



Eesti riikliku  
riskihinnangu aruanne  
terrorismi rahastamise  
tõkestamise valdkonnas  
2020–2024

# Sisukord

<b>1. ÜLDOSA</b>	3
1.1. Sissejuhatus	3
1.2. FATF-i definitsioonid ja mõisted	4
1.3. Kasutatud meetodika	4
1.4. Analüüsis kasutatud ohtude ja haavatavuste hindamiskriteeriumid	5
1.4.1. Riiklike ohtude hindamiskriteeriumid	6
1.4.2. Riiklike haavatavuste hindamiskriteeriumid	7
1.5. Andmete kogumine	8
<b>2. KOKKUVÕTE</b>	9
<b>3. TERRORISMOHT EESTIS</b>	12
3.1. Islamiäärmuslusest lähtuv oht	12
3.2. Vägivaldsest paremäärmuslusest lähtuv oht	12
3.3. Venemaa Föderatsioonist lähtuv oht	13
3.4. Vasakäärmuslusest lähtuv oht	13
<b>4. TERRORISMI RAHASTAMISE ÜLDINE ÜLEVAADE</b>	14
<b>5. RIIKLIKUD TERRORISMI RAHASTAMISE OHUD</b>	17
5.1. Sisemine oht	18
5.2. Eestist lähtuv oht	19
5.3. Väline oht	21
5.4. Transiidist tulenev oht	22
<b>6. HAAVATAVUSED</b>	23
6.1. Riiklikud terrorismi rahastamise haavatavused	23
6.2. Sektorite haavatavused	26
6.2.1. Virtuaalvääringu teenuse pakkujad	26
6.2.2. Krediitiasutused	29
6.2.3. Makseasutused, sh piiriülesed makseteenused (rahasiirde teenuse pakkujad, valuutavahetajad)	31
6.2.4. Ühisrahastusteenuse pakkujad	32
6.2.5. Teised valdkonnad	33
<b>LISAD</b>	
Lisa 1. Peamised terrorismi rahastamise tüpoloogiad	35
Lisa 2. Näidisjuhtumid	36
Lisa 3. Nõuanded sektoritele	38

# 1. Üldosa

## 1.1. Sissejuhatus

Terrorismi rahastamise riskihinnang on osa Rahandusministeeriumi eestvõttel läbi viidud suuremast riiklikust riskihinnangust, mis hõlmab riskide analüüsi seonduvalt rahapesu, terrorismi rahastamise ja massihävitusrelvade leviku finantseerimisega. Riiklik riskihinnang koostatakse Eestis regulaarselt iga nelja-viie aasta tagant ning see on aluseks ohtude ja haavatavuste maandamise tegevuskavale. Siinne riskihinnang viidi läbi 2024. aasta septembrist 2025. aasta juunini ning see hõlmab 2020.–2024. aasta andmete analüüsi. Riikliku riskihinnangu aruande kinnitas rahapesu ja terrorismi rahastamise tõkestamise valitsuskomisjon rahandusministri juhtimisel.

Terrorismi rahastamise riskide hindamiseks loodi eraldiseisev töögrupp. Töögruppi juhtis Siseministeerium ning sellesse kuulusid esindajad **Siseministeeriumist, Riigiprokuratuurist, Rahapesu Andmebüroost, Maksu- ja Tolliametist ning Kaitsepolitseiametist**. Töögrupp tegi koostööd ka paralleelselt rahapesu riskihinnangut koostanud töögruppidega, kus osales enam kui 100 valdkonna eksperti ministeeriumitest, valitsusasutustest ja erasektorist.

Riikliku riskihinnangu tulemuste valideerimiseks ja aruande valmimise hindamiseks moodustati riikliku riskihinnangu juhtrühm, kuhu kuulusid Rahandusministeeriumi, Justiits- ja Digiministeeriumi, Siseministeeriumi, Välisministeeriumi, Finantsinspektsiooni, Rahapesu Andmebüroo, Kaitsepolitsei ameti, Politsei- ja Piirivalveameti, Maksu- ja Tolliameti ning prokuratuuri esindajad.

Terrorismi rahastamise riskide hindamisel kasutati Maailmapanga<sup>1</sup> tunnustatud metoodikat (vt 1.1.2), mida koostöös riskihinnangu töögruppidega kohendati vastavalt Eesti eripäradele. Hinnang põhineb peamiselt töögrupi koosseisu kuulunud riigiasutuste vaadeldaval perioodil kogutud teabel (statistika, operatiivinfo, rahvusvaheline koostöö partneriteenistustega, muudatused seadustes jne) ning valdkonda puudutavatel rahvusvahelistel ja riigisisestel uuringutel ja analüüsidel.

Hindamisprotsessi esimeses etapis peeti esmased konsultatsioonid asutuste vahel, koguti vajalikku statistikat, kaardistati tüpoloogiad ning viidi läbi täiendkoolitusi ja konsultatsioone metoodikaekspertidega. Teises etapis täideti hindamismoduleid ja tehti analüüs, kasutades nii kvalitatiivset kui ka kvantitatiivset teavet. Korraldati kirjalikud küsitlused ja fookusgrupi intervjuud. Kolmandas etapis koostati aruanne. Erasektor kaasati kirjalike küsitluste ja fookusgruppides toimunud intervjuude kaudu.

Terrorismi rahastamise riskihinnangu koostamise käigus analüüsiti järgmiste terroriorganisatsioonide rahastamisega seonduvaid ohte Eestile, pidades muu hulgas silmas nende rahastusvajadusi, rahastusallikaid ja vahendite liigutamise kanaleid: **ISIS, ISIS-K, Taliban, HAMAS, Kurdi Töölispartei (PKK), Palestiina Islamidžihaad, Hezbollah**; paremäärmuslikud kiirendusgrupid, nagu **Atomwaffen Division, Feuerkrieg Division, Base, Nordic Resistance Movement** jne; **Vene Imperiaalne Liikumine, Venemaa Föderatsiooni eriteenistused**.

<sup>1</sup> World Bank, Washington, Ameerika Ühendriigid, [www.worldbank.org](http://www.worldbank.org).

Lisaks terroriorganisatsioonidele hinnati rahastamise ohte seonduvalt **üksikisikutega** (nii islamiäärmuslus kui ka paremäärmuslus).

Kuna terrorismi rahastamine on seotud üleüldise terrorismiohuga, antakse käesolevas riskihinnangus lühiülevaade ka terrorismiohust Eestis ning ülevaade terrorismi rahastamise valdkonna arengutest. Põhjalikumalt käsitletakse riiklikke terrorismi rahastamise ohte, riiklikke haavatavusi ja sektoripõhiseid haavatavusi. Sektoritest vaadeldi kõiki kohustatud isikuid, kuid põhjalikumalt analüüsiti suurema mõjuga sektoreid. Valiku aluseks oli sektori teenuste maht ja käive, senised juhtumid ja riskitüpoloogiad. Teistes sektorites ei tuvastatud olulisi terrorismi rahastamise riske<sup>2</sup>. Sektoreid puudutavad põhjalikumad andmed on avaldatud riikliku rahapesu riskihinnangu aruandes.

**Käesolevas riskihinnangus ei käsitleta vabaühendusi (mittetulundusühingud ja sihtasutused).** Vabaühendustest koostab Rahapesu Andmebüroo eraldi analüüsi.

## 1.2. FATF-i definitsioonid ja mõisted<sup>3</sup>

FATF määratleb terrorismi rahastamise riski kui kolme teguri kombinatsiooni.

1. **Oht.** Oht on isik, objekt või tegevus, millel on potentsiaal tekitada kahju – näiteks riigile, ühiskonnale, majandusele või finantssüsteemile. Näited: terroristlikud organisatsioonid ja terrorismi rahastamise kanalid.
2. **Haavatavus.** Haavatavus on nõrkus või olukord, mida oht saab ära kasutada või mis soodustab ohu tegevust. Näited: puudulik järelevalve, nõrgad sisekontrollimeetmed, teadmatus riskidest, ebapiisav seadusandlus.
3. **Tagajärg.** Kuigi mitte alati eraldi hinnatav komponent, viitab tagajärg sellele, millist mõju võib oht ja haavatavus koos avaldada – näiteks finantssüsteemi usaldusväärsele või majandusele laiemalt.

FATF-i soovitude kohaselt peaksid riigid ja asutused hindama neid tegureid, et kujundada riskipõhine lähenemine, mis võimaldab suunata ressursid sinna, kus riskitase on kõige kõrgem.

## 1.3. Kasutatud metoodika

Terrorismi rahastamise riske hindasid Eesti ametiasutuste esindajad iseseisvalt, kasutades selleks Maailmapanga terrorismi rahastamise riskihindamise metoodikat ja tööriistu (hindamismooduleid)<sup>4</sup>.

Maailmapanga meeskonna roll piirdus järgmisega: 1) tööriista ehk hindamismoodulite edastamine; 2) tehniliste juhiste andmine tööriista kasutamiseks; 3) riikliku riskihindamise aruande mustandi läbivaatamine ja tagasisidestamine.

<sup>2</sup> Vabaühenduste kohta (mittetulundusühingud ja sihtasutused) valmib eraldi analüüs. Äriühingute teenuse pakkujate kohta on lisatud eraldi kommentaar (6.2.5.).

<sup>3</sup> Siinses raportis lähtutakse terrorismi ja terrorismi rahastamise määratlemisel KarS § 237 sätestatust, mille järgi on terrorikuritegu rahvusvahelise julgeoleku vastase, isikuvastase, elu või tervist ohustava keskkonnastase, välisriigi või rahvusvahelise organisatsiooni vastu suunatud või üldohtliku kuriteo toimepanemine, keelatud relva tootmine, levitamine või kasutamine või vara ebaseadusliku hõivamine või olulises ulatuses rikkumine või hävitamine või arvutiandmetesse sekkumine või arvutisüsteemi toimimise takistamine. Samuti selliste tegude toimepanemisega ähvardamine **kui see on toime pandud eesmärgiga sundida riiki või rahvusvahelist organisatsiooni midagi tegema või tegemata jätma või tõsiselt häirida riigi poliitilist, põhiseaduslikku, majanduslikku või ühiskondlikku korraldust või see hävitada või tõsiselt häirida rahvusvahelise organisatsiooni tegevust või see hävitada või tõsiselt hirmutada elanikkonda.**

<sup>4</sup> Terrorist Financing Risk Assessment Tool (2022).

Hindamismoodulitesse sisestatud andmed, statistika ja muu teave, samuti riikliku riskihindamise protsessi käigus tehtud järeldused, tõlgendused ja hinnangud kuuluvad Eesti riikliku riskihinnangu projektis osalejatele ega kajasta Maailmapanga seisukohti.

Maailmapanga meetodika juhendid ja hindamismoodulid on avalikult kättesaadavad organisatsiooni kodulehel<sup>5</sup>. Rahandusministeeriumi ja Maailmapanga koostöö raames sai riikliku riskihinnangu koostamise projekti kogu meeskond koolitus- ja nõustamisteenuse Maailmapanga meetodika rakendamiseks ja kohendamiseks vastavalt Eesti eripäradele.

Terrorismi rahastamise riskihindamise tööriist käsitleb riski kahe põhikomponendi – ohu ja haavatavuse – koosmõjuna. Riskide tagajärgi ei hinnatud eraldi, vaid need on integreeritud ohtude ja haavatavuse analüüsi, kasutades selleks kaalutegureid, eeltingimusi ning võrgustikupõhist struktuuri. Sellist meetodikat rakendati nii riiklikul kui ka sektoripõhisel tasandil.

Hindamisprotsess algas ohtude tuvastamisega, mille käigus analüüsiti, millised allikad võivad terrorismi rahastamist mõjutada – näiteks rahvusvahelised võrgustikud ja rahavoogude kanalid. Seejärel hinnati riikliku tõkestamise süsteemi võimekust ja haavatavusi, näiteks puudused seadusandluses või järelevalves. Kolmandaks viidi läbi sektoripõhine analüüs. Iga sektori puhul hinnati kontrollimeetmete olemasolu, tõhusust ja järelevalve taset ning turuosaliste riskiteadlikkust.

Maailmapanga terrorismi rahastamise riskihindamise meetodikas kasutatakse ohtude ja haavatavuse tasemete hindamiseks punktiskaalat, mis aitab määrata, kui vastuvõtlik on sektor või süsteem terrorismi rahastamise riskidele.

## 1.4. Analüüsis kasutatud ohtude ja haavatavuste hindamiskriteeriumid

**Oht** viitab tõenäosusele, et terrorismi rahastamine võib aset leida riigi territooriumil või Eesti finantsüsteemi kaudu. Üldiselt on hinnangu aluseks nii terroristlike organisatsioonide võimalik kohalolek riigis kui ka teadaolevad või potentsiaalsed terrorismi rahastamise juhtumid.

**Haavatavus** viitab sellele, kui vastuvõtlik on sektor või süsteem terrorismi rahastamisele, sõltumata sellest, kas oht tegelikult realiseerub. Laialt võttes peegeldab see eelkõige ennetus- ja kontrollimeetmete tugevust või nõrkust, sh seadusandlust, järelevalvet, sisekontrolli ja riskijuhtimist. Mida nõrgemad või ebatõhusamad need mehhanismid on, seda kõrgem on süsteemi haavatavuse tase.

**Risk** on ohu ja haavatavuse koostoime.

Terrorismi rahastamise töögrupi eksperdid sisustasid hindamismoodulid hindamiskriteeriumide rohkete alakriteeriumide kaupa, kus skaala oli kümne- või sajapunktiline vahemikus 0–1. Hinnanguskaala jaotus järgmiselt: 0 – ei eksisteeri, 0,1 – peaaegu pole, 0,2 – **väga madal**, 0,3 – **madal**, 0,4 – **madal-keskmine**, 0,5 – **keskmine**, 0,6 – **keskmine-kõrge**, 0,7 – **kõrge**, 0,8 – väga kõrge, 0,9 – peaaegu suurepärase, 1,0 – suurepärase.

Maailmapanga terrorismi rahastamise riskihindamise meetodikat kasutades kujunes ohu ja haavatavuste ning riskitaseme lõplik hinnang sisemise loogika alusel automaatselt pärast hindamismoodulite täitmist, kus eksperdid andsid hinnangud konkreetsete hindamiskriteeriumide alusel.

<sup>5</sup> World Bank, Disclaimer and Terms of Use: National Money Laundering and Terrorist Financing Risk Assessment Toolkit, <https://www.worldbank.org/en/topic/financialmarketintegrity/brief/national-money-laundering-and-terrorist-financing-risk-assessment-toolkit-disclaimer-and-terms-of-use>.

## 1.4.1. Riiklike ohtude hindamiskriteeriumid

### Hindamiskriteeriumid riiklike ohtude analüüsil:

#### Terroristlik tegevus – riigisisene ja piiriülene oht:

- terrorismist tingitud surmajuhtumite määr hindamisperioodil,
- terroriaktide esinemissagedus hindamisperioodil,
- terroriakte toetavate kaasnevate tegevuste ulatus hindamisperioodil,
- terrorismi mõju jurisdiktsioonile hindamisperioodil.

#### Terroristlikud üksused – riigisisene ja piiriülene oht:

- jurisdiktsioonis aktiivsed terroriorganisatsioonid, rühmitused ja/või (kategooriatena) isikud,
- rahastamisvajaduse tase,
- hinnanguline vahendite kogumise aktiivsus,
- rahastamisallikad,
- varatüübid,
- vahendite liigutamise kanalid,
- isikute vahendite liigutamise ulatus mitteametlike või variteenuste kaudu (nt *hawala*), kaubanduse (sh ekspordikontrolli alla kuuluvad kaubad) ja salakaubaveo (sh sularahakullerid) abil.

