

Riigi majandusele oleks mõju väga suur: seoses MHR rahastamisega kaasnevate korrespondentpangandussuhete lõpetamisega kaasneks finantsteenuste kättesaadavuse vähenemine, mis kahjustab riigi majandust, tõstab intressimäärasid, inflatsiooni, kahjustunud usaldusväärsus ja klientide usalduse oluline langus põhjustab negatiivseid tagajärgi rahvusvahelistes ärisuhtes. See omakorda toob kaasa välismaiste otseinvesteeringute vähenemise või peatumise, finantsturgude ebastabiilsuse ja maksutulude vähenemise.

Tagajärg riigi poliitilisele olukorrale ja mainele on suur: kaasnev rahvusvahelise meedia negatiivne tähelepanu ja poliitilised skandaalid, millel on pikaajaline mõju riigi mainele, suur tõenäosus sattuda FATFi ICRG klassifikatsiooni alla „riigid ja territooriumid, kes ei tee koostööd“ seoses võimetusega rakendada efektiivselt rahvusvahelisi sanktsioone, olenevalt MHR leviku režiimist, mida rikutakse, võib kaasneda vähene mõju poliitilisele stabiilsusele takistuste tõttu rahvusvahelistes suhetes.

Tagajärg ühiskonnale oleks keskmine, kuivõrd MHR leviku tõkestamise sihtriigid asuvad Eestist nii geograafiliselt kui kultuuriliselt kaugel. Kaasneks kindlasti üldsuse hukkamõist, võimalikud viited eetika- ja demokraatiastandardite nõrgenemisele, majandus-, julgeoleku- ja poliitilise olukorra mõjud omaksid teatavad mõju töökohtade arvu langemisele ja elatustaseme vähenemisele.

12.6. Leevendavad meetmed

Kohustatud isikud peaksid lisaks nimekirjadele tuginemisele kohaldama täiendavaid hoolsusmeetmeid, et leevendada sanktsioonidest kõrvalehoidumise riski. Hoolsusmeetmete eesmärgiks on tagada, et kohustatud isikud mõistaks oma kliendi äritegevuse olemust ning tuvastavad ja kontrollivad klienti ja

tegelikke omanikke, tagamaks, et nad ei ole otseselt ega kaudselt seotud sanktsioneeritud isikute nimekirja kantud isikute ja üksustega.

Kohustatud isikud peaksid MHR rahastamise riskide maandamiseks kohaldama riskantsete tehingute indikaatorite nimekirja. Indikaator näitab või viitab ebatavalise või kahtlase tegevuse esinemise tõenäosusele. Ühe näitaja olemasolu seoses kliendiga või tehinguga ei pruugi üksi õigustada MHR leviku rahastamise kahtlust ega näita tingimata sellist tegevust selgelt, kuid see võib hõlbustada edasist jälgimist ja uurimist. Samas võib mitme indikaatori esinemine õigustada ka täiendavate meetmete kohaldamist ja info kogumist. See, kas üks või mitu indikaatorit viitab massihävitusrelvade levitamise rahastamisele, sõltub ka konkreetse ettevõtja ärisuundadest, toodetest või teenustest; sellest, kuidas ta suhtleb oma klientidega; inimressursside ja tehnoloogiliste ressursside võimalustest.

Kohustatud isikud peaksid tulenevalt oma tegevusvaldkonnast ja tehingupartneritest, eriti juhul, kui ollakse aktiivne piiriüleselt, määratlema sisemistes protseduurireeglites, ja kooskõlas enda riskihinnanguga, milliste indikaatorite esinemisel tuleks kohaldada hoolsusmeetmeid tugevdatud korras, kasutades erinevate täiendavate väliste allikate (nt finantstehingute, ekspordi/tolliandmete ja avatud turuhindade) võrdlemist.

<u>Kliendi riskiprofiiliga seonduvad indikaatorid</u>

- ärisuhte loomisel annab klient oma kavandatava kauplemistegevuse kohta ebamäärast või puudulikku teavet. Klient ei soovi oma tegevuse kohta lisateavet esitada, kui temalt küsitakse lisainfot negatiivse teabe foonil[62];
- hoolsusmeetmete edasisel rakendamisel ilmneb kliendi, selle omanike või tippjuhtide kohta negatiivset informatsiooni, näiteks varasemad rahapesuskeemid, pettused, muu kuritegelik tegevus või käimasolevad või varasemad uurimised või süüdimõistvad kohtuotsused, sealhulgas ekspordikontrollirežiimide isikute nimekirjade mittejärgmisega seoses;
- klient on isik, kes on seotud MHR levikuga seostatava või diversiooniriigiga (riik, mida on teadaolevalt kasutatud MHR levikule seatud piirangute vältimiseks), nt selliste riikide topeltkodakondsusega isikud.
- klient on isik, kes tegeleb keerukate seadmetega, mille jaoks tal puudub tehniline taust või mis ei vasta määratletud tegevusalale;
- klient sõlmib keerukaid kaubandustehinguid, mis hõlmavad arvukalt kolmandatest osapooltest vahendajaid ärivaldkondades, mis ei ole vastavuses ärisuhte loomisel määratletud riskiprofiiliga;
- ärikliendina tuvastatud klient või tehinguosaline teeb tehinguid, mis viitavad sellele, et nad tegutsevad rahaülekandeettevõtte või laiendatud kasutusõigusega korrespondentkontona. Need kontod hõlmavad suuremahuliste tehingute kiiret liikumist ja väikest päeva lõpu saldot ilma selgete äriliste põhjusteta. Mõnel juhul näivad algatajatega seotud olevat üksused, kes võivad olla seotud MHR leviku probleemiga riigiga (näiteks tuumarelva leviku tõkestamisega seonduvalt nimetatud riigi või diversiooniriikides tegutsevad varifirmad) ning tegelikud kasusaajad näivad olevat seotud ekspordikontrollirežiimide alla kuuluvad tootjad või logistikaettevõtted;
- ülikooli või teadusasutusega seotud klient tegeleb potentsiaalselt MHR-tundlike või ekspordikontrolli all olevate kaupadega.

