TARTU ÜLIKOOL

ÕIGUSTEADUSKOND

Karistusõiguse osakond

Andre Paju

INTERNETIST TULENEVAD PROBLEEMID TERRORISMIVASTASEL VÕITLUSEL

Magistritöö

Juhendaja PhD Anneli Soo

Tartu

2020

SISUKORD

Sissejuhatus

21. sajandil on julgeolek nii Euroopas kui mujal maailmas keerulise iseloomuga. Üheks probleemiks Euroopa julgeolekule on kujunenud terrorism. Viimaste aastate jooksul on toimunud erinevates Euroopa riikides mitmeid terrorirünnakuid, mille tagajärjel on inimesed hukkunud või vigastada saanud. 2015. aastal toimus Euroopas 17 lõpuleviidut terrorirünnakut, mille tagajärjel hukkus 150 inimest, 2016. aastal toimus 13 rünnakut ning hukkus 135 inimest, 2017. aastal 33 rünnakut, hukkunuid oli 62.[1] Paljudes Euroopa riikides on terrorioht jätkuvalt kõrge ning tõenäoliselt see lähiaastate jooksul ei vähene ja terroristlikud rünnakud jätkuvad.[2] Selline olukord Euroopa riikides tekitab ühiskonnas hirmu ning toime pandud terrorirünnakud halvavad või peatavad tavapärast elurütmi.

Terrorism ei ole ühe riigi probleem, vaid on oma olemuselt muutunud globaalseks ning piiriüleseks julgeolekuprobleemiks. 2019. aastal Europoli[3] poolt koostatud raportist Euroopa Liidu terrorismi situatsiooni ja suundumuste kohta selgub, et 2015. aastal oli Euroopas kokku 211 terrorirünnakut, mille hulka loeti lisaks lõpuleviidud rünnakutele ebaõnnestunud või takistatud rünnakud. 2016. aastal oli selliseid rünnakuid 142, 2017. aastal 205 ning 2018. aastal 129. Kõige rohkem toimus rünnakuid Suurbritannias ning Prantsusmaal.[4] Võrdluseks rünnakute arvuga toimus kõige rohkem terrorismiga seotud arreteerimisi samuti Prantsusmaal ja Suurbritannias. Kokku arreteeriti Euroopas 2017. aastal 1219 terrorismiga seotud isikut, 2018. aastal 1056 inimest.[5]

Eesti Kaitsepolitseiameti sõnul on terrorioht Eestis madal,[6] kuid Eestil on siiski seos terrorismiga. 2017. aasta aprillis jättis Riigikohus jõusse ringkonnakohtu süüdimõistva

---

[1] Euroopa Parlament. Terrorism Euroopa Liidus: arvud ja faktid. – Arvutivõrgus: https://www.europarl.europa.eu/news/et/headlines/priorities/terrorism/20180703STO07125/terrorism-euroopa-liidus-arvud-ja-faktid (27.02.2020)

[2] Eesti Kaitsepolitseiamet. Kaitsepolitseiameti aastaraamat 2019. Tallinn: Kaitsepolitseiamet 2019, lk 39

[3] European Union Agency for Law Enforcement Cooperation ehk Europol on Euroopa Liidu õiguskaitseasutus.

[4] European Union Agency for Law Enforcement Cooperation. European Union Terrorism Situation and Trend Report 2019. Haag: European Union Agency for Law Enforcement Cooperation 2019, lk 11-12 – Arvutivõrgus: https://www.europol.europa.eu/activities-services/main-reports/terrorism-situation-and-trend-report-2019-te-sat (10.04.2020).

[5] European Union Terrorism Situation and Trend Report 2019, lk 15

[6] Eesti Kaitsepolitseiamet. Olukord Eestis. – Arvutivõrgus: https://kapo.ee/et/content/olukord-eestis-1.html (27.02.2020)

otsuse, mille kohaselt mõisteti Roman Mankole 2 aastat vanglakaristust selle eest, et toetas Süüriasse terrorirühmituse ridadesse siirdunud isikut. Sama kohtuasjaga mõisteti süüdi Ramil Khalilov 3-aastane vanglakaristus.[7] Lisaks on terrorirünnakud jõudnud Eestile küllaltki lähedale. 18.08.2017 toimus Soomes Turu linnas terrorirünnak, kus pussitati 10 inimest.[8]

Viimastel aastatel toimunud terrorirünnakute pinnalt nähtub, et terrorismi olemus on ajaga muutunud. Terrorirünnakuid toimub varasemast tihedamalt ning need on muutunud lihtsakoelisemaks. Terroriorganisatsioonid on hakanud üha rohkem ressurssi lääneriikides suunama propagandasse, mille kaudu soovitakse leida isikuid, kes ilma otsese kontakti või juhendamiseta suudaksid korraldada terrorirünnakuid.[9] Sellest tulenevalt ei pane terroriakte toime enam ainult Lähis-Idast tulnud võitlejad, vaid rünnakuid on korraldanud ning läbi viinud Euroopas elavad isikud. Terrorismivastase võitluse tulemusena on rahvusvahelisi terroriorganisatsioone suudetud nõrgestad ning vähendada nende kontrolli all olevaid maa-alasid Lähis-Idas. Seeläbi on suudetud kahandada terroristlike rühmituste võitlusvõimet ning uute rünnakute korraldamist, kuid terroristlike rühmituste rahvusvahelised võrgustikud tagavad nende püsimajäämise.[10]

Kuna terrorism on ajaga paljuski muutunud, tekitab see terrorismivastases võitluses uusi probleeme ning väljakutseid. Terroristlikud rühmitused kasutavad üha jõudsamalt tehnoloogia kiiret arengut enda eesmärkide saavutamiseks. Eriti suureks probleemiks on muutunud interneti kasutus, mille kaudu terroristidel õnnestub värvata uusi liikmeid Euroopast ilma, et need uued liikmed peaksid terroristlike rühmituste juurde kohale tulema. Kuna suurematel terroriorganisatsioonidel on rahvusvaheline võrgustik, siis kasutatakse lisaks värbamisele interneti ja sotsiaalmeediat ära suhtlemise ning materjalide ja informatsiooni edastamise jaoks. Internet pakub terroristlikele rühmitustele kiiret ning anonüümset keskkonda, kus omavahel suhelda või rünnakuid planeerida. Lisaks kasutatakse meediat inimeste hirmutamiseks ning enda põhiliste veendumuste ja eesmärkide teavitamiseks üldsusele.

---

[7] RKKKo 10.04.2017, 3-1-1-101-16

[8] Finnish Security Intelligence Service. Supo Year Book 2018, lk 17 - Arvutivõrgus: https://www.supo.fi/instancedata/prime_product_julkaisu/intermin/embeds/supowwwstructure/77291_WWW_SUPO_Juhlakirja_70_2019_ENG.pdf?52e507f9e2d6d788 (15.04.2020).

[9] Kaitsepolitseiameti aastaraamat 2019, lk 39-40

[10] Samas, lk 39

Terrorismi ei saa määratleda riigipiiridega, vaid see on piiriülene probleem, mis vajab aktiivset koostööd erinevate riikide, rahvusvaheliste organisatsioonide ning suurettevõtete[11] vahel. Seetõttu on oluline, et riigid ning organisatsioonid ühiselt terrorismi defineeriksid ning ühiste strateegia aluste kaudu terrorismi vastu võitleksid. Üha suurem roll terrorismivastases võitluses on ennetamisel, mille kaudu on võimalik ära hoida suuremaid terrorirünnakuid. Kuid terroristlikud rühmitused on järjest rohkem kasutama hakanud internetti, mistõttu on terrorismivastases võitluses oluline kindlaks teha, miks internetti kasutatakse ja milliseid viiside kaudu seda tehakse. Kuigi aktiivse võitlusega on nõrgestatud suuremaid terroristlike rühmitusi, ei takista see neid uute rünnakute planeerimisel või toimepanemisel.

Käesoleva magistritöö eesmärgiks on tuvastada, kuidas kasutatakse internetti terroristlikul eesmärgil, kuidas selle vastu võideldakse ning kas ja kuidas on Eesti õiguses reguleeritud sellevastane võitlus. Seatud eesmärgi saavutamiseks on püstitatud alljärgnevad uurimisküsimused:

1. Kui palju kasutavad terroristlikud rühmitused internetti enda eesmärkide täideviimiseks?
2. Mis põhjustel terroristlikud rühmitused internetti kasutavad?
3. Milliseid probleeme interneti kasutamine terroristlike rühmituste poolt tekitab?
4. Kas ja kui suurel määral toimub internetis võitlus terroristlike rühmitustega?
5. Millised on õiguslikud võimalused terroristlike rühmituste interneti kasutamise tõkestamiseks?
6. Kas käesolevas magistritöös vaadeldud Euroopa Liidu liikmesriikide õigusest terrorismivastase võitluse kohta on Eestil midagi õppida või üle võtta?

Töös on analüüsitud lisaks Eesti terrorismivastase võitluse strateegiale ja regulatsioonidele veel Euroopa Liidu ning Euroopa Liidu liikmesriikide Rootsi, Soome, Prantsusmaa, Suurbritannia[12] ning Saksamaa terrorismivastase võitluse regulatsioone ning strateegiaid. Suurbritannia, Prantsusmaa ja Saksamaa on Euroopa juhtivad riigid terrorismivastases võitluses. Nendes riikides on seaduse tasandil reguleeritud interneti kasutamine terroristlikul eesmärgil. Seega on nende riikide terrorismivastaste strateegiate ning

[11] Suurettevõtete all käesolevas magistritöös on mõeldud Google, Facebook, Twitter, Instagram ning teisi sama valdkonna suuri ettevõtteid.

[12] Suurbritannia lahkus Euroopa Liidust küll 31.01.2020, kuid käesolevas magistritöös on Suurbritanniat käsitletud veel Euroopa Liidu liikmesriigina.

regulatsioonide võrdlemise eesmärgiks hinnata, kas nende riikide õigusest ja strateegiast oleks Eestil otstarbekas midagi üle võtta. Lisaks nendele kolmele terrorismivastast võitlust juhtivale Euroopa riigile on käesolevas töös vaadeldud Soome ja Rootsi terrorismivastaseid strateegiaid ja regulatsioone. Soome ja Rootsi on tugeva heaoluühiskonnaga riigid, mistõttu võib nende riikide terrorismivastases võitluses leida valdkondi, mida Eesti strateegiasse üle võtta. Kõikide töös käsitletud riikide seaduste ning strateegiate puhul on vaadeldud neid paragrahve ja punkte, mis võiksid magistritöö teemaga kokku puutuda ning püstitatud uurimisküsimustele vastuseid anda.