#### Poolehoidjad – riigisisene ja piiriülene oht:

- terrorismi rahastamisega seotud uurimiste, süüdistuste, süüdimõistmiste ja õigusabitaotluste hulk, mis puudutavad poolehoidu terrorismiideoloogiale (ka juhul, kui puudub otsene seos terrorirünnakute, terroristlike organisatsioonide või isikutega);
- finantsluure, sealhulgas kahtlaste tehingute teadete alusel (edaspidi „TFR-id“) kogutud info isikute kohta, kel on arvatavasti terrorismiideoloogiate suhtes poolehoid;
- juhtumid, kus isikud on reisinud Eestist piirkondadesse, kus esineb aktiivne terrorismioht;
- ülekanded (nii sissetulevad kui ka väljaminevad piirkondadesse, kus esineb aktiivne terrorismioht;
- jurisdiktsiooni kogukonnad, kellel on tihedad sidemed piirkondadega, kus esineb aktiivne terrorismioht, ning sellega kaasnev võimalik terrorismi rahastamise oht;
- avalike allikate, teadusuuringute, meediaraportite ja valdkonna ekspertide hinnangutele tuginev info isikute kohta, kel on terrorismiideoloogiate suhtes poolehoid.

#### Naaberriigid – riigisisene ja piiriülene oht:

- naaberriikide aktiivse terrorismiohu tase,
- hinnanguline terrorismiohvrite arv naaberriikides hindamisperioodi jooksul, kasutades vajaduse korral hindamisskaalat,
- terrorirünnakute hulk naaberriikides viimase viie aasta jooksul,
- terrorismiohuga seotud rahastamise tase naaberriikides ning selle seos terrorismiohu tasemega,
- naaberriikide terrorismiohuga seotud rahastamisvajaduste mõju Eestile,
- avalike allikate, teadusuuringute, meediaraportite ja valdkonna ekspertide hinnangutele tuginev info isikute kohta, kel on terrorismiideoloogiate suhtes poolehoid.

#### **Finants- ja transpordikeskused – riigisisene ja piiriülene oht:**

- jurisdiktsiooni tähtsus rahvusvahelise või piirkondliku finantskeskusena,
- jurisdiktsiooni tähtsus ümberlaadimise ja logistika keskpunktina,
- jurisdiktsiooni tähtsus kaubanduspiirkonnana.

#### **Strateegilised kaubad ja teenused – riigisisene ja piiriülene oht:**

- jurisdiktsiooni juriidiliste isikute osalus strateegiliste kaupade ja teenuste võimaldamisel terrorismiohuga piirkondadesse, sh piirkondadesse, mis on terroristlike organisatsioonide kontrolli all,
- jurisdiktsiooni valitsusasutuste, sealhulgas riigiettevõtete osalus strateegiliste kaupade, teenuste ja rahalise abi võimaldamisel piirkondadesse, kus esineb aktiivne terrorismioht,
- jurisdiktsiooni mittetulundusühingute kaudu strateegiliste kaupade, teenuste ja rahalise abi jõudmine piirkondadesse, kus esineb aktiivne terrorismioht.

### **1.4.2. Riiklike haavatavuste hindamiskriteeriumid**

**Riiklike haavatavuste hinnang** põhineb järgmiste tegurite analüüsil: 1) riigi võimekus terrorismi rahastamise ohte tõkestada, 2) sektorite haavatavused koostoimes kontrollimeetmete olemasolu, tõhususe ja turuosaliste teadlikkusega.

#### **Hindamiskriteeriumid<sup>6</sup> riigi võimekusel terrorismi rahastamise ohte tõkestada:**

- terrorismi rahastamise tõkestamise poliitika ja strateegia kvaliteet,
- terrorismi rahastamise kuriteo määratluse tõhusus,
- tolli- ja piirikontrollide tõhusus terrorismi rahastamise tõkestamisel,
- terrorismi rahastamist puudutava teabe kogumise ja töötlemise kvaliteet,
- terrorismi rahastamise uurimise kvaliteet,
- terrorismi rahastamise eest süüdistuse esitamise kvaliteet,
- terrorismi rahastamise eest kohtumõistmise kvaliteet,
- terrorismi rahastamisega seotud varade konfiskeerimise ja arestimise mehhanismide kvaliteet,
- terrorismi rahastamist puudutavate sihipäraste finantssanktsioonide kvaliteet seonduvalt terrorismiga ja terrorismi rahastamisega,
- strateegilise varustuse, kaupade ja teenuste kontroll seonduvalt konfliktipiirkondadega.

#### **Hindamiskriteeriumid sektorite haavatavuste analüüsil:**

##### **Sektori loomupärane haavatavus:**

- sektori sobivus/kasulikkus terrorismi rahastamisel,
- sektori maht ja käive,
- kliendibaasi profiil,
- väljaminevad rahvusvahelised tehingud,
- väljaminevad rahvusvahelised tehingud kõrgema riskitasemega jurisdiktsioonidesse,
- sissetulevad rahvusvahelised tehingud,
- sissetulevad rahvusvahelised tehingud kõrgema riskitasemega jurisdiktsioonidest,
- sularaha kasutamine,
- esindajate, teenusepakkujate ja vahendajate kasutamine,
- muud haavatavustegurid.

---

<sup>6</sup> Tegu on katuskriteeriumidega, millel olid omakorda alakriteeriumid.

**Terrorismi rahastamise tõkestamise kontrollide kvaliteet:**

- terrorismi rahastamise tõkestamise õigusliku raamistiku ulatus,
- järelevalve- ja kontrollitegevuste tõhusus,
- halduskaristuste kättesaadavus ja kohaldamine,
- kriminaalkaristuste kättesaadavus ja kohaldamine,
- turule sisenemise kontrollimehhanismide kättesaadavus ja tõhusus,
- sektori töötajate ausus ja usaldusväärsus,
- sektori töötajate teadmised ja teadlikkus terrorismi rahastamise tõkestamise valdkonnast,
- vastavuskontrolli tõhusus,
- rahvusvaheliste finantssanktsioonide (edaspidi „TFS“) rakendamise tulemuslikkus,
- kahtlaste tehingute seire ja neist teatamise tõhusus,
- tegelike kasusaajate andmete kättesaadavus ja juurdepääs neile,
- usaldusväärse isikusamasuse tuvastamise infrastruktuuri olemasolu,
- juurdepääs usaldusväärsetele infoallikatele.

## 1.5. Andmete kogumine

Riskide hindamisel toetuti nii ametkondlikest kui ka avalikest allikatest kogutud teabele. Ametkondlikest allikatest olid olulisel kohal Kaitsepolitsei ameti teave ja Rahapesu Andmebüroo statistilised andmed, prokuratuuri kriminaalstatistika jm. Lisaks kasutati andmeid erasektori kirjalikest küsitlustest ja fookusgruppide intervjuudest. Kõik hindamisel kasutatud andmed koguti aastate lõikes vaadeldava perioodi, st aastate 2020–2024 kohta.

## 2. Kokkuvõte

**Tabel 1.** Riiklikud terrorismi rahastamise riski tasemed

Kategooria	Ohutase	Haavatavuse tase	Riskitase
Sisemine	madal	keskmisest madalam	keskmisest madalam
Eestist lähtuv	keskmine	keskmisest madalam	keskmine
Väline	keskmine	keskmisest madalam	keskmine
Transiidist tulenev	keskmisest kõrgem	keskmine	keskmisest kõrgem

Terrorismi rahastamise riskitase kujuneb kahe põhikomponendi – ohu ja haavatavuse – koostoimes.

### Riiklikud terrorismi rahastamise ohud

Riiklik terrorismi rahastamise oht jaguneb neljaks: **1) sisemine** oht, **2) Eestist lähtuv** oht teistele riikidele, **3) väline** oht ja **4) transiidist tulenev** oht.

**Sisemise ohu** all on peetud silmas Eesti oludest tulenevaid ohte, kus kõik terrorismi rahastamise faasid toimuvad Eestis. **Eestist lähtuva ohu** all on peetud silmas Eesti jurisdiktsioonist lähtuvat ohtu teistele riikidele. **Välise ohu** all on mõeldud mujalt jurisdiktsioonidest Eestile lähtuvat ohtu. **Transiidist tuleneva ohu** all peetakse silmas olukorda, kus välismaalased väljaspool Eestit kasutavad terrorismi rahastamise eesmärgil Eesti jurisdiktsioonis pakutavaid tooteid ja teenuseid. Samuti võib see tähendada vahendite liigutamist Eesti kaudu füüsilisel moel. Vahendid ei jää Eestisse, vaid liiguvad siit läbi.

**Sisemine terrorismi rahastamise ohu tase on madal.** Eestis ei tegutse ühtki terroristlikku organisatsiooni ega nende rakukest ning siin ei ela ka nende võitlejaid. Äärmuslikult meelestatud isikute hulk, kellega võiks kaasneda terrorismi rahastamine, on madal. Terroristlikul eesmärgil kogutud vahendite kasutamise ohutase Eestis on madal. Suurim oht on radikaliseerunud üksikisikud ning Venemaa Föderatsioonist mõjutatud isikute oht. Ka vägivaldse paremääruslusega seotud juhtum puudutas üksikisikuid (vt näidisjuhtum 1). Vaadeldaval perioodil Eesti-siseseid terrorismi rahastamise juhtumeid ei esinenud.

**Eestist lähtuva terrorismi rahastamise ohu tase on keskmine.** Oluline oht on heategevuse sildi all toimuvad rahakogumiskampaaniad välisriikide jaoks, millesse võivad panustada ka Eesti elanikud (vt näidisjuhtum 2). Eriti puudutab see Gaza ja Venemaaga seotud terroristlike organisatsioonide toetamist. Eesti konteksti mõjutab ka ISIS-K aktiveerumine Kesk-Aasis, seda Kesk-Aasia päritolu tööliste kaudu, kes saavad kodumaale vahendeid piiriüleste makseteenuste ja finantseerimisasutuste kaudu. Ära tuleb märkida e-residentsuse programmi terrorismi rahastamise eesmärgil ärakasutamise oht ettevõtluse kattevarjus (vt näidisjuhtum 3 ning punkt 6.2.5).

**Välise terrorismi rahastamise ohtu tase on keskmine.** Suurim ja püsiv ohuallikas on Venemaa, kes agressoriina otsib Eestis oma huvides terroriakte toime panna soovivaid isikuid ning lubab neid ka rahastada. Lähinaabrusest on Skandinaavias ja Venemaal arvukas moslemikogukond, kelle seas on ka radikaalset islamiusku levitavaid isikuid ja tagasipöördunud välisvõitlejaid. Skandinaavias leidub ka küllaltki arvukalt paremäärmuslasi. Terrorismiohu tase, mis on seotud ka rahastamisega, on Balti riikides madal.

**Transiidist tuleneva terrorismi rahastamise ohtu tase on keskmisest kõrgem.** Peamine oht on seotud korrespondentsuhetega, kus välisriigis elav välisriigi elamislooga terrorismiseosega või radikaliseerunud isik võib soovida teha tehinguid terrorismi rahastamise eesmärgil Eesti teenusepakkuja kliendi vahendusel (vt näidisjuhtumid 5 ja 6). See puudutab nii VIBAN-teenuse pakkumist krediitiasutuste poolt kui ka endiselt küllaltki suurt virtuaalvääringu teenusepakkujate (edaspidi „VASP“) sektorit. Ehkki Eesti ei ole märkimisväärne reisi-, kauba- ega transpordikeskus, on üks ohuallikaid Skandinaavias elavate terrorismi- või radikaalse islami seostega isikute ja välisvõitlejate reisimine läbi Eesti. Eelkõige peitub siin oht sularaha, deebetkaartide ja sidevahendite transportimises konfliktipiirkondadesse.

## Haavatavused

### Riiklikud haavatavused

Riiklike haavatavuste hinnang põhineb järgmiste tegurite analüüsil: 1) riigi võimekus terrorismi rahastamise ohte tõkestada, 2) sektorite haavatavused ning kontrollimeetmete olemasolu, tõhusus ja turuosaliste teadlikkus. Riiklike haavatavusi vaadeldakse kategooriate kaupa: sisemine, Eestist lähtuv, väline, transiidist tulenev. Riikliku haavatavuse hinnangusse panustab ühelt poolt riigi võimekus konkreetset ohtu tõkestada ja teiselt poolt üldine sektorite<sup>7</sup> haavatavus.

**Peamine haavatavus on jätkuvalt see, et Eesti finantsüsteemi turuosalisi ja nende teenuskeskkondi võidakse ära kasutada vahendite edastamisel.** Arvestatav oht kaasneb välismaiste lepingupartneritega tehtud tehingutega, näiteks Eesti tegevuslooga teenusepakkujate **korrespondentsuhetega**, mille käigus ei kohaldata hoolsusmeetmeid piisaval määral.

Terrorismi rahastamise tõkestamise **riikliku süsteemi haavatavuse tase on keskmisest madalam**. Suurimaks probleemkohaks on teabevahetus EL-i mitte kuuluvate kolmandate riikidega ning riikidega, kellega puudub õigusala koostöö (sh Venemaaga).

### Sektorite haavatavused

Sektorite riskitasemesse panustab ühelt poolt oht ja teiselt poolt haavatavus. Ohutaset mõjutavad riiklik terrorismi rahastamise oht, ohud seonduvalt tüpoloogiatega, ohud seonduvalt sektorispetsiifiliste asjaoludega. Sektori haavatavuse taset mõjutavad 1) sektori loomupärane haavatavus ja 2) terrorismi rahastamise tõkestamise kontrollide kvaliteet, mis omakorda jagunevad alakriteeriumideks.

<sup>7</sup> Üldine sektorite haavatavuse hinnang (keskmisest madalam) võtab arvesse sektorite haavatavusi koostoimes kontrollimeetmete olemasolu, tõhususe ja turuosaliste teadlikkusega (vt 6.2).

Sektoritest vaadeldi kõiki kohustatud isikutena<sup>8</sup> käsitletavaid sektoreid, kellest põhjalikumalt analüüsiti valitud sektoreid. Valiku aluseks oli sektori teenuste maht ja käive, senised juhtumid ja riskitüpoloogiad. Üksikasjalikumaks hindamiseks valiti järgmised sektorid: virtuaalvääringu teenuse pakkujad (VASP-id), krediidasutused, makseasutused, sh piiriülesed makseteenused (rahasiirde teenuse pakkujad ja valuutavahetajad) ja e-raha asutused<sup>9</sup> (nii sise- kui ka välismaised) ning ühisrahastusteenuse pakkujad. Teistes sektorites ei tuvastatud olulisi terrorismise riske<sup>10</sup>. Eraldi kommentaar on lisatud äriühingute teenuse pakkujate ja e-residentsuse programmi kohta (vt punkt 6.2.5).

Nii krediidasutuste kui ka virtuaalvääringu teenuse pakkujate peamine haavatavus tuleneb korrespondent-suhetest. Krediidasutuste puhul on leevendavaks asjaoluks sektori suur teadlikkus ja hoolsusmeetmete kohaldamise tase. VASP-ide teadlikkus terrorismi rahastamise riskidest on ebaühtlane, kuid see paraneb järjepidevalt. Makseasutuste peamine haavatavus on seotud keerukusega tuvastada kolmandates riikides tegutsevate makseagentide kaudu vahendite saatja-saaja. E-raha asutuste puhul on suurimaks väljakutseks piiratud infovahetuse võimalused piiriüleste e-raha asutustega ning tihti leebemad tunne-oma-klienti nõuded.

Virtuaalvääringu teenuse pakkujate, krediidasutuste ja ühisrahastusteenuse pakkujate haavatavuse tase on keskmisest madalam, makseasutuste puhul keskmine. Virtuaalvääringu teenuse pakkujate ja makseasutuste puhul on ohutase keskmine, krediidasutuste puhul keskmisest madalam ja ühisrahastusteenuse pakkujate puhul madal. Jääkriski tase on kõige kõrgem virtuaalvääringu teenuse pakkujate ja makseasutuste sektoris – keskmine –, krediidi- ja ühisrahastusteenuse pakkujate puhul on see keskmisest madalam.