<u>Konto- või tehinguriskidega seonduvad indikaatorid</u>

- tehingu algataja või kasusaaja on isik või üksus, kelle alaline elu- või asukoht on MHR levitamise või diversiooni probleemiga riigis;
- kontoomanikud teevad tehinguid, mis hõlmavad massihävitusrelvadega seotud mitmepoolsete ekspordikontrollirežiimide või riiklike kontrollirežiimide alusel kontrollitavaid esemeid;
- kontod või tehingud hõlmavad võimalikke varifirmasid, nt. ettevõtetel ei ole piisavalt kapitali või nad avalikustavad (veebis) üksnes ettevõtte põhinäitajaid.

[62] Näiteks paludes lisainfot tegevuse ulatuse kohta rahvusvaheliste sanktsioode all olevates riikides

- eksisteerivad nähtavad seosed tehingu raames erinevate osapoolte ettevõtete esindajate, st omanike või juhtkonna, sama füüsilise aadressi, IP-aadressi või telefoninumbri või nende tegevuse vahel; viited, et nende tegevus võib olla kooskõlastatud;
- kontoomanik teostab ülekandeid nn „ringikujuliselt" – summa liigub kontolt-kontole ja jõuab sarnaselt tagasi algsele kontole;
- kontotegevus või tehingud, mille puhul seotud finantsasutuste algataja või saaja asukoht on nõrga ekspordikontrollirežiimiga riigis (see on oluline ka korrespondentpangandusteenuste puhul);
- tootmis- või kaubandusettevõtte klient soovib kasutada sularaha tööstuskaupade või kaubandustehingute puhul tehingute eest maksmisel. Finantsasutuste jaoks on tehingud nähtavad sularahasissevoolu kaudu ettevõtte kontodele, millele järgneb sularaha väljavõtmine;
- tehingud tehakse nn pearaamatu-korra alusel (s.h näiteks peegeltehingud), mis välistab vajaduse sagedaste rahvusvaheliste finantstehingute järele. Pearaamatu-korra tunnuseks on seotud ettevõtted, kes nähtavalt peavad arvestust üksteise nimel tehtud tehingute üle ja ülekanded näivad järgivat tasakaalustamise eesmärke;
- klient kasutab isiklikku kontot tööstuskaupade ostmiseks, mis on ekspordikontrolli all või mis pole muul viisil seotud ettevõtte tegevuse või ühtsete ärivaldkondadega.

<u>Merendussektori riskiindikaatorid</u>

- kaupleja on registreeritud aadressil, mis tõenäoliselt on massregistreerimise aadress, nt. suure elanike arvuga elamud, postkasti aadressid, ärihooned või tööstuskompleksid, eriti kui puudub viide konkreetsele üksuse tegutsemisele sellel aadressil;
- saadetist ettevalmistav isik või üksus märgib toote lõppsihtkohana ekspedeerimisettevõtte;
- saadetise sihtkoht erineb importija asukohast;
- vastuolud lepingutes, arvetes või muudes äridokumentides, nt. vastuolud eksportiva üksuse ja makse saaja nime vahel; erinevad arved ja nende aluseks olevad lepingud; või tegelike kaupade koguse, kvaliteedi, mahu või väärtuse ja nende kirjelduste lahknevused;
- kauba saatmine ei ole kooskõlas selle riigi tehnilise tasemega, kuhu see saadetakse, nt. pooljuhtide tootmise seadmed tarnitakse riiki, kus puudub elektroonikatööstus;
- kaubavedu toimub „ringikujuliselt" (kui kaubaveo teave on kättesaadav), sealhulgas mitu sihtkohta ilma nähtava ärilise eesmärgita;
- kaupade vedu ei ole kooskõlas tavapäraste geograafiliste kaubandusmudelitega, nt. sihtriik tavaliselt ei ekspordi ega impordi kaubandustehingute dokumentides loetletud kaupu;
- imporditud kaupade eest ei tasu kaupade saaja ilma selgete majanduslike põhjusteta, nt. tasub hoopis kaubandustehinguga mitteseotud kest- või varifirma.

<u>Kaubanduse rahastamise riskiindikaatorid</u>

- saadetis suunatakse läbi riigi, kus ekspordikontrolli seadused on nõrgad või ekspordikontrolli seaduste jõustamine nõrk;
- enne ärisuhte loomise lõpuleviimist taotleb klient akreditiivi eriregulatsioonidega või kahesuguse kasutusega kaupadega seotud tehingutele;
- vastuolud kaubandusdokumentides ja finantsvoogudes, nagu nimed, ettevõtted, aadressid, lõppsihtkoht jne;
- tehingud hõlmavad juhiseid või makseandmeid osapooltelt või nende poolt, kes ei ole algses akreditiivis või muus dokumendis märgitud.[63]

[63] Allikas: 2018 FATF Guidance on Counter Proliferation Financing ja UNSC PoE Raportid