Tegemist on kvalitatiivse uurimistööga, milles õigusdogmaatiline käsitlus põhineb terrorismi kui nähtuse toimimise analüüsil.

Käesolev töö on jaotatud kaheks suuremaks peatükiks. Töö esimene peatükk käsitleb terrorismi defineerimise raskuseid, terrorismi olemuse muutust ajaga ning terrorismivastast võitlust. Terrorismi defineerimine on oluline, kuna terrorismivastases võitlus on piiriülene ning oluline on riikide vaheline koostöö. Sellest tulenevalt on vajalik, et riigid defineeriksid terrorismi sarnaselt. Kuna tehnoloogia pakub terroristlikele rühmitustele erinevaid uusi võimalusi, on töö esimeses peatükis välja toodud, kuidas terrorism on läbi aegade arenenud ning milliseks oma olemuselt muutunud. Selles peatükis on välja toodud peamised viisid, kuidas terroristlikud ühendused internetti kasutavad ning millised probleemid sellega tekivad. Lisaks on esimeses peatükis on välja toodud terrorismivastase võitluse praktilised sammud, mis ilmestavad, kuidas terrorismi vastu võideldakse.

Magistritöö teine peatükk keskendub õigusliku regulatsiooni analüüsile**.** Selles peatükis on välja toodud Euroopa Liidu ja liikmesriikide strateegiad terrorismiga võitlemisel. Käesoleva töö teise peatüki eesmärgiks on välja selgitada, kas Eestil on magistritöös analüüsitud riikidega terrorismivastasel võitluse strateegiatest ning regulatsioonidest midagi üle võtta. Selle peatüki põhiline eesmärk on välja selgitada, millised on õiguslikud võimalused terroristlike rühmituste interneti kasutamise vastu võitlemisel.

Tööd iseloomustavad märksõnad: karistusõigus, terrorism, terrorismivastane võitlus, internet.

1. Terrorismi definitsioon ja areng ajas

1.1. Terrorismi definitsioon

Terrorismi puudutavate regulatsioonide mõistmiseks tuleb aga kõigepealt vaadelda, kuidas terrorismist kui mõistest rahvusvaheliselt aru saadakse. See on oluline, et rahvusvaheline koostöö riikide ja organisatsioonide vahel toimiks ühtselt ning kõigile osapooltele arusaadavalt. Rahvusvaheliselt ei ole suudetud leida ühist definitsiooni, mille järgi terrorismi määratleda. Mitmete rahvusvaheliste organisatsioonide, teadlaste ja erialaekspertide poolt on üritatud välja selgitada terrorismi kõiki aspekte hõlmav definitsioon, kuid see on osutunud problemaatiliseks ning tekitanud mitmeid eriarvamusi.[13]

Terrorismi defineerimine sai alguse juba 20. sajandi esimesel poolel. Kahe maailmasõja vahelisel perioodil, aastatel 1920-1930, toimusid erinevates Euroopa pealinnades konverentsid rahvusvahelise karistusõiguse ühtlustamise osas. Nende konverentside üheks tulemiks võiks lugeda esmaseid terrorismi defineerimise üritusi. 1935. aastal Kopenhaagenis toimunud konverents anti terrorismile definitsioon erinevate kuritegude loetelu kaudu.[14]

1937. aastal toimunud Rahvasteliidu konverentsil koostati terrorismi ennetamise ja karistamise konventsioon[15], mille artikkel 1 määratles terrorikuriteod. Selles artiklis välja toodud definitsioon ei määratle küll terrorismi kõiki aspekte, vaid keskendub peamiselt ainult terrorikuritegude välja toomisele. Ehk juba esimesest defineerimise üritusest alates lähtuti terrorismi määratlemisel kuritegude loetelust, mille sooritamine riigi vastu loetakse terrorikuriteoks.

Hollandi teadlane Alex P. Schmid viis 1980. aastatel läbi uurimise, millega soovis leida terrorismi definitsiooni. Alex P. Schmid oli seisukohal, et terrorismi tuleb määratleda kitsalt ning terrorismi tuleb eristada muudest poliitiliste kuritegude vormidest. Selleks tõi

[13] Kaitsepolitseiamet. Terrorismi mõiste. – Arvutivõrgus: https://kapo.ee/et/content/terrorismi-mõiste.html (27.02.2020)

[14] Levitt, G. Is Terrorism Worth Defining. – Ohio Northern University Law Review 13, no. 1. (1986), lk 97-100

[15] League of Nations. Convention pour la prévention et de la répression du terrorisme/ Convention for the Prevention and Punishment of Terrorism, 1937.

Schmid välja analoogina sõjakuriteod, mis on eristatud õigustatud sõjapidamisest. Ta leidis, et nii ÜRO konventsioonides kui ka teistes rahvusvahelistes õigusaktides on terrorismi defineeritud liiga laialt ning on maha jäädud terrorismi arengutele. Tema arvates tekitab liiga lai terrorismi definitsioon juurde suuremal hulgal olukordi, mil tuleb terrorismi vastu võidelda.[16]

Boaz Ganor[17] pakkus samuti välja terrorismi definitsiooni. Ganori arvates on terrorism vägivalla kavatsetud kasutamine tsiviilisikute või –objektide vastu või sellega ähvardamine poliitiliste eesmärkide saavutamiseks.[18] Sellel definitsioonil oli mitmeid puuduseid, mis takistavad selle sõnastuse kasutamist rahvusvaheliselt. Näiteks ei saa sellise definitsiooni järgi terrorismiks lugeda kaasnevat kahju tsiviilisikute hulgas, kui tegelikult oli vägivald suunatud sõjalise sihtmärgi vastu.[19]

Üheks probleemiks, miks ei ole suudetud terrorismi defineerida, et see oleks rahvusvaheliselt vastuvõetav, võib pidada asjaolu, et terrorism on tihedalt seotud poliitiliste motiividega. Seetõttu on keeruline terroriste käsitleda tavaliste kurjategijatena, kuna nende tegevuse ajendiks ei ole üldiselt ahnus või himu. Terroristid osalevad rahvusvahelises vaenutegevuses, kuid üldiselt ei liigitata neid samasse kategooriasse tavaliste relvajõududega. Probleeme tekitab terroristlike rühmituste rahvusvaheline määratlemine. Mõned terroristlikud rühmitused on niivõrd hästi organiseeritud, et neid võiks pidada riikideks, kuid tegelikult need rühmitused ei tegutse riikide nimel. Terroriorganisatsioonide korraldatud rünnakud mõjutavad paljusid riike ning vastumeetmete leidmine on raskendatud. Nende põhjuste tõttu on terrorismi raske sobitada mõne traditsioonilise rahvusvahelise õiguse kategooria alla ning seetõttu tekitab raskusi ka terrorismi liigitamine rahvusvahelises õiguses.[20]

Teine probleem tekib aga sellega, et kui ühtede meelest on tegemist terrorismiga, siis teiste jaoks on see aga hoopis õilis vastupanuvõitlus. Selle kohta on ütlus: ühe mehe terrorist on

---

[16] Schmid, A. P. The Way Forward on Counter-Terrorism: Global Perspectives. – Strathmore Law Journal 2 (2016), lk 52-53

[17] Boaz Ganor on Rahvusvahelise Terrorismivastase Poliitika Instituudi asutaja ja tegevdirektor

[18] Ganor, B. Defining Terrorism: Is One Man's Terrorist Another Man's Freedom Fighter? – Police Practice and Research: An International Journal. Volume 3, 2002, lk 287-289

[19] Värk, R. Riikide enesekaitse ja kollektiivse julgeolekusüsteemi võimalikkusest terroristlike mitteriiklike rühmituste kontekstis. Doktoritöö. Juhendaja Raul Narits. Tartu Ülikooli Kirjastus, 2011, lk 46

[20] Klabbers, J. Rahvusvaheline õigus. (Tallinn: Juura 2018), lk 268

teise vabadusvõitleja.[21] Tegemist on kahe erineva maailmavaate põrkumisega, kus on keeruline leida kompromissi. Üheks võimalikuks lahenduseks oleks jõuda algallikani, mis põhjustab konflikte. Seejärel peaks üks osapool loobuma enda vaadetest ning muutma oma veendumusi ja põhimõtteid. Näiteks peaksid Euroopa Liidu liikmesriigid muutma enda põhimõtteid terrorismi osas ning nõustuma terroristlike rühmituste välja toodud poliitiliste vastuoludega, mida tuleks terroristide meelest parandada. Selline olukord tähendaks rahvusvaheliselt kokkulepitud inimõiguste ning ka muude ühiskonna aluspõhimõtete hävitamist.

Nagu eelpool mainitud pole rahvusvaheliselt suudetud leida ühist definitsiooni. 2001. aastal võttis ÜRO vastu rahvusvahelise lepingu terroriaktide tõkestamiseks, kuid mõistet "terrorist" ei suudetud defineerida. See leping hõlmas väikest osa terrorismist ning terrorismi definitsiooni põhjendati poliitiliselt: vägivallaakt loetakse terroristlikuks, kui see põhjustab tõenäoliselt majanduslikku kahju, kui eesmärgiks on hirmutada elanikkonda, kui tahetakse sundida valitsust või rahvusvahelist organisatsiooni tegema või hoiduma konkreetsest tegevusest. 2007. aastal muudeti definitsiooni akadeemilisemaks ja üksmeelsemaks.[22] Terrorismi defineerimist saab pidada väljakutseks, sest läbi ajaloo on üritatud leida rahvusvaheliselt sobivat ühist definitsiooni, kuid senimaani pole see veel kõiki riike rahuldavat tulemust toonud.

Terrorismi defineerimisel on riigid lähtunud terrorikuriteo mõiste lahtiseletamisest ning senimaani on suuremas osas rõhk olnud karistamisel. See tähendab seda, et on välja toodud kindel loetelu, mida peetakse terroriaktideks. Kuid terrorism areneb samamoodi nagu ühiskond või tehnoloogia, mistõttu on vaja aja jooksul järjest rohkem tähelepanu pöörata terrorismiga seotud ja seda hõlbustavale tegevusele. Näiteks 1999. aastal sõlmiti terrorismi rahastamise tõkestamise rahvusvaheline konventsioon[23], mille kohaselt terroristlikuks tegevuseks vahendite andmine ja kogumine on karistatav.