**Tabel 2. Terrorismi rahastamise riskihinnangu tulemused sektorite lõikes**

Sektor	Terrorismi rahastamise ohu tase	Haavatavuse tase	Jääkriski tase
Virtuaalvääringu teenuse pakkujad	keskmine	keskmisest madalam	keskmine
Krediidasutused	keskmisest madalam	keskmisest madalam	keskmisest madalam
Makseasutused, sh piiriülesed makseteenused (rahasiirde teenuse pakkujad, valuutavahetajad ja e-raha asutused) <sup>11</sup>	keskmine	keskmine	keskmine
Ühisrahastusteenuse pakkujad	madal	keskmisest madalam	keskmisest madalam

<sup>8</sup> RahaPTS § 2. Vt <https://www.riigiteataja.ee/akt/113032019126?leiaKehtiv>.

<sup>9</sup> E-raha asutused pakuvad näiteks selliseid teenuseid nagu Paysera, Revolut, Koronapay, OpenPayd, Papaya, Paysafe, Payward jne.

<sup>10</sup> Vabaiühenduste kohta (mittetulundusühingud ja sihtasutused) valmib eraldi analüüs.

<sup>11</sup> E-raha asutused on nt Paysera, Revolut, Koronapay, OpenPayd, Papaya, Paysafe, Payward jne teenused. E-raha asutuste all on mõeldud nii sise- kui ka välismaiseid.

## 3. Terrorismioht Eestis

Selles peatükis esitatakse üksikasjalikud järeldused **terrorismi üldise ohutaseme kohta**. Alljärgnevad 4. ja 5. peatükk annavad ülevaate konkreetsetest ohtudest, mis on seotud **terrorismi rahastamisega**.

### 3.1. Islamiäärmuslusest lähtuv oht

Islamiäärmusliku terrorirünnaku ohu tase Eestis on **madal**.

Eestis ei ole tuvastatud ühtegi islamiäärmuslikku terroristlikku organisatsiooni või selle rakukest ega ka alaliselt siin elavaid võitlejaid. Eestis on suhteliselt väike islamikogukond, kelle seas on äärmuslike vaadetega inimesi väga vähe, valdav enamik kogukonnast pooldab mõõdukat islamiusku. Ühtegi islamiäärmuslusest ajendatud terroriakti aastatel 2020–2024 Eestis toime ei pandud.

Suurimaks ohuks on radikaalsest islamiideoloogiast mõjutatud üksikisiku terroristlik tegevus. Vaadeldaval ajavahemikul ühtki sellist isikut Eestis tuvastatud ei ole. Küll on tuvastatud potentsiaalse ohuallikana mitmeid vaimse tervise probleemidega isikuid, kes ei oma religioosset ega ideoloogilisi tõekspidamisi. Üksikisikute radikaliseerumist on keeruline avastada, seepärast ei saa neist lähtuvat ohtu täielikult välistada. Lisaks on vaadeldaval perioodil esinenud üksikuid juhtumeid, kus naaberriikides elavad endised islamistlikud välisvõitlejad ja terrorismiseostega isikud on Eestit külasthanud või siit läbi reisinud.

### 3.2. Vägivaldsest paremäärmuslusest lähtuv oht

Paremäärmusliku terrorirünnaku ohu tase Eestis on **madal**.

Seonduvalt vägivaldse paremäärmuslusega mõisteti 2021. aastal süüdi isik, kes postitas 2019. a Facebookis Siege'i<sup>12</sup> kultuuri järgivas vestlusgrupis noorpoliitikute suunal ähvardusi. Vaadeldaval ajavahemikul tuvastati Eestis kolm alaealist terroristliku ühenduse Feuerkrieg Division<sup>13</sup> liiget, kes mõisteti 2025. aasta jaanuaris kohtus süüdi terroristlikku gruppi kuulumises. Süüdimõistetud isikud piirdusid tegevuses üleskutsetega ja reaalseid vägivallaakte toime ei pannud.

Eestis on paremäärmuslaste hulk suhteliselt väike ja nende seas ei ole tuvastatud reaalseid terroriakte toime panna soovivaid isikuid. 2024. aasta seisuga ühtegi paremäärmuslikku terroriorganisatsiooni Eestis ei tegutse. Ka vägivaldse paremäärmusluse puhul on suurim oht potentsiaalse üksiktegutseja teke.

<sup>12</sup> *Siege'i* kultuur – katustermin John Masoni ideoloogiast lähtuvatele liikumistele, mille järgi tuleks viia läbi terroriakte väikeste ja sõltumatute üksustena. Eesmärk on kutsuda esile globaalse poliitilise süsteemi kokkuvarisemine ja rassisõda. Vt ka: <https://www.counterextremism.com/james-masons-siege-ties-to-extremists>.

<sup>13</sup> Feuerkrieg Division – terroriorganisatsioon, mis lähtub ühiskonna kokkuvarisemise kiirendamise (*accelerationism*) ideoloogiast.

### 3.3. Venemaa Föderatsioonist lähtuv oht

Venemaa Föderatsioonist lähtuva ohu tase oht on **keskmine**.

Terrorismi vaatest lähtub suurim oht Eestile Venemaa Föderatsioonist (edaspidi „VF“), mis intensiivistas tegevust NATO ja Euroopa Liidu riikide vastu pärast Ukraina vastu sõja alustamist 2022. aastal. Sellega seoses tuleb ära märkida ultranatsionalistlik organisatsioon **Vene Imperiaalne Liikumine**<sup>14</sup> (edaspidi „VIL“) ja selle sõjaline tiib **Vene Imperiaalne Leegion**. VIL on seotud Vene eriteenistustega ning värbab väljaspool VF-i territooriumi aktiivselt toetajaid diasporaa seast.

Terroriohu allikaks on ka **VF-i eriteenistuste tegevus**. Aastatel 2023–2024 leidsid nii Eestis kui ka teistes Balti riikides aset VF-i Kaitseministeeriumi Luure Peavalitsuse (edaspidi „GRU“) poolt organiseeritud erinevad rünnakud. Ründeobjektiks olid II Maailmasõjaga seotud monumendid ja praegused avaliku elu tegelased – poliitikud ja ajakirjanikud ning nende vara (autod). Eesmärgiks oli ühiskonnas hirmu õhutada ja konflikti tekitamine. VF-i eriteenistused üritavad rünnakute toimepanemiseks värvata kohapealt vene rahvuslastest äärmuslasi, aga ka tavalisi kurjategijaid.

### 3.4. Vasakäärmuslusest lähtuv oht

Vasakäärmuslike terroriorganisatsioonide ja üksikisikuid Eestis tuvastatud ei ole. Neist lähtuv **ohutase on madal**.

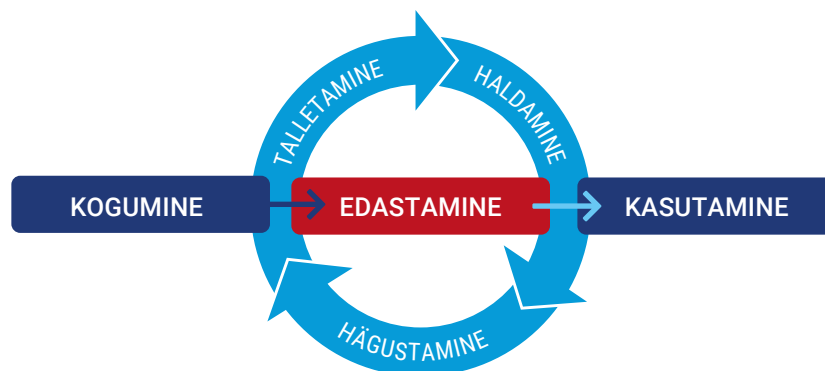
---

<sup>14</sup> Ukraina-vastases agressioonis osalemise tõttu käsitleb USA organisatsiooni terroristlikuna; Euroopa Liidu tasandil on lisatud sanktsiooninimekirja organisatsiooni juhtfiguurid.

## 4. Terrorismi rahastamise üldine ülevaade

Eestis kehtiva seadusandluse<sup>15</sup> järgi on terrorismi rahastamine terrorikuriteo rahastamine või muul viisil teadlik toetamine, vahendite kättesaadavaks tegemine või kogumine. Samuti loetakse terrorismi rahastamiseks terroristliku ühenduse või isiku, kelle tegevus on suunatud terrorikuriteo toimepanemisele, rahastamist või muul viisil toetamist, vahendite kättesaadavaks tegemist või kogumist või muul viisil teadvalt toetamist.

**Joonis 1. Terrorismi rahastamise faasid**



Terrorismi rahastamise juures eristatakse tavapäraselt kolme faasi: rahade kogumine, edastamine ja kasutamine. Analüütilisel eesmärgil on hakatud eristama terrorismi rahastamise all ka vahendite hägustamist, talletamist ja haldamist<sup>16</sup>. Siinses riskihinnangus on vaadeldud lihtsuse huvides kolme faasi.

Terrorismi rahastamise riskihinnangu koostamise käigus analüüsiti järgmiste terroriorganisatsioonide rahastamisega seonduvaid ohte Eestile, pidades muu hulgas silmas nende rahastusvajadusi, rahastusallikaid ja vahendite liigutamise kanaleid: **ISIS, ISIS-K, Taliban, HAMAS, Kurdi Töölispartei (PKK), Palestiina Islamidžihaad, Hezbollah**; paremäärmsuslikud kiirendusgrupid, nagu **Atomwaffen Division, Feuerkrieg Division, Base** jne; **Vene Imperiaalne Liikumine, Venemaa Föderatsiooni eriteenistused**. Lisaks terroriorganisatsioonidele hinnati rahastamise ohte seonduvalt **üksikisikutega** (nii islamiäärmsuslus kui ka paremäärmsuslus).

<sup>15</sup> Terrorismi rahastamise määratleb Karistusseadustik, kus terrorismi ja selle rahastamist käsitleb paragrahv 237<sup>1-6</sup> Terrorikuriteo ja selle toimepanemisele suunatud tegevuse rahastamist ning toetamist § 237<sup>3</sup>; terroristlikul eesmärgil reisimise korraldamist, rahastamist ja toetamist § 237<sup>6</sup>. RahaPTS lähtub terrorismi rahastamise käsitlemisel nimetatud KarS-i paragrahvidest.

<sup>16</sup> Davis, Jessica (2021). Prevention of Terrorist Financing. – Alex P. Schmid (Ed.), Handbook of Terrorism Prevention and Preparedness. The Hague: ICCT (International Centre for Counter-Terrorism), 444–473.

Vt <https://www.icct.nl/handbook-terrorism-prevention-and-preparedness>.

Üldistatult vajavad terroristlikud organisatsioonid vahendeid sõltuvalt suurusest, tegutsemishaardest ja eesmärkidest. Organisatsioonid vajavad vahendeid palkadeks, väljaõppe korraldamiseks, reisimiseks, konspiratsioonimeetmete rakendamiseks, logistikaks, propagandaks, uute liikmete ja toetajate värbamiseks jne. Islamiäärmusluse puhul võib lisanduda hukkunu lähedaste toetamine. Vägivaldse paremäärmusluse puhul vajab organisatsioon tihtipeale vahendeid ka õiguskulude katteks. Kui organisatsioon kontrollib territooriumi, lisanduvad siia kulutused selle haldamiseks ja ühtsuse hoidmiseks. Üksiktegutseja soovitud võib terrorirünnaku toimepanemiseks kasutada käepäraseid vahendeid.

Vahendite **kogumise** vaatest piisab üksiktegutsejal omarahastusest: palk, laenud, sotsiaalabi, lähedaste toetus, sh vanematelt saadud taskuraha. Viimasega oli tegu ka Eestit puudutanud kriminaalasjas seonduvalt vägivaldse paremäärmuslusliikumise (vt näidisjuhtum 1) – alaealised olid vanemate ülalpidamisel. Terroristlikud organisatsioonid võivad koguda rahalisi vahendeid annetuste ja toetuste (MTÜ-d, ühisrahastuskampaaniad) näol, näilise legaalse äritegevuse abil, kohaliku elanikkonna maksustamise või organiseeritud kuritegevuse kaudu (väljapressimine, röövimine, narkoäri, inimkaubandus, pettused jne). Vahendite saatmist ühisrahastuskampaaniate näol konfliktipiirkondadesse on üksikjuhtudel täheldatud ka Eestis. Vägivaldse paremäärmusluse puhul on iseloomulik raha kogumine ja ideoloogia levitamine võitlusklubide ja spordisaalide kaudu, sümbolikaga kaupade müügiga, ürituste korraldamisest saadava tuluga (kontserdid ja võistlused), muusika produtseerimise ja müügiga, iserahastamisega (annetused, liikmetasud, töötasud jne) ning kinnisvara rendiga.

Vahendite **edastamiseks** võidakse kasutada terrorismi rahastamise eesmärgil nii traditsioonilisi ülekandemeetodeid (laia globaalse makseagendivõrgustikuga makseteenused) kui ka moodsaid infotehnoloogilisi kanaleid nagu nt e-raha asutused ja virtuaalväeringud. Kõike seda on täheldada ka Eesti kaudu, nagu allpool välja toodud. Jätakuvalt on kasutusel nii *hawala*-süsteem<sup>17</sup> kui ka sularahakullerid. Tuleb märkida, et Eestis ei ole tuvastatud *hawaladar*'e ehk *hawala*-teenuse pakkujaid nende klassikalises mõttes, küll aga võib täheldada võimalikke *hawala*-tunnustega arvelduskontode kasutamist. Selle kohta on vaadeldaval perioodil esitanud krediidasutused Rahapesu Andmebüroole ka teateid. Terrorismi rahastamine võib toimuda ka sümbioosina eelmainitud erinevatest teenustest.

Virtuaalväeringu teenuse pakkujate sektoris võib täheldada kokkupuuteid kolmandates riikides tegutsevate veebikasiinode ja kaughasartmängude korraldajatega. Kuna selliste kasiinode ja mängukorraldajate klientideks on olnud isikuid, kes on omanud plokiahelas toimunud tehingute analüüsimisel puutumust ka terroristlikuna kategoriseeritud<sup>18</sup> krüptoadressidega, siis kätkeb see endas teatavat terrorismi rahastamise ohtu. Teadaolevate juhtumite puhul ei ole aga õnnestunud tõendada, et kasiinode ning mängukorraldajate sektorit oleks teadlikult kasutatud terrorismi rahastamiseks.

Nii Eesti kui ka kogu maailma infotehnoloogiline areng on täiendanud ka terrorismi rahastamise kanaleid: erisuguste maksevahendajate ja virtuaalväeringu teenuse pakkujate ülekandetasud globaalsete tehingute puhul on osutunud teatud juhtudel soodsamaks kui traditsioonilised pangamaksud. Globaalsete ettevõtete makselahendused pakuvad suuremat tehingu kiirust ja pahahti ka täiendavat anonüümsust, mida kasutavad ära kurjatelijad. Terrorismi rahastamisel jääb **suurem osa tehingutest vahemikku mõnest eurost kuni paarikümne euroni**. Ehkki on erandeid, nähtub terrorismi rahastamisele viitavatest teadetest Eesti kontekstis just väikeste summade kasutamine. Terroristlikud organisatsioonid ei jaga reeglina oma kampaaniates enam

<sup>17</sup> *Hawala* – Lähis-Idas, Aafrikas ja Aasias levinud, usaldusel põhinev traditsiooniline raha edastamise viis, kus raha ülekandmiseks ei pea seda füüsiliselt sihtkohta saatma. *Hawala* haldur (*hawaladar*) võib sularaha asemel vastu võtta ka väärisesemeid, kinnis- või vallasvara, mille väärtus arvestatakse ümber adressaadile antavasse rahasse.

<sup>18</sup> NBCTF – National Bureau for Counter Terror Financing of Israel.

avalikult maksedetaile, täpsemad rahastamisjuhised edastatakse privaatsetel suhtlusplatvormidel ning kinnistes jututubades. Üha enam on laiemale kasutajaskonnale kättesaadavaks saamas arenenud tehisintellekt, mis võimaldab luua süvavõltsingu abil realistlikku valeidentiteeti ning üles seada rahastamiskampaaniaid, mida toetavad realistlikena näivad võltsvideod. Ehkki Eesti kontekstis ei ole tuvastatud süvavõltsinguid, märkavad teenusepakkujad võltsitud dokumente.

Terrorismi rahastamise korral varjatakse teenuse pakkuja eest **tegevuse eesmärki, summa võib olla väga väike, vahendite päritolu võib olla ka seaduslik**. Samuti võidakse **varjata ka tehingu taga olevat isikut**, kasutades selleks näiteks **pereliikmeid**, varastatud või **võltsitud dokumente** (lisandub **süvavõltsingu** üha kasvav oht *selfie*'de puhul). Pereliikmete kasutamist ning varastatud ja võltsitud dokumentide kasutamist on näha ka Rahapesu Andmebüroole esitanud teadetest – eelkõige seonduvalt virtuaalvääringu teenuse pakkujate klientidega. Terrorismi rahastamise toetamise kahtluseni jõudmine võib lisaks üldisele **seirele ja tööriistade oskuslikule** kasutamisele vajada **teadmisi, mis puudutavad teisi kultuuriruumi ja geopoliitilisi konflikte**. Vägivaldse äärmuslusideoloogia toetaja tuvastamine eeldab laiemalt **erinevate ideoloogiate ja nende sümbolite head tundmist**. Lisaks on äärmuslusideoloogiate puhul võimalik täheldada aina enam nende ähmastumist ja segunemist – seda mitte ainult taktikate ja strateegiade vaatest, vaid üksikisik paneb ideoloogia kokku omale sobivatest komponentidest.

Harjumuspäraselt on terrorismivastane võitlus ja seetõttu terrorismi rahastamise tõkestamine koondanud tähelepanu geograafilisele riskile. Paraku ei ole selline lähenemine tänapäeval enam piisav, sest islamiradikaalide hulk on kasvanud ja kasvab ka geograafilisest sõelast välja jäävates lääneriikides. See teeb piiriüleste tehingute seire ja terrorismi rahastamise avastamise keerulisemaks ning nõuab turuosalistelt enam tähelepanelikkust ning teadmisi.

See on väljakutse kogu tõkestamissüsteemi seisukohalt. Üha tähtsam roll on seetõttu koostööl järelevalve- ja julgeolekuasutustega. Terrorismi rahastamise puhul on ka paratamatu, et see **toimub väikestes summades** ning juhtumeid on (tehingute arvu arvestades) vähe, **mistõttu võivad hälbed suurandmete analüüsi käigus jääda nähtamatuks**.

## 5. Riiklikud terrorismi rahastamise ohud

**Terrorismi rahastamise ohu tase Eestis on keskmine** (vt lisaks tabel 1).

Riiklik terrorismi rahastamise oht jaguneb neljaks: **1) sisemine oht**, **2) Eestist lähtuv oht** teistele riikidele, **3) väline oht** ja **4) transiidist tulenev oht**. Edaspidi kasutatakse ka eelnevaid kategooriaid hõlmavaid katusmõisteid „riigisisene oht“ ja „piiriülene oht“<sup>19</sup>:

- **Sisemise ohu tase – madal**
- **Eestist lähtuva ohu tase – keskmine**
- **Välise ohu tase – keskmine**
- **Transiidist tuleneva ohu tase – keskmisest kõrgem**

Ohutaseme hinnang (vt ka tabel 1) põhineb asjaolul, et Eestis on madal sisemine ja väga madal (aga kasvav) transiidist tulenev terrorismi rahastamise ohu tase ning keskmine Eestist lähtuv ja väline terrorismi rahastamise ohu tase. Eesti tugevale finantssektorile lisanduvad terrorismi rahastamise ohud, mis tulenevad finantsteenustest ja abi osutamisest kõrgema terrorismi rahastamise riskiga riikidesse<sup>20</sup>. Eesti riigisisene ja piiriülene terrorismi rahastamise oht kasvas seoses Venemaa sõjalise agressiooniga Ukraina suunal ning sellega kaasnenud NATO ja Lääneriikide suunalise vaenutegevusega. Venemaa naaberriigina seisab Eesti silmitsi strateegiliste kaupade/relvade kaubandusega seotud piirüleste ohtudega. Eestis kogutud rahaliste vahendite kasutamise ohu tase riigi sees terroristlikel eesmärkidel on madal. Siiski muudavad Eesti geograafiline asukoht, avatud majanduskeskkond ja pakutavad finantsteenused – eriti korrespondentsuhete kaudu – riigi haavatavaks terroristlikul eesmärgil vahendite edastamisega seotud ohtude ees ning vähemal määral ka vahendite kogumise ees.

Peamised ohud on seotud **vahendite edastamise** faasiga, mis võib leida aset Eesti jurisdiktsioonis tegutsevate turuosaliste vahendusel **korrespondentsuhete** kaudu.

<sup>19</sup> Riigisisese ohu moodustavad sisemine oht, Eestist lähtuv oht ja väline oht. Piiriülese ohu moodustavad Eestist lähtuv oht, väline oht ja transiidist tulenev oht. Nii riigisisese kui ka piiriülese ohu tase on keskmine. Mõlemad omakorda panustavad riikliku ohu tasemesse.

<sup>20</sup> Kõrgema terrorismi rahastamise riskiga riikide nimekiri on avaldatud Rahapesu Andmebüroo kahtlaste tehingute tunnuste juhendi lisana: <https://www.fiu.ee/oigusaktid-ja-juhendid/juhendid#korgema-terrorismi-r>. Kõrgema terrorismi rahastamise riskiga riikide määramisel on võetud arvesse rahvusvaheliste organisatsioonide (EL, FATF jne) hinnanguid ja raporteid kooskõlas Eesti ametiasutuste ohuhinnangutega, samuti Eesti teenusepakujate seniseid seoseid eri riikidega. Kõrgem terrorismi rahastamise riskitase ei tähenda, et konkreetne riik rahastab terrorismi, vaid see viitab riskile, mis võib asjaolude kokkulangemisel realiseeruda. Kõrgema terrorismi rahastamise riskiga riikide nimekiri vaadatakse läbi kord aastas ning seda uuendatakse vastavalt vajadusele.

**Terrorismi rahastamise ohu tasemed katuskriteeriumide kaupa:**

- **Tulenevalt terrorirünnakutest ja terroristlikust tegevusest jurisdiktsioonis.**  
**Riigisisene – madal, piiriülene – keskmine.**  
Trend: kasvav.
- **Tulenevalt terroristlikutest organisatsioonidest ja isikutest jurisdiktsioonis.**  
**Riigisisene – väga madal, piiriülene – väga madal.**  
Trend: püsiv.
- **Seonduvalt isikutega, kel on poolehoid terroristlike organisatsioonide, isikute ja ideoloogiate suhtes.**  
**Riigisisene – väga madal, piiriülene – väga madal.**  
Trend: kasvav.
- **Tulenevalt aktiivsest terrorismiohust naaberjurisdiktsioonides.**  
**Väline oht – keskmine, Eestist lähtuv oht – madal.**  
Trend: kasvav.
- **Tulenevalt finantskeskustest. Piiriülene oht (transiit): väga madal.**  
Trend püsiv.
- **Strateegiliste kaupade ja teenustega seonduvalt. Piiriülene oht (transiit): keskmine.**  
Trend: püsiv.

## 5.1. Sisemine oht

Sisemise ohu all on peetud silmas Eesti oludest tulenevaid riigisiseseid ohte. Sisemise ohu korral toimuvad kõik terrorismi rahastamise faasid Eestis (kogumine, edastamine, kasutamine).

Eesti sisemine terrorismi rahastamise ohu tase on **väike**.

Eestis ei tegutse ühtki islamistlikku, paremäärmuslikku ega vasakäärmuslikku terroristlikku organisatsiooni ega nende rakukest. Samuti ei ela siin terroristlike organisatsioonidega seotud võitlejaid. Peamine oht on radikaliseerunud üksikisikud, kes aga üldjuhul rahastavad end ise. Ka äärmuslikult meelestatud isikute hulk Eestis on väike. Siiski on vaadeldaval perioodil olnud üks juhtum alaealistega, kes levitasid vägivaldse paremäärmusluse ideoloogiat.

Vägivaldse ideoloogia toetamisest tulenevalt on sisemise ohu tase riigis madal. Moslemikogukond on suhteliselt väikesearvuline ja rahumeelne. Mõnevõrra suurem on paremäärmuslust toetavate isikute ning Venemaa Föderatsiooni sümpaatiaga suhtuvate isikute hulk. Vaadeldaval perioodil terrorismi rahastamise juhtumeid ei esinenud. Eeltoodust tulenevalt on ka islamistliku terrorismi eesmärgil kogutud finantsvahendite kasutamise oht Eestis väike. Vägivaldse paremäärmusluse rahastamise ohu tase on madal. Senised tuvastatud ja menetletud juhtumid on olnud seotud üksiktegutsejatega, kes rahastasid end omavahenditest.

Tulevikku silmas pidades ei saa mööda vaadata demograafilisest ohust: riskiriikide<sup>21</sup> seosega islamikogukonna kasvust Eestis. 2019. aastal elas Eestis u 4300, 2024. aastal aga juba u 10 000 riskiriikidest pärit isikut.

<sup>21</sup> Kõrgema terrorismi rahastamise riskiga riikide nimekiri on avaldatud Rahapesu Andmehüübebüroo kahtlaste tehingute tunnuste juhendi lisana: <https://www.fiu.ee/oigusaktid-ja-juhendid/juhendid#korgema-terrorismi-r>. Kõrgema terrorismi rahastamise riskiga riikide määramisel on võetud arvesse rahvusvaheliste organisatsioonide (EL, FATF jne) hinnanguid ja raporteid kooskõlas Eesti ametiasutuste ohuhinnangutega, samuti Eesti teenusepakujate seniseid seoseid eri riikidega. Kõrgem terrorismi rahastamise riskitase ei tähenda, et konkreetne riik rahastab terrorismi, vaid see viitab riskile, mis võib asjaolude kokkulangemisel realiseeruda. Kõrgema terrorismi rahastamise riskiga riikide nimekiri vaadatakse läbi kord aastas ning seda uuendatakse vastavalt vajadusele.

Suuremate kogukondade teke kipub kaasa tooma kogukondliku eraldumise – mida suurem on kogukond, seda rohkem on võimalik elada igapäevaelu oma keele- ja kultuuriruumist väljumata. Julgeoleku aspektist on oluline, et riigis ei tekiks paralleelühiskondi, kes võivad – sh välisriikide – karismaatiliste isikute mõjul soovida luua kogukonnasiseseid reegleid, mida võidakse pidada ülimuslikuks Eesti seaduste ja ühiskonnainormide suhtes. **Kogukondade kapseldumine ja eraldumine on kasvulavaks radikaliseerumisele**, tõstes nõnda nii terrorismi kui ka terrorismi rahastamise ohu taset. Rändesurve riskiriikidest Eestisse püsib. Lisandub ettevõtjatepoolne surve odava tööjõu sissetoomiseks ja selleks sisserändekvootide leevendamiseks. Välismaalasest tippspetsialistide sisserände puhul ei ole kehtestatud piirarvu, küll aga kehtib nende puhul tööandjatele 1,5-kordse Eesti keskmise töötasu maksmise nõue.

Kogukonnaliikmete integreerimine Eesti kultuuri- ja seadusruumi on oluline nii islamiäärmusliku kui ka Venemaalt lähtuva terrorismi rahastamise ohu vaates.

**Demograafiast** lähtub oht ka vägivaldse paremäärmusluse vaatest – suurenev immigratsioon kasvatab reeglina paremäärmuslike vaadetega isikute hulka. **Hetkel on demograafilisest olukorrast tuleneva ohu tase madal, kuid see on kasvutrendis.**

#### **NÄIDISJUHTUM 1. Vägivaldse paremäärmusliikumisega Feuerkrieg Division (FKD) seotud noored**

Veebikeskkonnas radikaliseerunud noored tegelesid valge rassi ülemvõimu propageerimisega Eestis ja mujal maailmas. Interneti suhtlusplatvormide ja plakatite kaudu õhutati viha immigrantide, juutide, tumedanahaliste, seksuaalvähemuste, ajakirjanike ja politseinike vastu. Lisaks levitati kiirendusgrupi ideoloogiast lähtudes vaenu riigivõimu vastu tervikuna. Kriminaalasjas terrorismi rahastamist ei tuvastatud; noored olid oma vanemate ülalpidamisel, viimased aga ei olnud laste tegemistest teadlikud.

## 5.2. Eestist lähtuv oht

Eestist lähtuva ohu all on peetud silmas Eesti jurisdiktsioonist lähtuvat ohtu teistele riikidele.

Eestist lähtuv terrorismi rahastamise ohu tase on **keskmise**.

Oluline ohuallikas on **Venemaaga seotud terroristlike organisatsioonide toetamine**. Arvestades Eesti suhteliselt arvukat VF-i inforuumis-mõjusfääris elavat kogukonda, on tõenäoline, et Vene Imperiaalse Liikumise (VIL) või Vene imperialismi idee toetajate hulk võib olla suhteliselt suur. Samas ei ole tuvastatud isikuid, kes sooviksid reaalselt VIL-i rahastada. VIL on teinud küll venekeelses sotsiaalmeedias rahakogumiskampaaniaid, aga Eestis ei ole tuvastatud sinna vahendite saatmist. Vene eriteenistuste puhul ei saa välistada vahendite hankimiseks keerulisemaid finantsskeeme, aga seni neid tuvastatud ei ole.

Islamiterrorismi osas on ohuks heategevuse sildi all toimuvad terroriorganisatsioonide rahakogumiskampaaniad, mis võivad läbi interneti jõuda ka Eesti elanikeni. See tähendab terroriorganisatsioonide rahastamist Eesti elanike poolt ühisrahastuse (ing k *crowdfunding*) või teiste rahastuste kaasamise (ing k *fundraising*) kaudu nii tahtlikult kui ka kogemata, teadmatusest või hooletusest. Peamine oht seisneb selles, et raha saadetakse **heategevuse eesmärgil (konflikti)piirkondadesse**, kus puudub selge ülevaade ja kontroll nii lõppkasutajast kui ka kogutud vahendite tegelikust kasutusviisist, ehk siis piirkondadesse, mis on suuremal või vähemal määral terroristlike organisatsioonide kontrolli all.

Välisriikide kogemust arvestades on tõenäoline, et Eestis kogutud vahendid võivad muutuda ühisrahastusplatvormide<sup>22</sup> kaudu kättesaadavaks välismaistele terroristlikele organisatsioonidele. Vaadeldava perioodi lõpul tõstis vahendite kogumisega seonduva ohu taset peamiselt 2023. aasta oktoobris alanud HAMAS-i<sup>23</sup>-Iisraeli sõda ja sellega kaasnenud rahvusvahelised heategevuslikud rahakogumiskampaaniad ja ühisrahastusplatvormide kasutamine. Sellistes kampaaniates osales ka Eesti elanikke – Eesti jurisdiktsioonist **koguti ja edastati** vaadeldava perioodi lõpus **vahendeid heategevuslikus korras Gaza sektori** tsiviilisikute toetuseks. Kuivõrd tol perioodil haldas territooriumi terroristlik organisatsioon (väljapressimine, röövimine, altkäemaksud), ei ole vahendite jõudmist heatahtlikelt toetajatelt terroristliku organisatsiooni käsutusse võimalik lõpuni välistada.