Eestis on terrorikuritegu sätestatud karistusseadustikus (KarS)[24] § 237 lg 1:

---

[21] Klabbers, J, lk 266

[22] Bruce, G. Definition of Terrorism – Social and Political Effects. – Journal of Military and Veterans' Health, Volume 21 No. 2. 2013, lk 26-27

[23] Terrorismi rahastamise tõkestamise rahvusvaheline konventsioon – RT II 2002, 12, 45.

[24] Karistusseadustik – RT I, 28.02.2020, 5.

Rahvusvahelise julgeoleku vastase, isikuvastase, elu või tervist ohustava keskkonnavastase,välisriigi või rahvusvahelise organisatsiooni vastu suunatud või üldohtliku kuriteo toimepanemise, keelatud relva tootmise, levitamise või kasutamise või vara ebaseadusliku hõivamise või olulises ulatuses rikkumise või hävitamise või arvutiandmetesse sekkumise või arvutisüsteemi toimimise takistamise eest, samuti selliste tegude toimepanemisega ähvardamise eest, 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.

Õigushüvena kaitstakse eelkõige sisemist ja rahvusvahelist julgeolekut, kuid ka riigi ja rahvusvaheliste organisatsioonide funktsioneerimisvõimet ning avalikku rahu. Koosseisutüübilt on tegemist alternatiiv-aktilise abstratkse ohudeliktiga. Tegemist on blanketse deliktidega, kuna koosseisupäraste tegude sisustamiseks tuleb pöörduda teiste karistusseadustikus sätestatud kuriteokoosseisude poole.[25]

Euroopa Parlamendi ja Nõukogu direktiivi 2017/541 terrorismivastase võitluse kohta[26] artiklis 3 on välja toodud terroriakti definitsioon. Artikkel 3 kohaselt võtavad liikmesriigid vajalikud meetmed, et tagada järgmiste siseriikliku õiguse kohaselt kuriteona määratletud tahtlike tegude, mis oma laadi või seose tõttu võivad tõsiselt kahjustada mõnd riiki või rahvusvahelist organisatsiooni, käsitamine terroriaktina, kui nende toimepanemise eesmärk on üks lõikes 2 loetletutest:

a) rünnakud inimelu vastu, mis võivad põhjustada surma;

b) rünnakud isiku kehalise puutumatuse vastu;

c) inimröövi või pantvangi võtmine;

d) riikliku või avaliku rajatise, transpordisüsteemi, infrastruktuurirajatise, sealhulgas infosüsteemi, mandrilavale kinnitatud aluse, avaliku koha või eraomandi tõsine kahjustamine, mis võib ohustada inimelu või põhjustada suurt majanduslikku kahju;

[25] Kiris, R. KarS § 237/1-2. – Karistusseadustik. Kommenteeritud väljaanne. 4 vlj. Tallinn: Juura 2015.

[26] Euroopa Parlamendi ja Nõukogu direktiiv (EL) 2017/541 terrorismivastase võitluse kohta, millega asendatakse nõukogu raamotsus 2002/475/JSK ning muudetakse nõukogu otsust 2005/671/JSK – ELT L 88/6, 15.03.2017

e) õhusõiduki, laeva või mõne muu ühistranspordi- või kaubaveovahendi ebaseaduslik hõivamine;

f) lõhkeainete või relvade, sealhulgas keemia-, bioloogiliste, radioloogiliste või tuumarelvade valmistamine, valduses hoidmine, omandamine, vedu, tarnimine või kasutamine, samuti keemia-, bioloogiliste, radioloogiliste või tuumarelvadega seotud teadus- ja arendustöö;

g) ohtlike ainete heite või tulekahjude, plahvatuste või üleujutuste põhjustamine, kui see ohustab inimelu;

h) vee, elektri või mõne tähtsa loodusvaraga varustamise häirimine või katkestamine, kui see ohustab inimelu;

i) ebaseaduslik süsteemi häirimine, nagu on osutatud Euroopa Parlamendi ja nõukogu direktiivi 2013/40/EL (1) artiklis 4, neil juhtudel, kui kohaldatakse kõnealuse direktiivi artikli 9 lõiget 3 või lõike 4 punkti b või c, ning ebaseaduslik andmetesse sekkumine, nagu on osutatud nimetatud direktiivi artiklis 5, neil juhtudel, kui kohaldatakse kõnealuse direktiivi artikli 9 lõike 4 punkti c;

j) mõne punktides a–i loetletud teo toimepanemisega ähvardamine.

Terrorismil on mitmeid eesmärke. Üheks eesmärgiks on üldiselt mingisuguste poliitiliste nõuete rahuldamine, mida näiteks terroristlik rühmitus enda arvates ei suuda saavutada poliitiliste või majanduslike meetodite abil. Sageli loodetakse saavutada koheseid tulemusi: hirm, surve avaldamine, radikaalne poliitiline muutus, abinõud, mis ohustavad süütute osapoolte põhilisi vabadusi.[27] Terroristlike rühmituste eesmärgiks on inimõiguste, demokraatia ja õigusriigi hävitamine. Seetõttu üritatakse rünnata just neid väärtusi, mis on ÜRO põhikirja ning teiste rahvusvaheliste õigusaktide keskmes: inimõiguste austamine, rahvaste ja rahvuste sallimine, relvastatud konfliktide ja tsiviilelanike kaitset regulatsioonid, konflikti rahumeelne lahendamine. Terrorismil on otsesed mõjud mitmele inimõigustele: õigus elule, vabadusele, füüsilisele puutumatusele. Lisaks võivad terroriaktid valitsusi destabiliseerida ning kahjustada ka ühiskonda, eelkõige rahu ja

[27] Holms, J.P. Burke, T. Terrorism: Tänapäeva suurim oht vabadusele. Tallinn: Ersen 2002, lk 20

julgeoleku seisukohalt, aga sotsiaalse ja majandusliku poole pealt. Neil kõigil on aga otsene mõju põhiliste inimõiguste kasutamisele.[28]

1.2. Terrorismi areng läbi aegade

Terrorism on olnud riikide julgeolekule probleemiks pikka aega. 19. sajandi teisel poolel hakkasid Euroopas pead tõstma teisitimõtlejad, kelle tegevust tol ajal võib lugeda alguseks süstemaatilisele terrorismile. Trüki-ja kirjastustehnoloogia areng lõi nende jaoks võimalused levitada enda ideid ning uudset mõtlemist laiemale hulgale. Seeläbi saadi suurema avalikkuse tähelepanu.[29] Loomulikult ei saa nende 19. sajandi teisitimõtlejate ning praeguste terroristlike ühenduste tegemiste vahele tõmmata võrdlusmärki, kuid sarnasusi on mitmetes aspektides. Põhiliseks on see, et eesmärkide saavutamiseks ollakse kõigeks valmis, ka vara hävitamiseks või inimeste tapmiseks. Ühiseks tunnusjooneks võib pidada ka ajendit, kuna ka tänapäeval on terrorirühmitustel poliitilised veendumused terrorirünnakute korraldamiseks.

David Charles Rapoport[30] on välja toonud terrorismi ajaloos neli erinevat perioodi. Esimeseks perioodiks saab pidada anarhistlikut, mis algas Venemaal 1880.aastatel ning kestis 1920. aastateni. See sai alguse anarhistide rahulolematusest Vene ühiskonna reformide aeglusega. Anarhistid püüdsid ühiskonna käitumisnorme ja tõekspidamisi terroriaktidega lõhkuda. Nende eesmärgiks oli terroriaktide kaudu õõnestada ühiskonnas kehtivaid reegleid ja norme. Teine ehk koloniaslismivastane terrorilaine algas 1920. aastatel ning lõppes 1960. aastatel, kolmas (vasakpoolne) terrorilaine algas 1960. aastatel, lõppes 1980. aastatel. Pärast seda algas viimane ehk religioosne terrorilaine ning see kestab tänapäevani.[31]

---

[28] Office of the United Nations. High Commissioner for Human Rigts. Human Rights, Terrorism and Counter-terrorism. Fact Sheet no. 32, lk 7 – Arvutivõrgus: https://www.refworld.org/docid/48733ebc2.html (10.02.2020)

[29] Holms, J.P, Burke, T, lk 17

[30] David Charles Rapoport on California Ülikooli emeriitprofessor, kes uuris terrorismi ning on asutanud ajakirja Terrorism and Political Violence.

[31] Rapoport, D.C; Cronin, A.K.; Ludes, J.M. Four Waves of Modern Terrorism. – Attacking Terrorism: Elements of a Grand Strategy. Washington DC: Georgetown University Press 2004, lk 47

Rapoporti poolt välja toodud periodiseering on mitmete teiste autorite poolt saanud kriitikat ning täpsustusi. Mark Sedgwick[32] oli küll üldiselt Rapoporti poolt välja pakutud periodiseeringuga nõus, kuid juhtis tähelepanu asjaolule, et tegelikult võis 1820. aastatel terrorismi laine hoopis Itaalias alata. Lisaks tõis Sedgewick välja, et ajavahemikus 1920-1960 tegutses maailmas rohkem terroristlike rühmitusi, kui tavaliselt mainitud on. Sedgewicki sõnul on terrorismi leviku kiirust mõjutanud väga suuresti just teiste terrorirühmituste strateegiate õppimine ja omandamine.[33]

Thomas Mockaitis[34] sõnul on Rapoport esitanud terrorismi osas olulised perioodid, kuid lisas nendele teatud erandid. Thomas Mockaitise arvates on mitmed uusvasakpoolsed terroristid teadlikult enda määratlenud hoopis anarhistidena. Teiseks tõi ta välja, et kolonialismivastaste terrorirühmituste tegevus muutus massiliseks alles pärast 1945. aastat. Põhiline erand, mille Mockaitis välja tõi oli see, et enamik religioosse terrorilaine rünnakuid on tegelikult ühe religiooni ehk islami järgijad toime pannud. Selle põhjal tõi Mockaitis välja, et suurem tähelepanu tuleb pöörata islami religioonile.[35] Seega saab Rapoporti poolt välja toodud periodiseeringut üldises plaanis üsna tõsiselt võtta ning selle järgi juhinduda. Loomulikult peab ka Rapoporti periodiseeringu kohta kriitikat avaldanud autoreid arvestama ning üldplaanis nende põhjal kokkuvõtteid tegema. Koos kriitikaga on selline periodiseering laialdasem ning mitmekülgsem.