Oluline oht on seotud ISIS-K<sup>24</sup> aktiveerumisega Kesk-Aasias, eelkõige Tadžikistanis, Kõrgõzstanis ja Türkmenistanis, mis on toonud kaasa liikmete värbamise kohaliku elanikkonna seas. Eestist lähtuvat ohtu kujutab see seonduvalt Kesk-Aasia päritolu töölistega, **kellele on iseloomulik vahendite saatmine kodumaale piiriüleste makseteenuste ja finantseerimisasutuste kaudu**. Kuna **Tadžikistani, Kõrgõzstani ja Türkmenistaniga** puudub õiguslane koostöö, on Eestist sinna saadetud vahendite saaja tuvastamine problemaatiline ning ei saa välistada rahaliste vahendite jõudmist hoopiski terroriorganisatsioonide või nendega seotud isikute toetuseks.

Samal ajal kasvas mainitud piirkonnast rändesurve nii Eestisse kui ka Euroopa Liitu tervikuna. Venemaa agressioonisõjast Ukraina vastu põhjustatud Venemaa, Ukraina ja Valgevene kodanike tööturult lahkumise kompenseerisid mitmed Eesti ettevõtjad Kesk-Aasia riikide kodanike lühiajalisele tööle värbamisega. Nende arv kasvas aastatel 2022–2023 märkimisväärselt<sup>25</sup>.

Terrorismi rahastamise ohu maandamiseks lisati kõik kolm eelnimetatud riiki kõrgema terrorismi rahastamise riskiga riikide nimekirja. Lühiajaliste töölubadega Kesk-Aasiast tööle saabumise ja nende Eestis viibimise seaduslikkuse üle suurendati kontrolli, mille tulemusel vähenes sealset päritolu tööjõu hulk Eestis 2024. aastal märkimisväärselt<sup>26</sup>.

Kindlasti tuleb ära märkida ohud, mis on seotud Eesti **avatud majandus- ja ettevõtluskeskkonna ning e-residentsuse programmi ära kasutamise**ga terroristide poolt nii Eestisse kui ka EL-i sisse imbumiseks seadusliku ettevõtluse arendamise katte all. E-residentidele on juriidilise isiku loomine lihtne. **E-residentsuse programmi ära kasutamise ohu tase terrorismi rahastamise eesmärgil on keskmine, kuna vaadeldaval perioodil tuvastati mitmeid terrorismi seostega isikuid, kellele oli väljastatud e-residentsus. Kõik sellised load tühistati.**

<sup>22</sup> Nt GoFundMe, [www.gofundme.com](http://www.gofundme.com).

<sup>23</sup> HAMAS – Ḥarakat al-Muqāwamah al-Islāmiyyah (Islami Vastupanuliikumine) – on sunni islamistlik poliitiline organisatsioon, millel on sõjaline tiib (Qassami Brigaadid). Organisatsioon on valitsenud Gaza sektorit alates 2007. aastast. Euroopa Liit, USA, Iisrael, UK, Jaapan, Uus-Meremaa ja Kanada on tunnistanud HAMASi terroristlikuks organisatsiooniks.

<sup>24</sup> ISIS-K – Islamic State Khorasan Province; tuntud ka kui ISKP. Daesh/ISIS Kesk-Aasia haru.

<sup>25</sup> 2022. aasta oktoobri seisuga oli lühiajalise töötamise luba antud 4147-le Kesk-Aasia riikide kodanikule, mis moodustas toona riskiriikide päritolu lühiajaliselt tööle registreeritustest u 75%.

<sup>26</sup> 2024. aasta novembri seisuga oli Eestis 1051 lühiajalise tööloaga Kesk-Aasia päritolu isikut.

### NÄIDISJUHTUM 2. Gazasse vahendite saatmise katsed (erinevad juhtumid)

2023. aastal soovisid erinevad isikud seonduvalt HAMAS-i-lisraeli sõjaga saata Eesti jurisdiktsiooni kaudu humanitaarkaalutlustel raha nii eraisikutele kui ka organisatsioonidele Gaza sektorisse. Enamik toetajatest olid välisriikide kodanikud, kuid oli ka e-residente ja Eesti kodanikke. Organisatsioonide seas tuvastati HAMAS-i seostega Gaza Now propagandakanalid.

Eelseisvad tehingud, mida krediidasutused märkasid, peatati. Toimunud tehingute ja osaliste väljaselgitamisel tehti õiguslast koostööd nii Eesti piires Kaitsepolitsei ameti ja Rahapesu Andmebürooga kui ka välisriiklike koostööpartneritega. Seotud isikute e-residendi staatused tunnistati kehtetuks.

### NÄIDISJUHTUM 3. E-residentide seas tuvastatud äärmuslusseostega isikud

2021. aastal tuvastati juhtum, kus kaks isikut löid e-residentidena Eestis ettevõtte, mis pakkus voogedastusteenust. Teenuse sisu oli muusika pakkumine enda loodud voogedastusplatvormil, mille ideoloogiline sõnum ühtis vägivaldse paremäärmuslusega. Isikud olid seotud organisatsiooniga Nordic Resistance Movement (NRM). Euroopa Liidu tasandil NRM terroristlike organisatsioonide seas pole, küll aga on kuulutanud selle terroristlikuks Ameerika Ühendriigid (USA), samuti on selle tegevuse keelustanud Soome. Organisatsioon tegutseb peamiselt Rootsis, aga ka Norras ja Taanis. Isikute e-residendi staatus tühistati.

### NÄIDISJUHTUM 4. ISIS-K seotuse kahtlusega lühiajalised töötajad

2022. aastal saabusid Kesk-Aasiast Eestisse lühiajalisele tööle isikud, kelle puhul tuvastati seotus ISIS-K-ga. Mainitud isikute töötamisega kaasnes paratamatult ka finantskomponent, st töötasu maksmine ning selle edasine kasutamine. Kesk-Aasiast pärit võõrtöölised saadavad reeglina osa palgast kodumaale. Kõnealuses juhtumis terrorismi rahastamist ei tuvastatud. Nüüdseks on kõik selle juhtumiga seotud võõrtöölised Eestist lahkunud.

## 5.3. Väline oht

Välise ohu all on mõeldud mujalt jurisdiktsioonidest lähtuvat ohtu. See tähendab olukorda, kus välisriigid või Eestist väljaspool asuvad isikud püüavad rahastada terroristlikku tegevust Eestis.

Väline terrorismi rahastamise ohu tase on **keskmine**.

Välismaalt Eestisse islamistlike terroriorganisatsioonide rajamiseks või siin islamismist ajendatud terroriaktide korraldamiseks raha saatmise ohu tase on madal.

Suurim ohuallikas on Venemaa, kes Euroopa- ja NATO-vaenuliku agressorriigina otsib aktiivselt oma eriteenistuste kaudu Lääneriikides, sh ka Eestis, oma huvides terroriakte toime panna soovivaid isikuid ning lubab neid ka rahastada. Venemaa on Euroopa- ja NATO-vaenuliku agressorriigina püsiv ohuallikas.

Mis puudutab naaberriikidest lähtuvat terrorismi rahastamise ohu taset, siis terrorismiohu tase Balti riikides on madal, mis omakorda mõjutab rahastamist. Skandinaavia riikides ja Venemaal on arvukas moslemikogukond, kelle seas on radikaalset islamiusku levitavaid isikuid ning üsna arvukalt tagasipöördunud välisvõitlejaid. Samuti leidub Skandinaavias küllaltki arvukalt paremäärmuslasi (Eesti konteksti kohta vt näidisjuhtum 3).

Nagu eelpool öeldud, ei ole Eestis terroristlike organisatsioone, samuti on radikaalseid ideoloogiad toetavate inimeste hulk väike. See tähendab, et siia terrorismi rahastamiseks vahendeid saata ei ole mõtet ja Eesti elanikkonda otseselt ei sihitata, küll aga on suurema mõjuga internetis tehtav propaganda ja mõjutustegevus, seda eelkõige üksikisikute puhul.

## 5.4. Transiidist tulenev oht

Transiidist tuleneva ohu all peetakse silmas olukorda, kus välismaalased väljaspool Eestit kasutavad terroristlike organisatsioonide või isikute toetamiseks Eesti jurisdiktsioonis pakutavaid tooteid ja teenuseid. Samuti võib see tähendada vahendite liigutamist Eesti kaudu füüsilisel moel.

Transiidist tulenev terrorismi rahastamise ohu tase on **keskmisest kõrgem**.

Peamine oht on seotud **korrespondentsuhetega** ning puudutab Eesti teenusepakkujate kaudu vahendite edastamist. Tehinguid tehakse Eesti teenusepakkujate (krediitiasutus või virtuaalvääringu teenuse pakkuja) juriidilisest isikust kliendi kaudu. Respondentasutuse füüsilisest isikust klient, kes vahendeid edastab, resideerub samuti mujal. Näiteks avati 2022. aastal VIBAN-konto isikule, kes oli mujal jurisdiktsioonis terrorismi rahastamises süüdi mõistetud ning viibis vangis (vt ka näidisjuhtum 6). Virtuaalvääringu teenuse pakkuja puhul on oht, et terrorismiseosega isik teeb tehinguid Eesti tegevusloaga VASP-i kliendi võimaldatud pesastusteenust (ing *nested service*) kasutades (vt näidisjuhtum 5). VASP-i respondentasutus ei pruugi kohaldada hoolsusmeetmeid vajalikul määral (ka paiknemine *offshore*-piirkonnas) ning võib pakkuda maksevõimalusi ka privaatmüntides.

**Eestist läbi reisivate terrorismiseostega isikute arv kasvab.** Lähiriikides (Venemaa Föderatsioon, Soome, Rootsi) asuvad suhteliselt suured Balkanimaade, Põhja-Kaukaasia, aga ka Somaalia, Iraagi ja Süüria päritolu islamikogukonnad, kelle seas on arvukalt terrorismiseostega isikuid, kes reisivad Eesti kaudu uue ja vana kodumaa vahet. Venemaa Föderatsiooni sõda Ukraina vastu ja hübriidründed Soome, Läti, Leedu ja Poola piiridel ning järgnenud piiride sulgemised tõid kaasa transiidi suurenemise läbi Eesti. Kui aastatel 2020–2022 läbis Eestit aastas u 50 isikut, kellel on tuvastatud seosed terrorismiga, siis 2024. aastal oli see arv u 200 inimest aastas. Kasv on eelkõige seotud inimeste reisimisega läbi Eesti Venemaale ja tagasi. Transiidis olevate terrorismiseostega isikute puhul on tuvastatud järgnevad asjaolud, mis võivad omada puutumust võimaliku terrorismi rahastamisega: suurem kogus sularaha eri valuutades (tegemist on Schengeni sisepiiridel, kus deklareerimiskohustus puudub, aset leidnud juhtumitega), erinevad deebetkaardid, sh VASP-ide omad, pakendis olevad nutiseadmed.

Ohutaset tõstvaks teguriks on asjaolu, et Schengeni ruumis liikudes üldjuhul puudub sularaha deklareerimiskohustus. Kuid mõnes liikmesriigis kehtivad ühendusesiseste sularahaliikumiste suhtes eraldi kontrolli- ja deklareerimisalased sätted, mida kohaldatakse lisaks Euroopa Liidu eeskirjadele. Ekspordi suunal on riskitase madalam, kuna Eesti-Vene piiril kehtib 100% piiri- ja tollikontroll. Terrorismi rahastamise juhtumeid [KarS § 237 (3)] hinnataval perioodil ei esinenud, küll aga viidi läbi teabehanke eesmärgil finantsuurimisi terrorismi võimaliku rahastamise tuvastamiseks.

## 6. Haavatavused

### 6.1. Riiklikud terrorismi rahastamise haavatavused

Riiklike haavatavuste hinnang põhineb järgmiste tegurite analüüsil: 1) riigi võimekus terrorismi rahastamise ohte tõkestada, 2) sektorite haavatavused ning kontrollimeetmete olemasolu, tõhusus ja turuosaliste teadlikkus. Riiklike haavatavusi vaadeldakse kategooriate kaupa: sisemine, Eestist lähtuv, väline, transiidist tulenev. Riikliku haavatavuse hinnangusse panustab ühelt poolt riigi võimekus konkreetset ohtu tõkestada ja teiselt poolt üldine sektorite<sup>27</sup> haavatavus.

#### Riiklike haavatavuste tasemed kategooriate kaupa:

- **Riikliku haavatavuse tase sisemise terrorismi rahastamise ees – keskmisest madalam**
  - o üldine sektorite haavatavuse tase – keskmisest madalam
  - o riigi võimekuse tase sisemist terrorismi rahastamist tõkestada – keskmisest kõrgem
- **Riikliku haavatavuse tase Eestist lähtuva terrorismi rahastamise ees – keskmisest madalam**
  - o üldine sektorite haavatavuse tase – keskmisest madalam
  - o riigi võimekuse tase Eestist lähtuvat terrorismi rahastamist tõkestada – keskmisest kõrgem
- **Riikliku haavatavuse tase välise terrorismi rahastamise ees – keskmisest madalam**
  - o üldine sektorite haavatavuse tase – keskmisest madalam
  - o riigi võimekuse tase välist terrorismi rahastamist tõkestada – keskmisest kõrgem
- **Riikliku haavatavuse tase transiidist tuleneva terrorismi rahastamise ees – keskmine**
  - o üldine sektorite haavatavuse tase – keskmisest madalam
  - o riigi võimekuse tase transiidist tulenevat terrorismi rahastamist tõkestada – keskmine

#### Kriteeriumid, mida hinnati, olid järgmised:

- terrorismi rahastamise tõkestamise poliitika ja strateegia kvaliteet,
- terrorismi rahastamise kuriteo määratluse tõhusus,
- tolli- ja piirikontrollide tõhusus terrorismi rahastamise tõkestamisel,
- terrorismi rahastamist puudutava teabe kogumise ja töötlemise kvaliteet,
- terrorismi rahastamise uurimise kvaliteet,
- terrorismi rahastamise eest süüdistuse esitamise kvaliteet,
- terrorismi rahastamise eest kohtumõistmise kvaliteet,
- terrorismi rahastamisega seotud varade konfiskeerimise ja arestimise mehhanismide kvaliteet,
- terrorismi rahastamist puudutavate sihivahendite finantssanktsioonide kvaliteet seonduvalt terrorismiga ja terrorismi rahastamisega,
- strateegilise varustuse, kaupade ja teenuste kontroll seonduvalt konfliktipiirkondadega.

Neil kriteeriumidel olid omakorda alakriteeriumid.

<sup>27</sup> Üldine sektorite haavatavuse taseme hinnang (keskmisest madalam) võtab arvesse sektorite haavatavusi koostöötajate kontrollimeetmete olemasolu, tõhususe ja turuosaliste teadlikkusega (vt 6.2).

**Tabel 3. Riiklik terrorismi rahastamise tõkestamise võimekus**

Kategooria	Ohu tase	Haavatavuse tase	Tõkestamise võimekuse tase	Jääkriski tase
Sisemine	madal	keskmisest madalam	keskmisest kõrgem	keskmisest madalam
Eestist lähtuv	keskmine	keskmisest madalam	keskmisest kõrgem	keskmine
Väline	keskmine	keskmisest madalam	keskmisest kõrgem	keskmine
Transiidist tulenev	keskmisest kõrgem	keskmine	keskmine	keskmisest kõrgem

## Suurimad haavatavused

Terrorismi rahastamise tõkestamist korraldavad seadusandlus on Eestis hästi reguleeritud. Rahapesu ja terrorismi rahastamise tõkestamist reguleerib vastav seadus – rahapesu ja terrorismi rahastamise tõkestamise seadus (edaspidi „RahaPTS“). Karistusseadustik (edaspidi „KarS“) defineerib terrorikuritegusid pea kõigis selle võimalikes aspektides. KarS § 237<sup>3</sup> raames on karistus proportsionaalne ning piisava heidutusefektiga<sup>28</sup>.