Religioosne terrorism on viimastel aastakümnetel muutunud kõige levinumaks terrorismi liigiks. Religioosne terrorism erinevalt teistest terrorismi liikidest rahvusvaheline, kuna islamistlike terrorirühmituste põhiliseks eesmärgiks on Lääne tsivilisatsiooni mõju kaotamine islamimaailmas ning kogu islamimaailma ühendamine ühtseks kalifaadiks nagu prohvet Muhamedi ajal. 11.09.2001 USA-s toimunud terrorirünnak on üheks näiteks, milleks on valmis enda usu nimel võitlevad terroristid. Nende poolt korraldatud terrorirünnakute tagajärjed on raskemad ning ühiskonnale veel suurema mõjuga kui poliitiliste eesmärkide poole püüdlevad terroristid. Seda USA-s toimunud terrorirünnakut

[32] Mark Sedgwick on Briti ajaloolane, kes on spetsialiseerunud muuhulgas terrorismi uurimisele.

[33] Sedgewick, M. Inspiration and the Origins of Global Waves of Terrorism. – Studies in Conflict & Terrorism, Volume 30. 2007, lk 97–112

[34] Thomas Mockaitis on Wisconsini ülikooli professor.

[35] Mockaitis, T.R. The “New” Terrorism: Myths and Reality. London: Praeger Security International, 2007, lk 38

peetakse üheks olulisemaks murdepunktiks ajaloos terrorismivastasel võitlusel.[36] Seda kuupäeva võib pidada alguseks terrorismi sõjale. 11.09.2001 toimunud terrorirünnak on kõige ohvrite rohkem rünnak ajaloos. Koheselt pärast terrorirünnakuid alustas USA vasturünnakuid terroristlikele rühmitustele, mille tulemusena hakkas aktiivne võitlus terrorismiga Lähis-Idas.[37]

Terrorism on tänapäeval väga aktuaalseks teemaks. Igapäevased on uudised, kus antakse teada, et terroristlike rühmituste valduses olevatel territooriumidel käib aktiivne võitlus. See aga ei tähenda, et nende territooriumide pommitamine nende tegevust täielikult takistaks ning terroristlikud rühmitused üritavad muutuvate oludega kohaneda. Seda ilmestab näiteks Islamiriik[38], mille retoorikas toimus 2016. aasta mais muutus, mille kohaselt ISIS-le ei ole enam oluline territoorium, vaid ideoloogia. ISIS on kaotanud suurel hulgal rühmituse kontrolli all olevaid territooriume, mistõttu on ISIS muutnud oma narratiivi, mille põhiline rõhk on veelgi rohkem suunatud lääneriikidele, kus korraldada senisest veelgi rohkem terrorirünnakuid. Üheks põhjuseks, miks seda soovitakse teha, on vajadus tõestada, et nad on suutelised selliseid rünnakuid korraldama. Terrorirühmituse korraldatud rünnakud on muutnud sihtmärke ning sooritamise vahendeid, mis omakorda tekitab raskusi terrorismivastasel võitlusel, kuna rünnakute korraldamise muutus teeb raskemaks ennustamise, kus võib terrorirünnak toimuda. See jällegi võib tähendada seda, et rünnakute tagajärjed võivad muutuda veelgi jõhkramaks, kuna avastamise tõenäosus on väiksem.[39] Selline muutus rünnakute sihtmärkide või vahendite osas näitab, et terroristlikud rühmitused on analüüsivõimelised, kuidas ja mis viisil on rünnakud nende eesmärkide jaoks edukamad. Sellest lähtuvalt suudavad nad leida alternatiive, mille abil oma eesmärke ellu viia. Terroristlike rühmituste oludega kohanemine muudab järjest rohkem terrorismi olemust.

Tänapäeva ühiskonna üheks tunnusjooneks on tehnoloogia kiire areng. Heaks näiteks on interneti kasutamise võimalus. Võrreldes 21. sajandi algusega, oleme jõudnud sellisesse

---

[36] Eesti Kaitsepolitseiamet. Terrorismi liigid – Arvutivõrgus: https://www.kapo.ee/et/content/terrorismi-liigid.html (13.01.2020)

[37] Ritchie, H.; Hasell, J.; Appel, C.; Roser,M. Terrorism. – Arvutivõrgus: https://ourworldindata.org/terrorism (15.02.2020)

[38] Terroristlik rühmitus Islamiriik, tuntud ka kui ISIS või IS. Käesolevas magistritöös kasutatakse selle rühmituse puhul lühendit ISIS.

[39] Teabeamet. Eesti rahvusvahelises julgeolekukeskkonnas 2017. (Tallinn: Teabeamet 2017), lk 56-59 – Arvutivõrgus: https://www.valisluureamet.ee/pdf/TA_raport_2017_EST.pdf (15.04.2020)

olukorda, kus suuremal osal inimestest on olemas nutitelefon, millega omab juurdepääsu interneti avarustesse. Eestis on inimestel internetiühendus nii Tallinna vanalinnas kui ka Lõuna-Eesti metsade vahel. Mujal maailmas on samuti tehnoloogia abil inimestel praktiliselt kõikjal olemas püsiv internetiühendus, mida nad saavad enda nutitelefonidega kasutada. See on ainult üks näide, mis ilmestab tõsiasja, et tehnoloogia on muutnud 21. sajandi inimese elu palju mugavamaks.

Terrorismi võib pidada hetkel ühiskonna üheks suurimaks julgeoleku ja rahu ohuks ning tehnoloogia areng tekitab terrorismivastases võitluses uusi probleemseid kohti. Seetõttu on oluline terrorismivastases võitlust teada, kuidas tänapäeva terroristlikud rühmitused üldse enda eesmärkide täideviimiseks tehnoloogia arengut ära kasutavad. Põhiliselt kasutavad terroristlikud ühendused tehnoloogiat ära turvalise side loomiseks, värbamise, psühholoogilise sõjapidamise, propaganda levitamise, teabe kogumise ja küberrünnakute jaoks. Näideteks, kuidas tehnoloogiat kasutatakse, on masinõpe, tehisintellektid, robotid, mehitamata sõidukid, biotehnoloogia, 3D-printimine ja nanotehnoloogia. Tehnoloogiat kasutatakse ära ka terrorirünnakute korraldamiseks. Terroristidel on samuti võimalik kasutada erinevate rünnakute korraldamiseks mehitamata sõidukeid ning droone. tehnoloogia arenguga on loodud võimalused valmistada ka järjest võimsamaid ning ohtlikemaid relvi, siis on ka terroristlikud rühmitused seda enda kasuks ära kasutanud, kuna terroristide käsitluses on ka massihävitusrelvad.[40] Samuti võimaldab Google Maps terroristidel rünnakuks ettevalmistusi teha. Seda ilmestab Al Qaeda terrorirühmituse propagandavideo[41], millelt nähtub, et rühmituse liikmed kavandavad Lähis-Idas rünnakut ning kasutavad selleks Google Mapsi abi.

Terroristlikul eesmärgil interneti kasutamine aitab terroristlikel rühmitustel tugevadada rahvusvahelist võrgustikku, kuna internet, sealhulgas meedia ja sotsiaalmeedia, pakub lihtsat ja kiiret juurdepääsu miljonitele inimestele. Meedia kaudu on levinud tohutult suurel hulgal videoid ja pilte terroristlike rühmituste tegemiste kohta, millega paljud inimesed on mingilgi määral kokku puutunud, seda nii Eestis kui mujal maailmas. Selleks võib olla mõni terrorirünnaku kajastus mõnes meediaväljaandes või propagandavideo

[40] North Atlantic Treaty Organization, Weapons of mass destruction. – Arvutivõrgus: https://www.nato.int/cps/en/natohq/topics_50325.htm (15.03.2020)

[41] Daily Mail, Terrorism 2018: Al Qaeda uses Google Maps to plan a terrorist attack in new propaganda video that features a former Guantanamo prisoner. 21.04.2018. – DailyMail. Arvutivõrgus: https://www.dailymail.co.uk/news/article-5642361/Al-Qaeda-appears-use-Google-Maps-plan-terrorist-attack-new-propaganda-video.html (10.02.2020)

terrorirühmituste poolt. Seega on oluline kindlaks teha, kuidas üldse terroristlikud rühmitused interneti kasutavad ning mis on põhilised põhjused, miks internetti, meediat ja sotsiaalmeediat neil vaja on.

Äärmuslike veendumuste ja väärtuste tõttu nõuavad terroristid anonüümsust. Nad tegutsevad sotsiaalses keskkonnas, mis ei pruugi nende konkreetse ideoloogia või tegevusega nõustuda. Internet pakub esmapilgul kõikidele kasutajatele anonüümsust. Lisaks iseloomustab internetti veel juurdepääsu lihtsus, kiire infovoog ning suur potentsiaalne publik. Samuti pole veel välja kujunenud interneti kasutamise osas kindel regulatsioon ning interneti kasutamine on odav.[42] Ehk kõik need aspektid omavad olulist rolli sellel, miks terroristlikud ühendused internetti enda eesmärkide täideviimiseks väga jõuliselt on kasutama hakanud.

Terrorirühmitus ISIS oli suure tõenäosusega esimene rühmitus, kes hakkas terroristlikul eesmärgil internetti ja sotsiaalmeediat kasutama. Selleks hakkas rühmitus korraldama online-propaganda kampaaniad, mille eesmärgiks oli uute liikmete värbamine. Need kampaaniad sisaldasid endas erinevaid videoid, millega anti teada enda veendumustest ja eesmärkidest. Lisaks oli videote eesmärgiks ühiskonnas hirmu külvamine. Bruce Hoffman mainis juba 2006. aastal, et internet on muutumas üheks olulisemaks propaganda tööriistaks terroristlike rühmituste jaoks. Hoffmann väitis, et terroristidel on internetis võimalik odavate, kuid samas professionaalselt toodetud ja redigeeritud videote kaudu levitada enda veendumusi. Sellised videod võimaldavad terroristidel suhelda ilma tsensuuri või muude takistusteta ning lisaks meelitada uusi allikaid värbama, rahastama ja toetama.[43]

Internet on terroristlike rühmituste jaoks kui ressurss, mida igapäevaselt kasutatakse. Tehnilisest vaatepunktist ei erine terroristide interneti kasutamine oluliselt interneti tavaliste inimeste igapäevasest kasutamisest, kuna nad kasutavad sama lihtsat juurdepääsu, kergesti kasutatavat või täiustatud internetiteenuseid, mida kõik teised kasutajad. Terroristid kasutavad vägivaldse propaganda materjali levitamiseks sotsiaalmeediat, kus alustatakse ka uute liikmete värbamist ja radikaliseerumist. Radikaliseerunud inimeste puhul hakatakse neid meelitama ideoloogiliste veebisaitide kaudu, kus propageeritakse

[42] Weimann, G. Terror on the Internet: The New Arena, the New Challenges. (Washington, DC: Endowment of the United States Institute of Peace, 2006), lk 4

[43] Hoffman, B. Inside terrorism. (New York; Columbia University Press, 2013), lk 199-200

vägivalda. Lisaks kasutatakse neid veebisaite käsiraamatutena ning muu teabe levitamiseks rünnakute ja muude kuritegude kavandamise, korraldamise ja läbiviimise kohta.

Kuigi sotsiaalmeedia platvormid pakuvad terroristlikele rühmitustele kerge ligipääsu suurele publikule, mida kasutatakse ära propaganda levitamiseks ning uute liikmete värbamiseks, on suurematel terrorirühmitustel ka enda meediakanaleid, mille kaudu hakatakse levitama propagandat. Selleks kasutatakse ära sotsiaalmeedia võimalusi, kuna sotsiaalmeedia platvormid on eemaldanud täielikult sisu barjääri sõnumi saatja ja sõnumi saaja vahel.[44] Internet ja küberruum on ideaalseks kohaks, kus on võimalik nii suhelda kui ka oma tegevusi koordineerida. Selle kasuks räägivad kiirus, lihtsus ja anonüümsus. Kõik need aspektid raskendavad jälgimist ning järelevalvet ja kontrolli internetis ning küberruumis toimuva üle. Kui on selge, et terroristlikud rühmitused kasutavad peamiselt internetti uute liikmete värbamiseks, propaganda levitamiseks ning suhtlemiseks, siis on teada ka juhtumitest, kus on terrorirühmitused toime pannud traditsioonilisi küberkuritegusid nagu näiteks pettused.[45]

Terroristid on välja töötanud keerukad krüpteerimisvahendid ning veel muud loomingulised tehnikad, mis muudavad interneti nende jaoks tõhusamaks ja turvalisemaks. Nende hulka kuuluvad näiteks steganograafia[46] ehk tehnika, mida kasutatakse erinevate sõnumite peitmiseks graafikafailidesse. Terroristlikud rühmitused edastavad omavahel teavet salvestatud e-kirjade kaudu e-posti kontole, mis on kättesaadavad kõigile, kellel on parool.[47] Need on ainult kaks näidet, kuidas on terroristlikud ühendused leidnud võimaluse suhelda ning materjale jagada nende jaoks turvalisel viisil, kuna kõike internetis kontrollida on suhteliselt võimatu missioon. Üha rohkem kasutatakse terroristlike rühmituste poolt krüpteeritud sideplatvorme, mis peidavad kasutajaidentiteete. Näiteks platvormi Telegramm kaudu saavad terroristlikud rühmitused suhelda salaja võrgus, kuna neil on võimalik oma tegevuste ja rünnakute koordineerimisel põhivõrgust välja minna. Lisaks kasutatakse terroristlike rühmituste poolt Threema, Kik, Wickr, SureSpot and

[44] Bertram, L. Terrorism, the Internet and the Social Media Advantage: Exploring how terrorist organizations exploit aspects of the internet, social media and how these same platforms could be used to counter-violend extremism. – Journal for Deradicalization, Summer 2016 nr 7, lk 233

[45] Biller, J.T. Cyber-Terrorism: Finding a common starting point. – Journal of Law, Technology & The Internet, Vol 4, No 2, 2013, lk 317-319

[46] Informatsiooni peitmise tehnika

[47] Kaplan, E. Terrorists and the Internet – Council on Foreign Relations. Arvutivõrgus: https://www.cfr.org/backgrounder/terrorists-and-internet (15.03.2020).

WhatsApp programme suhtlemiseks ning värbamiseks.[48] Kõik need platvormid võimaldavad anonüümset ning üsnagi turvalist suhtlemist, mis ongi peamiseks põhjuseks, miks terroristid neid kasutavad. Probleemseks on krüpteeritud suhtlus, mida on keeruline avastada. Krüpteeritud suhtlust kasutavad ka paljud inimesed, asutused ning organisatsioonid, kellel on kokkupuude mõne salastatud teabega. Seega terroristlikel rühmitustel on võimalus suhelda turvaliselt ning anonüümselt internetis legaalsete platvormide kaudu.

Nagu eelpool kirjeldatud on tänapäeva terrorism on väga suurel hulgal internetiga seotud. Kõigil suurtel või väikestel terroristlikel organisatsioonidel on enda veebisaidid, mille kaudu saavad nad enda propagandat levitada ja enda eesmärkidest muule maailmale teada anda. Kuid lisaks kasutatakse selliseid veebisaite rahaliste vahendite kogumiseks ja rahapesuks, aga ka uute liikmete värbamiseks ja koolitamiseks, suhtlemiseks ning rünnakute käivitamiseks.[49]

Ilmestamaks probleemi tõsidust saaks tuua ühe aktuaalse näite tänapäeva terrorismi võimalusest. Praegusel ajal ei pea enam uue liikme värbamiseks seda isikut enda rühmituse juurde kohale kutsuma, vaid piisab internetist, mille kaudu saab esmalt mõne sarnaste veendumustega isikuga ühendust võtta, seejärel enda eesmärke ja ideoloogiat sellele isikule tutvustada. Seda võib piltlikult öeldes pidada selliseks faasiks, kus üritatakse isikut enda rühmitusse värvata, rääkides ja tutvustades talle terroristliku rühmituse põhimõtteid. Kui see värbamine osutub edukaks, saab interneti vahendusel seda isikut ka koolitama hakata, selle jaoks on võimalik edastada talle materjale ning muud olulist teavet, mida võiks näiteks mõne rünnaku korraldamiseks või mõne muu eesmärgi täideviimiseks vaja minna. Seda teist faasi saab pidada koolitamise faasiks. Ehk sellise näite põhjal on näha, et internet on loonud terroristlikele ühendustele võimaluse uute liikmete värbamiseks ning välja koolitamiseks. Lisaks on tehnoloogia areng loonud ühiskonnale uusi võimalusi ka raha ülekandmisel, mida terroristlikud rühmitused enda kasuks on pööranud (üheks näiteks on Paypal). Virtuaalsete valuutade ning mobiilse sularaha kaudu on terroristlikel rühmitustel võimalik teha koheseid ja anonüümseid ülekandeid, mille abil finantseerida enda rühmitust.

---

[48] The NYU Dispatch. Is technology helping or hindering the fight against terrorism? (15.12.2017) – The NYU Dispatch. Arvutivõrgus: https://wp.nyu.edu/dispatch/2017/12/15/is-technology-helping-or-hindering-the-fight-against-terrorism/ (14.03.2020)

[49] Weimann, lk 6

Ajavahemikul 8.03-08.06.2018 tehti CEP-i[50] poolt Youtube'i kohta uuring, kus otsiti ISIS-e sisuga videoid Youtube'i keskkonnas. Uuringuga leiti Youtube keskkonnast 1348 ISIS-e videot, mis said kokku 163 391 vaatamist. Uuringu eesmärgiks oli selgeks teha, kuivõrd kiiresti suutis Youtube videod avastada ning eemaldada. Kauem kui kaks tundi läks 322 video leidmiseks, kokku said need videod 148 590 vaatamist. Ülejäänud videod avastati kiiremini kui kahe tunniga, saades selle ajaga kokku 14 801 vaatamist. Kuigi suurem osa videoid avastati kiiresti ning eemaldati platvormilt, koorus selle uuringuga välja järgmine probleem, kuna 91% kõigist nendest videotest laeti üles mitu korda mõne teise kasutaja alt.[51] See tekitab küsimuse, kas Youtube segamissüsteemid töötavad ikka nõuetekohaselt, mis välistaksid teadaolevate terroristide videote taaskasutamist mõne teise kasutaja alt.

Uuringuga tehti kindlaks, et videote üles laadimiseks kasutati 278 erinevat kasutajat ning enamik nendest kasutajatest laadis üles mitu video. 60% kontodest jäid Youtube keskkonda alles, kustutati ära küll nende poolt üles laetud videod, kuid kontosid ära ei kustutatud. CEP-i poolt tehti mitmeid järeldusi, mis seavad kahtluse alla Youtube'i väited provokatiivse sisu eemaldamise kohta. Üheks järelduseks oli, et Youtube'is üleval olevate videote inimeste märgistamise jõupingutused ei ole praegu piisavalt heal tasemel terroristliku sisu järjepidevaks leidmiseks ja eemaldamiseks, mida ilmestab asjaolu, et 24% videotest jäi Youtube üles kauemaks kui 2 tundi. Teiseks jõudis CEP järeldusele, et Youtube pole suutnud oma sisu moderaatoreid teadaolevate ISIS-e videote kohta ette valmistada ning koolitada. CEP-i uuringu kohaselt peetakse ebatõenäoliseks, et Youtube ning Google kasutaksid asjakohast tehnoloogiat, kuna teadaolevad terroristliku sisuga videoid oli võimalik uuesti üles laadida. Uuringu raames toodi välja ISIS-e poolt üles laaditud video Hunt Them O'Monotheist. See oli algselt ISIS-e Somaalia partnerite poolt välja antud juba 25.detsember 2017. Video soodustab tulirelvi ning sõidukitega sooritatud rünnakuid lääneriikides. See video laaditi Youtube'i 10.märtsil 2018 ning oli saadaval 29 tundi. Enne video eemaldamist sai video 405 vaatamist. Seda videot pandi üles veel vähemalt 10 korda ning kokku sai see video natukene alla 1000 vaatamise.[52]

---

[50] Counter Extremism Project

[51] Counter Extremism Project, The Eglyho Web Crawler: ISIS Content on Youtube, 2018, lk 6 – Arvutivõrgus: https://www.counterextremism.com/sites/default/files/eGLYPH_web_crawler_white_paper_July_2018.pdf (15.03.2020)

[52] Samas, lk 6-8

See ilmestab praeguse aja olukorda, et terroristlikud rühmitused kasutavad aktiivselt samu portaale, mida kõik teised tavakasutajad. Youtube'i keskkonda laetakse üles ühes päevas tuhandeid erinevate sisuga videoid. See uuring näitab, kuivõrd aktiivselt kasutavad terroristid Youtube. Üheks peamiseks põhjuseks võib pidada seda, et Youtube'il on väga suur kasutajate arv ehk terroristliku sisuga videotel võiks olla potentsiaalselt suur publik.