Aastatel 2020–2024 ei alustatud Eestis ühtegi terrorismi rahastamise kriminaalasja (st KarS § 237<sup>3</sup> järgi kvalifitseeritavat kuritegu). Hinnataval perioodil on korduvalt kaalutud Rahapesu Andmehüübebüroo edastatud teadete põhjal kriminaalasja alustamise perspektiivi KarS § 237<sup>3</sup> kvalifikatsioonis (terrorikuriteo ja selle toimepanemisele suunatud tegevuse rahastamine ning toetamine). Kuna aga reeglina on tegemist olnud virtuaalväeringute teenuse pakkujate korrespondentsuhte osutamisega kolmandates riikides tegutsevate ettevõtete poolt konfliktipiirkonnas viibivatele isikutele, siis tõenäosus neid üle kuulata, kohtulikku menetlusse kaasata ning süüdi mõista on pea olematu. Kaaluti ka võimalust viia kriminaalmenetlusi läbi ühisuurimisena rahvusvahelise koostöö raames. Rahapesu Andmehüübebüroo ja Kaitsepolitsei ameti tihedas koostöös võeti kasutusele alternatiivne meede: lisaks info edastamisele rahvusvahelise koostöö raames piiras Rahapesu Andmehüübebüroo (viitega Euroopa Liidu Nõukogu 27. detsembri 2001. aasta määrusele nr 2580/2001, art 2 lg 1) terrorismi rahastamise kahtlusega vahendite kättesaadavust mainitud isikutele konfliktipiirkondades.

Täiendavat reguleerimist vajaks terroristliku propaganda säilitamise valdkond, mis pole reguleeritud EL-i terroristlikku veebisisu ja selle levitamist tõkestava TCO (ing k *terrorism content online*) määrusega. Terrorismi rahastamine on esimese astme kuritegu, mis võimaldab karistada piisava rangusega<sup>29</sup>. Kohtutel on võimalus ja kohustus vajaduse korral kuritegu ümber kvalifitseerida, seda vastavalt kriminaalmenetluse seadustikule (KrMS p 306) ja ka kohtupraktikale. Eestis on olemas finantskuritegudele spetsialiseerunud kohtunikud ja prokurörid, prokuratuuril on olemas finantsanalüüsi tugi. Terrorismiga seotud kriminaalasjade kohtueelse uurimise pädevus on Kaitsepolitsei ametil. Nii kohtute, prokuratuuri, menetlus- kui ka järelevalveasutuste sõltumatuse ja usaldusväarsuse tase on kõrge. Nii Kaitsepolitsei ametil kui ka prokuratuuril on terrorismiga seotud kriminaalasjade menetlemise kogemus olemas.

Riigi terrorismi rahastamise tõkestamise strateegia (Siseministeeriumi siseturvalisuse arengukava, STAK) on sõnastatud piisava detailsusega ja seda ajakohastatakse regulaarselt. Sellele lisanduvad ka terrorismi tõkestamise eest vastutavate ametite sisemised tegevus- ja teabehankeplaanid.

<sup>28</sup> Siiski on oluline välja tuua, et 2022. aasta Moneyvali raportis hinnati Eesti tehnilist vastavust FATF-i 5. soovitusel (terrorismi rahastamise kuritegu) LC-ks (parandamist vajavaks). Raportis märgitakse, et kuigi enamik terrorismi rahastamise tõkestamise rahvusvahelise konventsiooni lisas loetletud kuritegusid on Eestis kriminaliseeritud, ei peeta nende rahastamist terrorismi rahastamise kuriteoks. Puudujääk on endine.

<sup>29</sup> Terrorismi rahastamise eest võib määrata kuni kümme aastat vangistust (nagu ka Soomes ja Saksamaal).

Terrorismi rahastamise tõkestamise eest vastutavad asutused on eelkõige Rahapesu Andmebüroo, Finantsinspeksioon ja Kaitsepolitsei amet, kelle ülesanded on selgelt määratletud ja reguleeritud. Pädevate asutuste koostöö ja infovahetus riigi sees toimib väga hästi. Rahapesu Andmebüroo ressurss ja võimekus on vaadeldaval perioodil kasvanud, see väljendub nii töötajate arvus, vajalike analüüsitööriistade olemasolus kui ka väljaõppes. Mandaat teavet saada on hea. Rahvusvaheline koostöö ja infovahetus Lääneriikide partnerasutustega on väga hea, osaletakse erinevates rahvusvahelistes koostööprojektides ja EL-i töögruppides.

Õiguskaitseasutustel on juurdepääs nii riigi- kui ka sõltumatutele andmebaasidele ning tegelike kasusaajate infole. Infobaase puudutav infrastruktuur Eestis on väga hea. Ka avalikkusel on juurdepääs osale riigi andmebaasidest (äriregister, tegelike kasusaajate andmekogu, kinnistusraamat, kohtulahendite baas jne).

Maksu- ja Tolliameti (MTA) sularahaveo kontroll Schengeni välispiiril ning strateegiliste kaupade kontroll piiril on tõhus.

Eespool käsitletud valdkondades on riigi võimekuse tase terrorismi rahastamist tõkestada **keskmisest kõrgem**.

## Valdkonnad, kus riigi võimekus terrorismi rahastamise tõkestamisel vajab täiendamist

- **Rahvusvahelise terrorismivastase koostöö tõhusus – haavatavuse tase keskmisest kõrgem**  
Samu väärtusi jagavate riikide/liitlasriikide vaheline infovahetus on hea ja kiire. Probleemne on teabevahetus EL-i väliste kolmandate riikidega ja nendega, kellega puudub õiguslane koostöö (sh Venemaaga). Paraku on just nendes riikides suurim hulk terroriste ja terroriorganisatsioone.
- **Varade konfiskeerimine ja külmutamine – haavatavuse tase keskmisest madalam**  
Seadusandlik raamistik on olemas ja suuresti toimiv. Süsteemi puuduseks on, et konfiskeerida saab ainult süüdimõistva otsuse korral. Terrorismi rahastamise kuritegude puhul ei pruugi kahtlusalune/süüdlane olla üldse Eestis ja tema süüasja ei ole võimalik Eestis menetleda, st teda süüdi mõista. Halduskonfiskeerimiste kohtupraktika on alles kujunemas.
- **Rahvusvaheliste sanktsioonide kehtestamine – haavatavuse tase keskmisest madalam**  
Euroopa Liidu sanktsiooninimekirjadesse lisamine on lihtne, ÜRO liinis aga vetostamise ohu tõttu keeruline. Eesti rakendab ÜRO Julgeolekunõukogu resolutsioone viivitusega ning selleks on olemas asjakohane riigisisene õiguslik raamistik. Säilisid väiksemad puudujäägid varade külmutamise regulatsioonis, näiteks varade külmutamise piiratud juhud ja varade liigid. Samuti on piirangud varade kättesaadavaks tegemise keelul ning esineb väiksemaid puudusi seoses kohustatud isikutele suunatud juhendmaterjalide ajakohastamisega.

## Terrorismi rahastamise kriminaalasjade menetlemiseks vajalikud ressursid ja võimekused – haavatavuse tase keskmisest madalam

KarS-i ja kriminaalmenetluse vaates on olukord hea. Tagasilööke oli perioodi jooksul tõendite hankimise võimekuse osas – Euroopa Kohtu otsused piirasid sidevahendite andmete kogumist. Õiguskaitseasutuste tõendite kogumise võimekus halvenes ja tõendite hankimise võimalused vähenesid.

## 6.2. Sektorite haavatavused

Sektoritest vaadeldi kõiki kohustatud isikutena<sup>30</sup> käsitletavaid sektoreid, kellest põhjalikumalt analüüsiti valitud sektoreid. Valiku aluseks oli sektori teenuste maht ja käive, senised juhtumid ja riskitüpoloogiad. Üksikasjalikumaks hindamiseks valiti järgmised sektorid: virtuaalväeringu teenuse pakkujad (VASP-id), krediidi-asutused, makseasutused, sh piiriülesed makseteenused (rahasiirde teenuse pakkujad ja valuutavahetajad) ning e-raha asutused<sup>31</sup> (nii sise- kui ka välismaised) ning ühisrahastusteenuse pakkujad. Teistes sektorites ei tuvastatud olulisi terrorismise riske<sup>32</sup>. Eraldi kommentaar on lisatud äriühingute teenuse pakkujate ja e-residentsuse programmi kohta (vt punkt 6.2.5).

Peamine haavatavus on jätkuvalt see, et Eesti finantssüsteemi turuosalisi ja nende teenuskeskkondi võidakse ära kasutada **vahendite edastamisel**. Arvestatav oht kaasneb välismaiste lepingupartneritega tehtud tehingutega, näiteks Eesti tegevuslooga teenusepakkujate pakutava pesastatud teenusega (ing k *nested service* (VASP-i sektori puhul) ja **korrespondentsuhtega (krediidiasutuste sektori puhul)**, kus ühe konto kaudu võidakse teenindada sadu või tuhandeid kliendi kliente, kelle seirel tuginetakse olulises ulatuses respondentasutuse protsessidele ja süsteemidele) *offshore*-piirkondades registreeritud teenusepakkujatele. Jätkuvalt kätkevad endas riske need VASP-id, kes osutavad pesastusteenust kolmandates riikides, kus ei kohaldata vajalikul määral hoolsusmeetmeid ning pakutakse maksevõimalusi privaatumüntides (ing k *privacy coins*).

Sektorite haavatavuse taset mõjutavad **1) sektori loomupärane haavatavus** ja **2) terrorismi rahastamise tõkestamise kontrollide kvaliteet**, mis omakorda jagunevad alakriteeriumideks.

**Kriteeriumid, mida nende kahe hindamiseks vaadeldi, olid järgmised:**

- sektori sobivus/kasulikkus terrorismi rahastamisel,
- sektori maht ja käive,
- kliendibaasi profiil,
- väljaminevad rahvusvahelised tehingud,
- väljaminevad rahvusvahelised tehingud kõrgema riskiga jurisdiktsioonidesse,
- sissetulevad rahvusvahelised tehingud,
- sissetulevad rahvusvahelised tehingud kõrgema riskiga jurisdiktsioonidest,
- sularaha kasutamine,
- esindajate, teenusepakkujate ja vahendajate kasutamine,
- muud haavatavustegurid,
- terrorismi rahastamise tõkestamise poliitika ja strateegia kvaliteet,
- terrorismi rahastamise tõkestamise praktikate ja tegevuste kvaliteet.

Neil kriteeriumidel olid omakorda alakriteeriumid.

### 6.2.1. Virtuaalväeringu teenuse pakkujad

Sektori ohutase on keskmine, **haavatavuse tase keskmisest madalam**, jääkriski tase keskmine.

Peamised ohud puudutavad pesastatud teenuseid, kus Eesti virtuaalväeringute teenuse pakkujate sektorit on kasutatud terrorismi rahastamiseks (vt allpool näidisjuhtum 5). Enamik ohtudest tuleneb välismaal elavatest välisriikide kodanikest. Suurim oht puudutab transiiti, kuid võimalik on ka väline oht ja Eestist lähtuv oht.

<sup>30</sup> RahaPTS § 2. Vt <https://www.riigiteataja.ee/akt/113032019126?leiaKehtiv>.

<sup>31</sup> E-raha asutused on nt Paysera, Revolüt, Koronapay, OpenPayd, Papaya, Paysafe, Payward jne teenused.

<sup>32</sup> Vabäühenduste kohta (mittetulundusühingud ja sihtasutused) valmib eraldi analüüs.

## Suurimad haavatavused

- Võimaldab anonüümsust ja on muu hulgas seetõttu atraktiivne.
- Korrespondentsuhted.

Tehingud tehakse Eesti teenusepakkuja juriidilisest isikust kliendi ehk respondentasutuse kaudu, kes tegutseb mujal jurisdiktsioonis. Respondentasutuse klient ehk nn lõppklient – tavaliselt füüsiline isik, kes vahendeid saata soovib – resideerub samuti mujal. Eesti teenusepakkujate lõppklientide seas on tuvastatud terrorismiseostega isikuid, kes teevad tehinguid mujalt jurisdiktsioonidest.

- Sektori käive on väga suur.

Eesti tegevusloaga VASP-ide tehingute väärtuse maht erinevate meie jurisdiktsioonis osutatavate teenuste lõikes on suur, aastas üle 30 miljardi euro<sup>33</sup>. Eesti tegevusloaga VASP-id moodustavad siiski väikese osa globaalsest turust. Enamik tehingutest teostatakse globaalsete ettevõtete platvormidel.

- Võimalus kiiresti, anonüümselt ja rahvusvaheliselt tehinguid teha.

Võimalus kaugteel (sh süvavõltsingute oht) ja suhteliselt anonüümselt kliendisuhteid luua ja tehinguid teha; tehingute kiirus ja rahvusvahelisus, anonüümsust võimaldavad *token*'id ja teenused, sh ülekannete varjamise võimalused (mikserid) teevad sektori terrorismi rahastamise vaatest väga sobivaks. Turul on palju erinevate omaduste ja kasutusalaadega vääringuid, mille kasutamise statistika üle arvepidamine ei ole praegu võimalik.

- Plokiahelasüsteemis toimuva jälgitavuse suutlikkus kehtib praktikas vaid enam levinud virtuaalväeringute puhul.

See eeldab, et Eesti tegevusloaga teenuseosutajad pakuvad töötajatele tööriista kasutamiseks vajalikku väljaõpet, täidavad seadusest tulenevaid hoolsusmeetmeid ning teavitavad terrorismi rahastamise kahtlusest seaduses ettenähtud korras.

- Terrorismi rahastamise riski ja kahtlusega teateid esitab väike osa teenusepakkujatest.

Virtuaalväeringute teenuse pakkujate teadete esitatud arv (terrorismi rahastamise riski ja kahtlusega teated) on küll kasvanud (vt tabel 4), aga teateid esitab endiselt vaid väike osa (alla kümne) kõigist teenusepakkujatest. See võib viidata sektori vähesele ja ebaühtlasele teadlikkusele terrorismi rahastamise võimalustest ning vähesele ja ebaühtlasele võimekusele selliseid tehinguid tuvastada, sh puudulikule hoolsusmeetmete kohaldamisele.

<sup>33</sup> Täpsem statistika VASP-ide sektori kohta on leitav NRA rahapesu raporti peatükis.

**Tabel 4. VASP-ide Rahapesu Andmebüroole esitatud terrorismi rahastamisele viitavad teated**

	2020	2021	2022	2023	2024
<b>TFR-134</b>	44	67	144	87	48
<b>TFR-235</b>	3	0	3	34	11
<b>Kokku</b>	<b>47</b>	<b>67</b>	<b>147</b>	<b>121</b>	<b>59</b>

Allikas: RAB

- Ettevõtted, millele on väljastatud Eestis tegevusluba, kuid mille reaalne äri käib väljaspool Eestit.  
Sellised ettevõtted ei tunne reeglina vajalikul määral Eesti õigussüsteemi, ei lähtu oma tegevuses siinsetest juhendmaterjalidest ega täida nõuetekohaselt hooldusmeetmeid, mis teeb nad haavatavaks.
- Nn hallil alal tegutsevad ettevõtted.  
Mõned virtuaalväringu ettevõtted on registreeritud Eestis, siin pakutakse ka teenust, kuid seda tehakse mõne teise jurisdiktsiooni VASP-i tegevusloaga, juhendades sealse riigi seadustest. Selline ettevõtetus ei kätke endas mitte ainult julgeolekuohtu, vaid probleemide ilmnemisel toob kaasa mainekahju Eestile, mitte tegevusloa väljastanud riigile.
- Paljudel ettevõtetel on maksekontod väljaspool Eestit.  
Sektori tegevuse läbipaistvust vähendab tõsiasi, et märkimisväärne osa maksekontodest asub Leedus, Ühendkuningriigis ning Maltal.