Youtube kohta oleks ebaõiglane öelda, et Youtube ei ole midagi teinud selleks, et peatada terroristlike sisuga materjalide jõudmist enda keskkonda. Youtube on rangelt ära keelanud sisu, mis on mõeldud terroristlike organisatsioonide värbamiseks, vägivalla õhutamiseks, terrorirünnakute tähistamiseks või muul viisil terroriaktide edendamiseks. Platvorm lubab siiski üles laadida sisu, mis on mõeldud terroriaktidega seotud sündmuste dokumenteerimiseks või terroristliku tegevuse kohta uudiste edastamiseks, kuid sellekski on vajalik piisav kontekst ning kavatsus ja üldjuhul kehtib selliste videote osas vanusepiirangud ning hoiatused. Youtube'is on võimalik kasutajatel võimalik teada anda reeglite vastastest videotest. Lisaks on kasutusel ka erinevaid automatiseerituid lahendusi, mis avastaksid terroristlikku sisu. Kuid vaatamata Youtube poolsetele pingutustele teha võimalikult keeruliseks terroristliku sisu jõudmist nende platvormile, siis on terroristlikud rühmitused on leidnud erinevaid viise, kuidas kõrvale hiilida Youtube'i poolsetest piirangutest. Üheks näiteks on viis, mille kaudu edastatakse videoid ainult lingi kaudu. See tähendab seda, et selliseid videoid ei ole võimalik otsida, juurdepääsu saab ainult konkreetselt lingi abil. Lisaks sellele kasutavad terroristid viisi, kus lisatakse üles video, kus on ainult pilt ning mängib mingisugune heli, millega edastakse sõnumeid.

Terroristlikud rühmitused laevad üles ka videoid, mis pole konkreetselt terroristliku sisuga, vaid näiteks video kirjelduse osas on erinevad lingid, millele klikkides satutakse lehtedele, kus on terroristliku sisuga postitused ning materjalid. Probleemne on ka Youtube kommentaarium, kuhu lisatakse samuti erinevaid linke, mis suunavad edasi terroristliku sisuga saitidele.[53] Keeruliseks teeb veel olukorra see, et terroristlikud rühmitused kasutavad üleslaaditavaid skripte nagu Rapidleech, mis võimaldab samaaegselt laadida sisu mitmesse teenusesse. Seega selle programmi kaudu on võimalik laadida üles materjali nii Youtube'i kui ka muudesse portaalidesse. Seda protsessi on võimalik korduvalt iga uue

[53] Katz, R. How Terrorists Slip Beheading Videos Past YouTube's Censors. – Arvutivõrgus: https://motherboard.vice.com/en_us/article/xyepmw/how-terrorists-slip-beheading-videos-past-youtubes-censors (14.04.2020).

sisu jaoks korrata.[54] Oluline on välja tuua ka see, et suured platvormid nagu Youtube, Facebook, Instagram ei suuda kogu aeg kõiki platvormile üles pandud teavet võimalikult kiiresti läbi sõeluda. Näiteks Youtube kasutab üle miljardi kasutaja, sinna laetakse iga minutiga suurel hulgal videoid, lisaks veel postitakse erinevaid kommentaare. Seetõttu on ääretult keeruline ainult Youtube platvormil endal kõik võimalikud terroristliku sisuga videod või kommentaarid avastada ning eemaldada.[55]

Uus-Meremaal 15.03.2019 korraldanud mošeerünnaku meesterahvas tõi välja ühe radikaliseerumise põhjusena Prantsuse paremäärmuslaste liidri Marine Le Peni lüüasaamise presidendi valmistel. Rünnaku eest vastutuse võtnud Austraalia kodanik avaldas 74-leheküljelise immigrantidevastase manifesti, milles ütles, et on 28-aastane valgenahaline austraallane, kes tuli Uus-Meremaale vaid rünnakut kavandama ja selleks harjutama. Kirjutises selgitas mees, et pidas rünnakut terroriaktiks. [56] Lisaks sellele filmis rünnakut ning postitas sotsiaalmeediasse selle otseülekandena ülesse.

Suureks väljakutseks Euroopa julgeolekuasutustele, sh Kaitsepolitseiametile on üksikud, äärmusideoloogiate mõjul teistele märkamatult radikaliseerunud isikud. Terroriorganisatsioonide eesmärk on läbi propaganda, ilma konkreetsete juhiste ja otsekontaktideta taoliste isikute mõjutamine terrorikuritegude toimepanemisele.[57]

1.3. Terrorismivastane võitlus

Riiklike ametiasutuste üheks peamiseks ülesandeks on eelkõige enda elanikkonna ja kriitilise tähtsusega infrastruktuuride kaitsmine, seda nii terrori- ja massihävitusrelvade rünnaku eest kui ka looduskatastroofide vastu. NATO[58] ülesandeks on riike aidata, toimides mingil määral justkui foorumina, kus arendatakse mittesiduvaid nõuandeid ja

[54] Samas

[55] Cohen-Almagor, R. The Role of Internet Intermediaries in Tackling Terrorism Online. – Fordham Law Review 86, no. 2, November 2017, lk 432

[56] Postimees. Mošeeründaja: radikaliseerusin pärast Marine Le Peni lüüasaamist (15.03.2019. – Postimees. Arvutivõrgus: https://www.postimees.ee/6545788/moseerundaja-radikaliseerusin-parast-marine-le-peni-luuasaamist (20.03.2020).

[57] Eesti Kaitsepolitseiamet. Olukord Eestis – Arvutivõrgus: https://www.kapo.ee/et/content/olukord-eestis-1.html (27.02.2020).

[58] North Atlantic Treaty Organization

standardeid ning jagada parimaid võimalikke tegevusi ja õpetusi, kuidas parandada rahvusvahelist julgeoleku olukorda. Näiteks on NATO välja töötanud juhise esmaseks tegevuseks massihävitusrelvade rünnaku puhuks ning korraldab rahvusvahelisi õppusi massihävitusrelvade rünnaku esmareageerijatele.[59] Loomulikult on NATO ülesandeks ka reageerimine erinevate sõjaliste tegevuste puhul, kuid niivõrd suur organisatsioon peab tegelema ka terrorismiga, mis samamoodi õõnestab julgeolekut ning põhilisi demokraatlike väärtuseid. Seetõttu on oluline, et NATO-sugune organisatsioon jagab erinevaid nõuandeid ja juhiseid teatud juhtudeks, mis on seotud terrorismiga. Selline olukord aitab kaasa ka rahvusvahelisele koostööle riikide vahel, kuna läbi organisatsiooni on võimalik jagada nii teadmiseid, kogemusi, luureandmeid kui ka vahendeid, kuidas terrorismi vastu võidelda.

Lisaks rahvusvahelisele koostööle erinevate teadmiste või andmete jagamisele toimub ka aktiivne võitlus Lähis-Idas terroristlike rühmitustele kuuluvatele aladel. Selle eesmärgiks on terroristide alad vallutada ning seeläbi nende rühmituste eksistentsi vähendada või täielikult ära likvideerida.

Kuigi aktiivne võitlus terroristlike rühmituste aladel on kandnud vilja, sest paljude alade üle pole enam terroristlikel rühmitustel võimu ega kontrolli, siis on samaaegselt vajalik tegeleda ka aktiivse võitlusega internetis, et takistada terroristlike rühmituste suhtlemist, värbamist ning treenimist. Selliste ülesannetega tegeleb üle maailma mitmeid erinevaid organisatsioonid ning küberjulgeoleku teenused, eesmärgiga avastada ja eemaldada internetist terroristliku sisuga materjali. Üheks näiteks on Ühendkuningriigi CTIRU[60], mis eemaldas 2016. aastal üle 3500 äärmusliku sisuga materjali internetist. Nende materjalide hulgas oli erinevaid propagandafilme ja- videoid, terroriaktide läbiviimise käsiraamatuid ning väljaandeid, mis toetasid terrorismi ja ekstremismi. Viimastel aastatel on kümneid terrorirünnakuid terrorismivastaste asutuste poolt takistatud ning seda just kahtlaste tegevuste tõttu internetis. Sellisteks avastuseks on kasutatud erinevaid jälgimiseks mõeldud lahendusi, kuid suurem osa nendest lahendustest on riiklikult salastatud. Ühe näitena saab välja tuua veel USA riikliku julgeolekuameti, kes andis 2013. aastal teada, et kaks nende internetiandmeid ja telefonikõnesid jälgivat programmi on takistanud üle 50 võimaliku terrorirünnaku. Terrorismivastases võitluses on kasutuses ka niinimetatud superarvutid,

[59] North Atlantic Treaty Organization. Countering terrorism – Arvutivõrgus: https://www.nato.int/cps/en/natohq/topics_77646.htm

[60] CTIRU on lühend Ühendkuningriigi üksusest Counter-Terrorism Internet Referral Unit, mis tegeleb terroristliku veebisisu eemaldamisega.

mida kasutatakse üldiselt massiliste andmemahtude kogumiseks ja analüüsimiseks. Sellised võimalused aitavad kaasa avastada erinevate inimeste ja sündmuste vahelisi reisimustreid ja –linke, mille abil oleks võimalik ühendada terroristliku tegevuse ja varasemalt teada olevate isikute liikumised.[61] Seega kokkuvõtvalt kasutatakse terrorismivastases võitluses palju erinevaid tehnoloogilisi lahendusi. Tehnoloogia areng aitab kaasa luua järjest paremaid lahendusi ning võimalusi terrorismivastaseks võitluseks.

Eesti Välisluureameti hinnangul mõjutab 2019. aastal nõrgenenud ja territooriumist ilma jäänud ISIS endiselt Euroopa julgeolekut. Kuigi Euroopa õiguskaitse organite ja julgeolekuteenistuste süstemaatilise töö tulemusena on muutunud ISIS-il terrorirünnakute korraldamine Euroopas väga keeruliseks, on siiski suuremates Euroopa riikides jätkuvalt terroriohu tase kõrge, kuna nendes riikides on palju potentsiaalselt ohtlike radikaale. Näiteks Suurbritannias ja Prantsusmaal on terroriohu allikaks peetavate radikaliseerunud isikute nimekirjas üle 20 000 inimese.[62] Europoli andmetel on viimaste aastate jooksul terrorikuritegudes kahtlustatud vahistatute arv kahekordistanud. Kui aastail 2012-2017 oli 2880 vahistatut, siis 2006-2011 1056 vahistatut.

Terroristlikud rühmitused kasutavad värbamisel, radikaliseerumisel, planeerimisel ja rahastamisel sotsiaalmeediat. Interpol analüüsis ühises projektis ÜRO terrorismivastase võitluskeskusega (UNCCT) sotsiaalmeedia platvormide terroristlikel eesmärkidel kasutamist. Selle uuringuga sooviti koguda luureinformatsiooni terrorirühmituste tegevuste kohta sotsiaalmeedia platvormidel. Interpol korraldab enda uurijatele regulaarselt seminare, mis hõlmavad nelja peamist valdkonda:

- terroristidega seotud tegevuste avastamine Internetis;
- e-tõendite kogumine;
- e-tõendite taotlemine piiriüleselt;
- erasektoriga suheldes õiguskaitseasutuste juurdluste edendamiseks.

Seminaride eesmärk on ka suurendada osalejate arusaamist välismaa terroristide võitlejate nähtusest, näiteks soolistest stereotüüpidest ja naiste suurenevast kaasamisest terroristlikesse tegevustesse. Näotuvastustehnoloogiat saab kasutada ka sotsiaalmeedias.

---

[61] The NYU Dispatch, Is technology helping or hindering the fight against terrorism? https://wp.nyu.edu/dispatch/2017/12/15/is-technology-helping-or-hindering-the-fight-against-terrorism/ (14.11.2019)

[62] Välisluureamet. Eesti rahvusvahelises julgeolekukeskkonnas 2019. (Tallinn: Välisluureamet 2019), lk 63 – Arvutivõrgus: https://www.valisluureamet.ee/pdf/raport-2019-EST-web.pdf (14.04.2020)

See pakub uusi võimalusi andmete jagamiseks ja võrdlemiseks, et tuvastada terroriste, huvitute tundmatuid isikuid ja teemasid, mis võivad esineda sotsiaalmeedia kanalite ametikohtadel. Üks viis, kuidas saab toetada terrorismivastast uurimist, on sotsiaalmeedia platvormide otsimine võimalike tunnistajate tuvastamiseks. Seda on tehtud Ühendkuningriigis pärast 2017. aastal toimunud Londoni rünnakut ja Keenias 2019.aasta jaanuaris pärast Nairobis toimunud rünnakut.[63]

Sellega seoses tekib küsimus, et kas tehnoloogia areng aitab ka terrorismiga võitlemisel? Järjest rohkem ilmub mõnes Eesti ajalehes uus uudis[64] selle kohta, kuidas pommitati mõnda territooriumi, kus on näiteks terroristliku rühmituse ISIS peamised alad. Relvastuse seisukohalt on sellise aktiivse võitluse osas muutunud paremaks. Kuid oluline töö tehakse ära ka enne seda, kui läheb reaalseks ründamiseks või pommitamiseks. Tänapäeval kasutatav tehnika võimaldab pealt kuulata telefonikõnesid, positsioneerida telefonide abil kasutajate asukohtasid. Paremaks on muutunud erinevad jälituseks kasutatavad tehnikad, mille abil on võimalik pealt kuulata või varjatult kuskile territooriumidele siseneda. Üheks märksõnaks on ka droonide kasutuselevõtt, mis võimaldab drooni abil saada kiirelt ja inimeste jaoks ohutult vajalikku informatsiooni mõnest piirkonnast, kus tegutseb konkreetne terroristlik rühmitus, mille osas on aktiivne võitlus. Tehnoloogia võimaldab ametivõimudel omada suuremat ja paremat ülevaadet inimeste andmete osas. Loodud on näiteks tulirelvade avastamise süsteemid. Linnakaamerad ja turvakaamerad tänavatel on täiesti tavaliseks nähtuseks ning paljudes linnades on võimalik ka reaalajas jälgida linnas toimuvat. See tõstab tõenäosust, et võimalik kuritegu avastatakse enne selle toimepanemist. Seega on tehnoloogia areng loonud väga palju erinevaid viise terrorismiga võitlemiseks, kuid sellel on ka negatiivne külg, kuna ka terroristlikud rühmitused kasutavad tehnoloogiat enda eesmärkide saavutamiseks ära.

NATO üheks eesmärgiks on arendada uusi tipptasemel tehnoloogiad, mis oleksid abiks terrorirünnakute takistamiseks. Selleks on loodud organisatsioon DAT POW[65], mille peamine eesmärk on leida tehnoloogilisi lahendusi terrorirünnakute mõjude leevendamiseks. Ajaga on selle organisatsiooni valdkond laienenud, kuna organisatsiooni

---

[63] Interpol. Analysing social media. – Interpol. Arvutivõrgus: https://www.interpol.int/Crimes/Terrorism/Analysing-social-media(20.03.2020)

[64] Postimees. Süürias andsid alla tunnelitest välja ilmunud džihadistid (24.03.2019). – Postimees. Arvutivõrgus: https://www.postimees.ee/6552732/suurias-andsid-alla-tunnelitest-valja-ilmunud-dzihadistid (20.03.2020).

[65] Defence Against Terrorism Programme Of Work

tegevus hõlmab endas ka harjutuste, katsete, prototüüpide ja mõistete väljatöötamist. Enamik programmi raames läbiviidavatest projektidest keskendub lahendustele, mis vastavad NATO sõjalistele vajadustele.[66]

Kuna tehnoloogia pakub terroristlikele rühmitustele uusi võimalusi ka relvastuses, on NATO kõrgeim prioriteet tõkestada massihävitusrelvade levikut ning NATO liitlaste elanikkonna ohutuse ja julgeoleku tagamine keemiliste, bioloogiliste, radioloogiliste ja tuumaohtude ees. NATO on selleks loonud eraldi üksuse Joint CBRN Defence Task Force, mille ülesandeks on reageerida ja juhtida keemiliste, bioloogiliste, radioloogiliste tuumarelvade kasutamise tagajärgi nii NATO vastutusalas kui ka väljaspool seda.[67]

[66] North Atlantic Treaty Organization. Defence Against Terrorism Programme of Work. – Arvutivõrgus: https://www.nato.int/cps/en/natohq/topics_50313.htm (15.02.2020)

[67] North Atlantic Treaty Organization. Combined Joint Chemical, Biological, Radiological and Nuclear Defence Task Force. – Arvutivõrgus: https://www.nato.int/cps/en/natohq/topics_49156.htm (15.02.2020)

2. Euroopa Liidu ja liikmesriikide terrorismivastane võitlus

2.1. Euroopa Liit

2.1.1. Euroopa Liidu strateegia

Euroopa Nõukogu võttis 2005. aastal vastu Euroopa Liidu terrorismivastase strateegia. Selle eesmärgiks on võidelda terrorismiga ning seeläbi muuta Euroopa turvalisemaks. Strateegia põhineb neljal sambal:

1) ennetamine
2) kaitse
3) jälitamine
4) reageerimine.[68]

Seda strateegiat muudeti 2014. aasta juunis, kuna terrorismi olemus on aastate jooksul muutunud ning strateegia puhul on vajalik pidada silmas terrorismi uusi suundumusi. 2014. aasta muudetud strateegias on välja toodud üksi tegutsevad terroristid, välisvõitlejad ja sotsiaalmeedia kasutamine. Samal aastal võeti Euroopa Nõukogu poolt vastu ka suunised muudetud strateegia kohta Euroopa Liidu liikmesriikides. [69] Strateegia üldised põhimõtted on samad, kuid on lisatud mõned uuemad aspektid, mis terrorismi arenguga on kaasnenud ning mida tuleb terrorismivastases võitluses silmas pidada.

04.07.2018 võeti vastu Euroopa Nõukogu poolt terrorismivastase võitluse strateegia aastateks 2018-2022, milles toodi välja kolm põhilist valdkonda, millega terrorismivastases võitluses tegeleda tuleb. Nendeks valdkondadeks on ennetamine, jälitamine ja kaitsmine. Kõigi valdkondade all on välja toodud põhilised punktid, kuidas terrorismi vastu võidelda või seda ennetada. Iga punkti juures toodi omakorda välja üldiselt põhilised tegevused, millega konkreetse punkti all tegeletakse. Lisaks kirjutati välja kõikvõimalikud põhjused, miks selle punktiga tegeleda tuleb, töömeetodid ja vastutavad organisatsioonid.

[68] European Union: Council of the European Union. The European Union Counter-Terrorism Strategy. 30.11.2005. – 14469/4/05 REV 4, lk 6

[69] Euroopa Ülemkogu, Euroopa Liidu Nõukogu. ELi terrorismivastane võitlus. – Arvutivõrgus: https://www.consilium.europa.eu/et/policies/fight-against-terrorism/ (10.04.2020)

Punktipõhiliselt on välja toodud ka soovitud tulemused, mida konkreetsete tegevustega soovitakse saavutada.[70]

Kuigi 2005. aastal vastu võetud Euroopa Liidu terrorismivastase võitluse strateegiat on ajaga muudetud, siis tulevad üldised põhimõtted sellest strateegiast. Euroopa Liidu terrorismivastane strateegia põhineb neljal samblal. Esimene sammas on ennetamine, mille põhiline eesmärk on küll võidelda radikaliseerumise ja terroristide värbamise vastu, kuid sellele lisanduvad ka suurem ning mitmekülgsem kontroll tulirelvade kohta Euroopas. Ennetamine võimaldab ära hoida suuri terrorirünnakuid, mille tagajärjel võivad inimesed hukkuda või vigastada saada. Seetõttu on selle samba all pööratud tähelepanu teabevahetuse osas erinevate riikide ja organisatsioonide vahel, kuid muuhulgas ka tõhusam koostöö kolmandate riikidega, lisaks veel terroriaktide käsitamine kuritegudena ning tugevdatud kontroll välispiiridel.[71]

Käesoleva magistritöö esimeses peatükis on välja toodud erinevad funktsioonid, kuidas terroristlikud rühmitused internetti enda eesmärkide täitmiseks kasutavad. Seetõttu on Euroopa Liit hakanud järjest suuremat tähelepanu pöörama internetis toimuvale radikaliseerumisele, kuna selle tulemusena leiavad terroristlikud rühmitused endale uusi liikmeid, keda välja koolitada ning juhendada rühmituse eesmärkide täitmiseks. Kuna terroristlikul eesmärgil interneti kasutamise tõkestamine on suuresti seotud ennetamisega, siis on Euroopa Liidu terrorismivastase strateegia muudatustega täiendatud seda teemat puudutavaid valdkondi.