## Haavatavust maandavad tegurid

- Virtuaalväringu teenuse pakujate turgu on olulisel määral korrastatud ja riiklike regulatsioone põhjalikult täiendatud.  
Kui 31.12.2020 seisuga oli virtuaalväringu teenuse pakujate tegevuslubade arv 846 (millest aktiivseid 473), siis 31.12.2024 seisuga oli see arv 42. Lisaks suleti Eestis virtuaalvaluuta ostuks ja müügiks mõeldud sularahaautomaadid, mida perioodi alguses oli Eestis 10.
- Rahapesu Andmebüroo ja Kaitsepolitseiameti koostöös 2022. aastal uuendatud sektoripõhine juhendmaterjal.  
Kahtlaste tehingute tunnuste juhend, mis aitab turuosalistel terrorismi rahastamise riski ja kahtlusega tehinguid paremini ära tunda, toob välja vastavad indikaatorid ka virtuaalväringu teenuse pakujate vaatest.

<sup>34</sup> **TFR-1** – terrorismi rahastamise riskile viitav teade. Tuleb esitada, kui tehinguga on seotud riskiriigi seosega osaline (füüsiline isik, juriidiline isik või muu ühendus), esineb riskiindikaator ning lisandub ebaharilikuse aspekt. Tehingut või toimingut võib jätkata, kui kohaldatakse tugevdatud hooldusmeetmeid. Lisaajendina tuleb esitada kõik teadaolevad riskiindikaatorid. Vt <https://fiu.ee/terrorismi-rahastamisele-viitava-teate-esitamine-rahapesu-andmebuuroole>.

<sup>35</sup> **TFR-2** – terrorismi rahastamise kahtlusele viitav teade. Tuleb esitada, kui esineb kahtlusindikaator. TFR-2 teate esitamiseks piisab kahtlusindikaatorist, seos riskiriigiga ei mängi rolli. Seesugune tehing tuleb peatada kuni pädeva asutuse edasise juhiseni ning kohustatud isikul on keelatud kliendile mistahes rahalisi vahendeid kättesaadavaks teha. Lisaajendina tuleb esitada kõik teadaolevad riski- ja kahtlusindikaatorid. Vt <https://fiu.ee/terrorismi-rahastamisele-viitava-teate-esitamine-rahapesu-andmebuuroole>.

Lisaks tehti 2022. aastal juhendi lisana avalikkusele ja turuosalistele kättesaadavaks Eesti vaates kõrgema terrorismi rahastamise riskiga riikide nimekiri, mida uuendatakse kord aastas või vastavalt vajadusele.

- Turuosaliste oluliselt paranenud teadlikkus ja hoolsusmeetmete kohaldamise võimekus.

Sellesse on panustanud nii suurem reguleeritus, jõuline järelevalvetegevus kui ka koolitustegevus<sup>36</sup>. Probleemkohti esineb siiani – terrorismi rahastamisele viitavaid teateid esitab sektorist vaid väike osa ning probleeme on ka teadete kvaliteediga<sup>37</sup>. Siiski nähtub sektori esitatud teadetest, et aktiivsed teenusepakkujad suudavad terrorismi rahastamise kahtlust ja kahtlustäratavaid isikuid ära tunda, kasutades oskuslikult vastavaid tööriistu ja meetodeid, sh avalikke allikaid.

### NÄIDISJUHTUM 5. Terroristliku organisatsiooniga Palestiina Islamidžihaad seotud võrgustiku katse liigutada virtuaalvääringsid Eesti teenusepakkuja kaudu

2023. aastal soovisid isikud, kes olid varem teinud mujal platvormidel tehinguid terroristliku organisatsiooniga Palestiina Islamidžihaad, deponeerida vahendeid Eesti virtuaalvääringu teenuse pakkuja juures. Tegu oli 18-liikmelise võrgustikuga, mis tuvastati tänu teenusepakkuja kohaldatud hoolsusmeetmetele.

Eesti tegevuslooga virtuaalvääringu teenuse pakkujal oli korrespondentsuhte raames mujal jurisdiktsioonis paiknev juriidilisest isikust klient, kellel omakorda olid füüsilisest isikust kliendid (nn lõppkliendid), kes paiknesid samuti mujal jurisdiktsioonis. Füüsilised isikud olid mujal platvormidel saatnud vahendeid terroristliku organisatsiooni eri krüptoadressidele. Lisaks olid nad terroriorganisatsioonidelt aga ka vahendeid saanud, mida viitab otseselt organisatsiooni huvides tegutsemisele. Tehingusummad olid terrorismi rahastamise vaatest väga suured: sadades tuhandetes eurodes.

Seejärel proovisid võrgustiku liikmed teha tehinguid Eesti jurisdiktsiooni kaudu, deponeerides siin vahendeid väikestes summas. Võrgustiku Eesti jurisdiktsioonis asuvad vahendid külmutati kogusummas 8205 eurot (8963 USDT, krüptovaluuta Tether).

## 6.2.2. Krediidiasutused

Sektori ohutase on keskmisest madalam, **haavatavuse tase keskmisest madalam**, jääriski tase keskmisest madalam.

Europoli hinnangul<sup>38</sup> liigutatakse terrorismi rahastamiseks vahendeid endiselt tavapäraselt ka pankade kaudu. Seda aga vähem neis riikides, kus rakendatakse rangeid kontrollimehhanisme ja riskide profileerimist või kus on täiendatud rahapesuvastast seadust. Eesti pangandussektor vastab eelkirjeldatud tingimustele.

Peamine oht on krediidiasutuste kasutamine terrorismi rahastamise toetamise eesmärgil VIBAN-kontode ja korrespondentsuhete kaudu. Tegu on jällegi eelkõige transiidil põhineva ohuga.

<sup>36</sup> Rahapesu Andmebüroo korraldas vaadeldaval perioodil virtuaalvääringu teenuse pakkujate sektorile 13 koolitust, mis käsitlesid muu hulgas sektori hoolsusmeetmeid ja teatamiskohustust. Neist 4 koolitust käsitlesid spetsiifiliselt terrorismi rahastamise tõkestamist virtuaalvääringute vaatest. Lisaks oli sektor kaasatud kõigile sektoriülestele koolitustele.

<sup>37</sup> Kvaliteeti puudutav statistika on olemas perioodi 2022–2024 kohta ning hõlmab kõiki sektori esitatud teateliike. Probleemsete teadete protsent oli vastavalt 14%, 12% ja 11%.

<sup>38</sup> Europol: European Union Terrorism Situation and Trend Report 2023. Publications Office of the European Union, Luxembourg 2023, lk 21.

## Suurimad haavatavused

- Korrespondentsuhted.

Sektori suurim haavatavus on sarnane VASP-i sektoriga. Tehingud tehakse Eesti teenusepakkuja juriidilisest isikust kliendi ehk respondentasutuse kaudu, kes tegutseb mujal jurisdiktsioonis. Respondentasutuse klient ehk nn lõppklient – tavaliselt füüsiline isik, kes vahendeid saata soovib – resideerub samuti mujal. Eesti teenusepakkujate lõppklientide seas on tuvastatud terrorismiseostega isikuid, kes teevad tehinguid mujalt jurisdiktsioonidest.

- Teenuse pakkumine VIBAN-kontode kaudu.

Reeglina on see seotud piiriüleste makseteenuse osutajate ning virtuaalväringu teenuse pakkujatega. Hooldusmeetmete kohaldamine nähtub sellisel juhul rahuldaval määral, kuid teadete esitamine võib korrespondentsuhtest tulenevalt olla vahel liiga aeglane.

- Suur käive ja kliendibaas.

## Haavatavust maandavad tegurid

- Pankade arv, kellel on korrespondentsuhted VIBAN-teenuse osutamise näol, on väike<sup>39</sup>.

Üksikud krediidasutused pakuvad korrespondentsuhete raames teistele krediidi- ja finantsasutustele arvelduskontosid nende enda klientide teenindamiseks. Korrespondentpangandusega seotud riskid on Eestis kontsentreeritud vaid üksikute turuosaliste kätte.

- Hea teadlikkus terrorismi rahastamise ohtudest.

Hea teadlikkus nähtub nii teatamiskohustuse täitmisest, koostöövalmidusest kui ka töögruppides osalemisest. Mitteresidentidele lähenemine on konservatiivne. E-residente koheldakse mitteresidentidena. Eesti krediidasutuste klientidest ligi 5% moodustavad mitte-residendid, kõrgema riskitasemega riikide residentsusega klientide osakaal on vaadeldaval perioodi langenud<sup>40</sup>.

- Rahapesu ja terrorismi rahastamise tõkestamise valdkonda laiemalt investeeritakse hästi ning töötajaid koolitatakse regulaarselt.
- Sektoril on olemas aktiivselt toimiv katusorganisatsioon Eesti Pangaliidu näol ning terrorismi rahastamise tõkestamist puudutuvat infot vahetatakse ka pankade vahel eraldi töögrupis.

---

<sup>39</sup> Vt täpsemalt NRA rahapesu finantssektori haavatavuste peatükk.

<sup>40</sup> Vt täpsemalt NRA rahapesu finantssektori haavatavuste peatükk.

### NÄIDISJUHTUM 6. VIBAN-konto avamine terrorismi rahastamises süüdi mõistetud välisriigi kodanikule

Välisriigi kodanikule avati korrespondentsuhte raames Eesti finantssüsteemis 2022. aastal virtuaalne kontonumber ehk VIBAN-konto. Isik oli mõistetud mujal jurisdiktsioonis süüdi terrorismi rahastamises ning viibis seal vangis. Ta oli üritanud ühineda võitlejatega Tšetšeenias, saatnud vahendeid võitlejate toetuseks Süüriasse ning üritanud osta materjale lõhkeseadeldise valmistamiseks. Isiku taust tuvastati siiski enne, kui ta jõudis Eesti finantssüsteemi kaudu makseid teha.

### 6.2.3. Makseasutused, sh piiriüleised makseteenused (rahasiirde teenuse pakkujad, valuutavahetajad)

Sektori ohutase on keskmine, **haavatavuse tase keskmine**, jääkriski tase keskmine.

Peamine oht on Eesti makseasutuste kasutamine vahendite saatmiseks kõrgema terrorismi rahastamise riski tasemega riikidesse. Tegu on peamiselt Eestist lähtuva ohuga.

#### Suurimad haavatavused

- Sularahasaadetised välisriikide tegevuslooga piiriüleste makseteenuse pakkujate ja finantseerimisasutuste kaudu.

Sularaha kasutamine on endiselt laialdaselt levinud nn riskiriikides, kus pangandussektor on nõrk või enamikule elanikele kättesaamatu.

Teenus võimaldab sularahasiiret kõrgema terrorismi rahastamise riski tasemega riikidesse, kus tavapärased kanalid ei pruugi piisavalt hästi toimida või kui soovitakse neist teadlikult hoiduda. Selliste alternatiivsete maksekanalite kaudu teostatud tehingute kolmandates riikides asuvate osaliste tuvastamine on reeglina raskendatud. Raha lõppsaaja ei pruugi olla selgelt tuvastatav. Tehinguid võidakse teha ka läbipaistvamate kanalite vältimiseks. Rahasiirde teenus on mugav kanal terrorismi rahastamiseks, eelistatumad on globaalselt laia makseagentide võrgustikuga Western Union ja Moneygram. Koostöös nii Western Unioni teenusepakkuja kui ka kohapealse makseagendi Omniva kaudu on tuvastatud mitmeid terrorismi rahastamise kahtlusega tehinguid.

- Valuutavahetuse puhul ei pea alla 1000 EUR summade puhul isikut tuvastama.

Samas toimub terrorismi rahastamine enamjaolt just väikeste summadena. Turuosalistelt on teateid vähe ning reeglina koonduvad need vaid ühe teenusepakkuja teadeteks, mis võib viidata sektori kui terviku väiksele teadlikkusele terrorismi rahastamise ohtudest.

- Makseasutusi võidakse kasutada pikemas tehinguahelas, näiteks rahasiire koos virtuaalvääringute kasutamisega, mis omakorda raskendab terrorismi rahastamise tuvastamist.
- Teenusepakkujate riskiriikides tegutsevate vahendajate (makseagentide) meetmed terrorismi rahastamise tõkestamiseks on valdavalt kesised või suisa olematud. Tehingu teise, riskiriigis asuva poole tuvastamine on keeruline.

## Haavatavust maandavad tegurid

- Rahasiirde teenuse puhul on väljuvate ja sissetulevate maksete puhul Eestis asuv osapool reeglina hästi dokumenteeritud.
- Sisse- ja väljaminevate tehingute hulk ei ole suur.

E-raha asustuste oluline haavatavus on seotud välisriikide tegevuslooga piiriüleste e-raha teenuste pakkujate ning nende teenuste edasimüüjatega<sup>41</sup>. E-raha teenusepakkujate puhul on suurimaks väljakutseks piiratud infovahetuse võimalused piiriüleste e-raha asutustega ning tihti asukohariigi leebemad tunne-oma-klienti nõuded. Eesti krediidasutuste väikse riskiisu tõttu on Eestis resideeruvate kolmandatest riikidest pärit isikute järgmine valik e-raha teenusepakkujad.

### 6.2.4. Ühisrahastusteenuse pakkujad

Sektori ohutase on madal, **haavatavuse tase keskmisest madalam**, jääkriski tase keskmisest madalam.

Peamine oht on vähesest teadlikkusest tulenev Eesti ühisrahastusplatvormide kasutamine terrorismi rahastamiseks. Sektor võimaldab anonüümset vahendite kogumist ja saatmist piirkondadesse, kus vahendite lõppkasutuse üle puudub kontroll.

#### Suurimad haavatavused

- Ühisrahastus sobib suurepäraselt terroristlikul eesmärgil vahendite kogumiseks.
- Sektori vähene teadlikkust terrorismi rahastamise ohtudest.

Seda on märgata nii ühisrahastuse kui ka kogumist laiemalt võimaldavate<sup>42</sup> platvormide puhul. Reeglina kasutatakse globaalseid finantstulu mittepakkuvaid ühisrahastusplatvorme (nt GoFundMe, JustGiving, Fundly jne). Platvormidelt endilt terrorismi rahastamisele viitavaid teateid ei laeku. Sama kehtib ka kohalike ühisrahastusplatvormide ja investeerimisühingute kohta, mis viitab võimalusele, et teadlikkus võimalikest terrorismi rahastamise riskidest on väike ning puudub oskus neid ära tunda.

- Suur võimalus, et raha investeerija või annetaja usalduse kuritarvitamise kaudu kasutatakse kogutud vahendeid hoopis terroristlikel eesmärkidel. Välisriikide juhtumitest nähtub, et ühisrahastusplatvormide kaudu on kogutud vahendeid nii islamiäärmuslaste kui ka vägivaldsete paremäärmuslaste huvides.
- Annetajate ja raha saajate tuvastamise võimalused on piiratud.

## Haavatavust maandavad tegurid

- Isikute hulk Eestis, kes võiksid soovida terrorismi rahastamist toetada, on väike.

<sup>41</sup> E-raha asutuste loetelu ning teenuste edasimüüjad on leitavad Finantsinspektsiooni koduleheküljelt [www.fi.ee](http://www.fi.ee).

<sup>42</sup> Ühisrahastus (ing k *crowdfunding*) vs. vahendite kogumine laiemalt: muu rahastuse kaasamine (ing k *fundraising*).

## 6.2.5. Teised valdkonnad

### 6.2.5.1. Äriühingute teenuse pakkujad

Äriühingute teenuse pakkujaid ei ole analüüsitud detailselt, kuid sektor väärib töögrupi hinnangul eraldi märkimist kui väravahoidjad, kel on täita riskide maandamisel oluline roll.

Samuti tasub välja tuua, et äriühingute teenuse pakkujate teenused, mis hõlmavad ettevõtte asutamist, on loomulikult riskantsed nii rahapesu kui ka terrorismi rahastamise aspektist. Sageli on need teenused suunatud Eestis eelkõige välismaalastele ning suur osa sektorist loob ärisuhteid ja osutab teenuseid kliendiga füüsiliselt kohtumata, mis tõstab anonüümsusega seotud riskide tasemeid. Äriühingute teenuse pakkujaid võidakse ära kasutada eriti **e-residentsuse abil juriidilise isiku asutamiseks terrorismi rahastamise kaalutlustel** (vt ka näidisjuhtum 3). Sektori haavatavused võivad olla: turuosaliste väike teadlikkus; hoolsusmeetmete kohaldamise puudulik tase, puudused tegeliku kasusaaja ja vara päritolu tuvastamisel, puudused riskihinnangutes ja protseduurireeglites (vt ka kontrollimenetlustes tuvastatud puuduste kohta)<sup>43</sup>. Teatamiskohustuse puudulik täitmine – sektor on esitanud terrorismi rahastamisele viitavaid teateid vaid loetud korrad<sup>44</sup>. Puudub ka ametlik katusorganisatsioon, mis aitaks sektori tegevust koordineerida. Ehkki riigil on sektorist selge ülevaade (vt ka NRA rahapesu riskihinnang), on terrorismi rahastamise tõkestamisega seonduvalt vajakajäämisi. On tõenäoline, et see vajakajäämine mõjutab riiklikku riskipilti.

### 6.2.5.2. E-residentsuse programm

Äärmuslaste või terroristide võimalikuks motiiviks osaleda Eestis e-residentsuse kaudu ettevõtluses on soov viia majandustegevus oma elukohariigi julgeolekuasutuste järelevalve ja jurisdiktsiooni alt välja. Radikalseerunud isikute ja terroristide võimalik motiiv e-residentsuse taotlemisel ei ole niivõrd kasu saada digiriigi e-teenuste hüvedest legaalse ettevõtluse edendamisel, kuivõrd testida programmiga kaasnevaid hüvesid. Näiteks soovitakse testida uute finantseerimiskanalite võimalusi ning ootust lihtsustatud korras Euroopa Liitu siseneda või tekitada endale õiguslik alus Euroopa Liidus viibimiseks. Eeltoodud kinnitab olemasolev teadmine, et kui pärast e-residendi staatuse saamist varasemalt seatud ootused reeglina ei täitu, siis ka reaalse äritegevusega Eestis ei alustata.

E-residentsusega seonduvalt tuvastati vaatlusperioodil kokku vähemalt 26 islamistliku terrorismi või äärmuslusega seotud inimest. Tagantjärele tuvastamine jätkub seniajani. Terrorismi rahastamise vaatest olid aastatel 2020–2024 e-residentsusega seotud järgnevad probleemkohad.

- Probleemne on hankida kontrollitud teavet e-residentsuse taotleja kohta riikidest, millega Eestil puudub toimiv justiits-, korrakaitse- ja julgeolekualane koostöö. Tegemist on jätkuva probleemiga, mistõttu on kavas piirata e-residentsuse väljastamist selliste riikide kodanikele.
- Perioodi alguses (2020) esines kombinatsioon, kus kõrgema terrorismi rahastamise riski tasemega riikidest pärit e-residendid taotlesid VASP-i tegevusluba ning esines tõsiseid puudujääke tunne-oma-klienti (ehk KYC) põhimõtete täitmisel. Sellega kaasnesid terrorismi rahastamise riskid. Praeguseks on need riskid suures osas maandatud.

<sup>43</sup> Rahapesu riiklik riskihinnang.

<sup>44</sup> Vaatlusperioodil esitas sektor neli terrorismi rahastamisele viitavat teadet, kõik aastal 2024, kuid sisulises plaanis ei kvalifitseerunud neist ükski terrorismi rahastamisele viitavaks teateks.

- Perioodi alguses oli ülevaade ja järelkontroll e-residentide reaalse ettevõtlusega tegemise suhtes puudulik. 2024. aastaks oli olukord paranenud, kuna üldist järelkontrolli e-residentide ja nende ettevõtlusaktiivsuse üle on parandatud.
- Kõrgema terrorismi rahastamise riski tasemega riikidest pärit e-residentidel oli tekkinud arusaam, et e-residentsus võimaldab ka lihtsamal moel EL-i pääseda. Kaudset toetust sellele avaldasid Startup-komitee kinnituskirjad. Eestis äriühingu loomisega kaasneb kaudne alus Schengeni viisa saamiseks, mis usutava tausta loomisel võib viisa saamist lihtsustada. Seega esineb juhtumeid, kui e-residentsust taotlev isik üritab kas teadlikult või teadmatusel kasutada e-residentsust nende hüvede saamiseks, mida e-residentsus otseselt ei anna (nt elamisõigus või Eestisse või Euroopa Liitu sisenemise õigus).
- E-residentsuse taotlemine võimaldab kontrollida, kui võimekas on EL-i liikmesriik julgeolekut ohustavate inimeste tuvastamisel. Kui kellegi e-residentsuse taotlus saab keelduva vastuse viitega temast tulenevale ohule, saab inimene tagasiside, et tema taust on Eestile teada.

# Lisad

## Lisa 1. Peamised terrorismi rahastamise tüpoloogiad

- **Riskiriigi seosega radikaliseerunud** isik ja/või terrorismiseosega endine võitleja teeb mujal **Euroopa riigis elades virtuaalväeringus tehinguid Eesti jurisdiktsiooni vahendusel** läbi korrespondentsuhte.

See tähendab ühtlasi, et tehingut tegev isik ei pruugi olla Eesti osalusest teadlik ning võib olla valinud väljaspool EL-i asuva platvormipakkuja näiteks selle väiksemate hooldusmeetmete tõttu. Niisugusel juhul on tuvastatud isiku taust avalike allikate põhjal.

- **Tehingud väikestes summates**, toetuse tegeliku eesmärgi varjamine, sotsiaalabi või kogukonnaga seotud liikumise või **kodanikualgatuse liikumise** kogumiskampania sildi taha.
- **Ühisrahastuse** abil annetuste kogumine **konfliktipiirkonna toetuseks** – eriti HAMAS-i-Iisraeli sõja ajal Gaza sektori tsiviilelanike heaks.

Territooriumi kontrollib terroristlik organisatsioon ning heausketel annetajatel ei ole võimalik kontrollida, kes on vahendite lõppkasutaja. Peamine oht on see, et annetajate saadetud vahendid jõuavad tsiviilelanike asemel terroristlikule organisatsioonile (sh väljapressimine, röövimine).

- Vahendite edastamine **sularahakulleri** abil.

Schengeni alal puudub sularaha deklareerimise kohustus. Välispiiril välditakse deklareerimiskohustuse määra või üritatakse vedada raha peidetul kujul.

## Lisa 2. Näidisjuhtumid

### **NÄIDISJUHTUM 1. Vägivaldse paremäärmusliikumisega Feuerkrieg Division (FKD) seotud noored**

Veebikeskkonnas radikaliseerunud noored tegelesid valge rassi ülemvõimu propageerimisega Eestis ja mujal maailmas. Interneti suhtlusplatvormide ja plakatite kaudu õhutati viha immigrantide, juutide, tumedanahaliste, seksuaalvähemuste, ajakirjanike ja politseinike vastu. Lisaks levitati kiirendusgrupi ideoloogiast lähtudes vaenu riigivõimu vastu tervikuna. Kriminaalasjas terrorismi rahastamist ei tuvastatud; noored olid oma vanemate ülalpidamisel, viimased aga ei olnud laste tegemistest teadlikud.

### **NÄIDISJUHTUM 2. Gazasse vahendite saatmise katsed (erinevad juhtumid)**

2023. aastal soovisid erinevad isikud seonduvalt HAMAS-i-lisraeli sõjaga saata Eesti jurisdiktsiooni kaudu humanitaarkaaluksustel raha nii eraisikutele kui ka organisatsioonidele Gaza sektorisse. Enamik toetajatest olid välisriikide kodanikud, kuid oli ka e-residente ja Eesti kodanikke. Organisatsioonide seas tuvastati HAMAS-i seostega Gaza Now propagandakanalid.

Eelseisvad tehingud, mida krediidasutused märkasid, peatati. Toimunud tehingute ja osaliste väljaselgitamisel tehti õiguslast koostööd nii Eesti piires Kaitsepolitsei ameti ja Rahapesu Andmebürooga kui ka välisriikide koostööpartneritega. Seotud isikute e-residenti staatused tunnistati kehtetuks.

### **NÄIDISJUHTUM 3. E-residentide seas tuvastatud äärmuslusseostega isikud**

2021. aastal tuvastati juhtum, kus kaks isikut löid e-residentidena Eestis ettevõtte, mis pakkus voogedastusteenust. Teenuse sisu oli muusika pakkumine enda loodud voogedastusplatvormil, mille ideoloogiline sõnum ühtis vägivaldse paremäärmuslusega. Isikud olid seotud organisatsiooniga Nordic Resistance Movement (NRM). Euroopa Liidu tasandil NRM terroristlike organisatsioonide seas pole, küll aga on kuulutanud selle terroristlikuks Ameerika Ühendriigid, samuti on selle tegevuse keelustanud Soome. Organisatsioon tegutseb peamiselt Rootsis, aga ka Norras ja Taanis. Isikute e-residenti staatus tühistati.

### **NÄIDISJUHTUM 4. ISIS-K seotuse kahtlusega lühiajalised töötajad**

2022. aastal saabusid Kesk-Aasiast Eestisse lühiajalisele tööle isikud, kelle puhul tuvastati seotus ISIS-K-ga. Mainitud isikute töötamisega kaasnes paratamatult ka finantskomponent, st töötasu maksmine ning selle edasine kasutamine. Kesk-Aasiast pärit võõrtöölised saavad reeglina osa palgast kodumaale. Kõnealuses juhtumis terrorismi rahastamist ei tuvastatud. Nüüdseks on kõik selle juhtumiga seotud võõrtöölised Eestist lahkunud.

### **NÄIDISJUHTUM 5. Terroristliku organisatsiooniga Palestiina Islamidžihaad seotud võrgustiku katse liigutada virtuaalvääringsid Eesti teenusepakkuja kaudu**

2023. aastal soovisid isikud, kes olid varem teinud mujal platvormidel tehinguid terroristliku organisatsiooniga Palestiina Islamidžihaad, deponeerida vahendeid Eesti virtuaalvääringu teenuse pakkuja juures. Tegu oli 18-liikmelise võrgustikuga, mis tuvastati tänu teenusepakkuja kohaldatud hoolsusmeetmetele.

Eesti tegevusloaga virtuaalvääringu teenuse pakkujal oli korrespondentsuhte raames mujal jurisdiktsioonis paiknev juriidilisest isikust klient, kellel omakorda olid füüsilisest isikust kliendid (nn lõppkliendid), kes paiknesid samuti mujal jurisdiktsioonis. Füüsilised isikud olid mujal platvormidel saatnud vahendeid terroristliku organisatsiooni eri krüptoadressidele. Lisaks olid nad terroriorganisatsioonidelt aga ka vahendeid saanud, mida viitab otseselt organisatsiooni huvides tegutsemisele. Tehingusummad olid terrorismi rahastamise vaatest väga suured: sadades tuhandetes eurodes.

Seejärel proovisid võrgustiku liikmed teha tehinguid Eesti jurisdiktsiooni kaudu, deponeerides siin vahendeid väikestes summates. Võrgustiku Eesti jurisdiktsioonis asuvad vahendid külmutati kogusummas 8205 eurot (8963 USDT, krüptovaluuta Tether).

### **NÄIDISJUHTUM 6. VIBAN-konto avamine terrorismi rahastamises süüdi mõistetud välisriigi kodanikule**

Välisriigi kodanikule avati korrespondentsuhte raames Eesti finantssüsteemis 2022. aastal virtuaalne kontonumber ehk VIBAN-konto. Isik oli mõistetud mujal jurisdiktsioonis süüdi terrorismi rahastamises ning viibis seal vangis. Ta oli üritanud ühineda võitlejatega Tšetšeenias, saatnud vahendeid võitlejate toetuseks Süüriasse ning üritanud osta materjale lõhkeseadeldise valmistamiseks. Isiku taust tuvastati enne, kui ta jõudis Eesti finantssüsteemi kaudu makseid teha.

## Lisa 3. Nõuanded sektoritele

Pädevad asutused koostavad eraldiseisva tegevuskava, et käsitleda käesoleva riskihindamise aruande järeldusi. Allpool on siiski toodud mõned näited meetmetest, mida sektorid saavad riskide maandamiseks rakendada.

- **Korrespondentsuhete loomisel veenduda ka praktikas**, et klient kohaldab hoolsusmeetmeid (andmed on vajaduse korral kättesaadavad), mis sobituvad Eesti jurisdiktsiooni nõuetega. Samuti tuleb pöörata tähelepanu kliendi tegevusalale, et tuvastada, kas ta vajab teenuse pakkumiseks tegevusluba ning kas ja millises jurisdiktsioonis on see väljastatud. Terrorismi rahastamise vaatest tuleks olla erakordselt ettevaatlik välisriikide teenusepakkujatega, kes kasutavad EL-i turule sisenemiseks pesastusteenust Eesti ettevõtete kaudu, kes on registreeritud ja tegutsevad *offshore*-piirkonnas. On oluline, et Eesti teenusepakkuja hindaks enda respondentasutusest klientide terrorismi rahastamise tõkestamise organisatsioonilist lahendit ja selle tõhusust.
- Terrorismi rahastamisele viitavate tehingute tuvastamisel on abiks Rahapesu Andmebüroo uuendatud **juhendmaterjal** kahtlaste tehingute tunnuste kohta ning selle lisa – kõrgema terrorismi rahastamise riskiga riikide ehk nn **riskiriikide nimekirj**. Siiski ei ole juhendis toodud terrorismi rahastamise indikaatorid ammendav loetelu, vaid abistav materjal. Seetõttu on vajalik terrorismi rahastamise **trendide**<sup>45</sup> jälgimine.
- Finantssektori ja VASP-ide puhul on kriitilise tähtsusega, et Eesti teenusepakkujatel oleksid **sobivad ning nende riskide ja tehingumahtudega vastavuses protseduurilised ja tehnoloogilised lahendid ja tööriistad** nii **plokiahela analüüsimisel** kui ka **avalike allikate** kasutamisel.
- Tööriistad peaksid hõlmama ka **monitooringustsenaariume**, mis võtavad lisaks juhendmaterjalide indikaatoritele arvesse **konkreetselt sektori ja teenusepakkuja** ohte ja haavatavusi, trende ja tüpoloogiasid.
- Turuosalised peaksid virtuaalväringu tehingute tegijaid tuvastama kehtiva isikut tõendava dokumendi alusel, kontrollides perioodiliselt nende kontaktandmeid. Lisaks dokumentidele tuleb registreerida kontaktandmetena ka **sideandmed** (kõik meiliaadressid ja telefoninumbrid) ning **sotsiaalmeedias** kasutatavad kontod.
- Julgustada ja võimaldada töötajate spetsialiseerumist terrorismi rahastamise tõkestamisele kui spetsiifilisele valdkonnale, mis erineb rahapesu tõkestamisest.

<sup>45</sup> Kasulikke raporteid annavad lisaks Rahapesu Andmebüroo, Finantsinspektsiooni ja Kaitsepolitsei aastaraamatutele, juhenditele ja uuringutele välja muu hulgas järgmised organisatsioonid: FATF, RUSI, Project CRAFT, EUROPOL, EGMONT, Global Terrorism Index, International Centre for Counter-Terrorism, UNOCT, UNODC, UNOCT, UNCTED.



RAHANDUSMINISTEERIUM