Euroopa Liidu terrorismivastase strateegia teine sammas hõlmab endas peamiselt kodanike ning taristu kaitsmist. Selle valdkonna alla kuuluvad erinevate välispiiride kontroll ning kindlustamine, lisaks veel transpordi turvalisus. Kuna terrorirünnakute üks põhilisi eesmärke on tekitada ühiskonnas hirmu ning takistada lääneühiskonna toimimist, siis on Euroopa Liit enda strateegias välja toonud ka kindlad strateegilised piirkonnad või kohad, mille osas tuleb kohaldada suuremat kaitset.[72]

Strateegia kolmandaks sambaks on jälitamine, mis keskendub peamiselt terroristide võimekuse takistamisel. Selle samba eesmärgiks on olla võimalikult detailselt kursis

[70] Council of Europe: Ministers'Deputies. Counter-Terrorism Strategy (2018-2022). 04.07.2018. – CM (2018)86

[71] The European Union Counter-Terrorism Strategy, lk 7-8

[72] Samas, lk 10

erinevate terrorirühmituste, sinna hulka kuuluvate isikute ning nende rühmituste eesmärkidega. Selle saavutamiseks aitab Euroopa Liit suurendada riikide suutlikkust ning võimekust informatsiooni kogumiseks terrorirühmituste kohta. Strateegia kolmanda samba üheks eesmärgiks ning märksõnaks võib pidada koostööd, mille all mõeldakse põhiliselt erinevate õiguskaitseorganite omavahelist koostööd. Nii riigid kui ka erinevad organisatsioonid jagavad enda luureandmeid ja oskusi ning ka vahendeid, et tagada võimalikult efektiivne võitlus terrorismi vastu. Jälitamise kui strateegia ühe samba väga oluliseks valdkonnaks on ka terrorismi rahastamise tõkestamine ning terroristide ilmajätmine toetus- ja suhtlemisvahenditest.[73]

Euroopa Liidu terrorismivastase strateegia viimane ehk neljas sammas käsitleb endas valmisolekut terrorirünnakutega toimetulemiseks. Selle samba põhiline ülesanne on minimeerida rünnaku tagajärgi ning seda ohjata. See tähendab seda, et kui kuskil Euroopa Liidu liikmesriigi territooriumil toimub terrorirünnak, siis on kõik liikmesriigid üheselt valmis rünnaku tagajärgedega tegelemiseks.[74]

Euroopa Liidu terrorismivastase võitluse nelja samba hulgast ei saa välja tuua ühte kõige olulisemat ning terrorismivastase võitluse seisukohalt on oluline, et iga samba kõik funktsioonid ja eesmärgid oleksid omavahel kooskõlas ning toimiksid. Kuid terrorismivastases võitluses ei saa siiski lootma jääda ainult Euroopa Liidule ning Euroopa Liidu organisatsioonidele. Euroopa Liidu poolt tulevad küll üldised tõekspidamised terrorismiga võitlemisel ning regulatsioonid, kuid siiski põhiline töö jääb liikmesriikide ning nende õiguskaitseorganite teha. Euroopa Liit on terrorismivastases võitluses rohkem toetavas rollis, kuna liidu eesmärgiks on luua ühendusesiseselt ühtne õigusraamistik ning tagada riikidevaheline koostöö. Kuna terrorism on muutunud piiriüleseks, siis põhiline rõhk sellega võitlemisel on koostööl.

2016. aasta jaanuaris loodi Euroopa terrorismivastase võitluse keskus (ECTC[75]), mis keskendub operatiivtoe pakkumisele liikmesriikidele. Keskus võimaldab Euroopa Liidu liikmesriikidel parandada teabevahetust ja teha rohkem operatiivkoostööd terroristidest välisvõitlejate seire ja uurimise osas, jagada luureandmeid ja kogemusi. Selle keskuse kaasabil on võimalik liikmesriikidel saada parem ning suuremat territooriumi hõlmav

[73] Samas, lk 11

[74] Samas, lk 15

[75] European Counter Terrorism Centre

informatsioon ebaseaduslike tulirelvadega kauplemise ning terrorismi rahastamise alal. Euroopa terrorismivastase võitluse keskuse kaudu on võimalik parandada ning efektiivsemaks muuta terroristide interneti propaganda ja äärmusluse jälgimine.[76]

Selleks, et internetis toimuva radikaliseerumise vastu tõhusamalt võidelda, loodi 2015. aasta juunis Euroopa Liidu internetisisust teavitamise üksus EU IRU.[77] Selle üksuse üks peamiseid eesmärke on jälgida internetisisu. Üksuse ülesanded on kooskõlas Europoli strateegiliste eesmärkidega.[78] Näiteks on üksuse üheks ülesandeks terroristide interneti radikaliseerumise ja värbamispüüdluste vastu tõhus võitlemine. Selle jaoks on vajalik kõigepealt kaardistada terroristide propagandavõrgud ehk selgeks teha, milliseid kanaleid ja platvorme internetis terroristlikud rühmitused kasutavad. Oluline on ka tugevdada kohanemisvõimet ning mõjutada terroristide propagandavõrke. Terrorismivastase võitluse üksuse üheks ülesandeks on veel internetipõhise uurimisabi võimekuse loomine ning arendamine. Selle ülesande täitmiseks on vajalik kõigepealt strateegiline analüüs ehk aru saada, millised meetmed on kõige efektiivsemad internetis leiduva terroristliku sisuga materjalide levitamise tõkestamiseks.[79]

EU IRU üksuse eesmärk on võimalik efektiivne võitlus internetis leiduva terroristliku sisuga võitlemisel. Seetõttu korraldab üksus Euroopa Liidu liikmesriikide õiguskaitseorganite esindajatele koolitusi, mille eesmärgiks on parandada terrorismivastase võitluse efektiivsust internetis. Näiteks toimus 14-15.03.2018 koolitus, kus osalesid Belgia, Prantsusmaa, Madalmaade, Sloveenia ja Ühendkuningriigi riiklike üksuste esindajad. Koolituse raames vaadeldi internetiportaali www.wordpress.com, et tuvastada seal paiknev terroristlik sisu. Kokku tuvastati üle 900 terroristliku propagandaga seotud materjali või sisu. Pärast terroristliku sisu tuvastamist võeti ühendust internetiportaali moderaatoridega, et nende kaasabil terroristliku sisuga materjalid lõplikult ära kustutataks. Pärast praktilist poolt andsid õiguskaitseüksused hinnangud avastatud sisule ning analüüsiti leitud materjale. Selle koolitusega oli võimalik välja selgitada peamised meetodid, mida

---

[76] Europol. European Counter Terrorism Centre. – Arvutivõrgus: https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc (30.03.2020)

[77] European Union Internet Referral Unit

[78] Europol. Europol's internet referral unit to combat terrorist and violent extremist propaganda. – Arvutivõrgus: https://www.europol.europa.eu/newsroom/news/europol%E2%80%99s-internet-referral-unit-to-combat-terrorist-and-violent-extremist-propaganda (30.03.2020)

[79] Europol: EU Internet Referral Unit. Year one report – highlights, lk 4 – Arvutivõrgus: https://www.europol.europa.eu/publications-documents/eu-internet-referral-unit-year-one-report-highlights (20.04.2020)

terroristlikud rühmitused internetis kasutavad. Koolituse käigus avastatud terroristliku materjalid olid peamiselt üles pandud ISIS-e või al-Qaeda poolt. Leitud materjalide hulgas oli propagandavideoid, veebilehti, mis austasid või toetasid terrorismi ja ekstremismi. Nii liikmesriikide õiguskaitseorganid kui ka EU IRU teevad internetiplatvormidega koostööd, et tuvastatud terroristliku sisuga materjal lõplikult eemaldatakse ning piirata sellise sisuga materjalide kättesaadavust internetis. Koolitusel tõstatus üks probleem, kuna internetiplatvormide tegevus terroristliku sisuga materjalide eemaldamisel on vabatahtlik ning tuleb võtta arvesse portaali reegleid ja kasutustingimusi.[80] Sellise sisuga materjali eemaldamine ei tohiks olla platvormidele vabatahtlik otsustamise koht, vaid peaks olema kohustus koheselt sellise sisuga materjalid enda platvormilt eemaldama. Kuna internetti kasutatakse terroristlike rühmituste poolt järjest rohkem, siis on oluline, et kõik platvormid, mis on kättesaadavad Euroopa Liidu liikmesriikides, oleksid kohustatud tegema täielikku koostööd nii Euroopa Liidu enda kui ka liikmesriikide üksustega, et viia internetis leiduva terroristliku sisuga materjalide hulk võimalikult minimaalseks.

Euroopa Liit on kokku kogumas kõik võimalikku praktika, kuidas ennetada ja võidelda terrorismiga internetis, kuidas samas on Euroopa Liidu jaoks oluline võitluses säilitada ka inimõigused ning põhivabadused, õigusriigi põhimõtted ning demokraatia.[81] Euroopa Liidu jaoks on oluline välja töötada terviklik ülevaade vahenditest ja meetoditest, mida liikmesriigid kasutavad terroristide internetiteenuste kuritarvitamise vastu võitlemiseks. Samuti on vajalik edendada meedia- ja interneti-teenuse pakkujate ja teiste asjaomaste osalejate vastutustundlikku käitumist, et nad ei lubaks terrorismi ja selle ideoloogia levikut enda platvormidel. Ennetava töö edasiarendamiseks on kasulik riikide kogemustel põhinevate parimate tavade kogumi koostamine. Kuna erasektoril, sealhulgas tehnoloogia- ja sotsiaalmeedia ettevõtted, on selles protsessis oluline roll toetab Euroopa Nõukogu mitmeid algatusi ja uurimisprogramme selles valdkonnas. 8. novembril 2017 allkirjastas Euroopa Nõukogu peasekretär Thorbjørn Jagland esialgsed partnerluslepingud - kirjavahetuse vormis - kümne juhtiva tehnoloogiaettevõtte ja kuue ühingu esindajatega. See partnerlus võimaldab ettevõtetel osaleda mitmetes Euroopa Nõukogu valitsustevahelistes tegevustes ja sellega seotud töös ning olla kaasatud internetipoliitika

[80] Europol. More than 900 instances of online terrorist propaganda uncovered. (16.03.2018). – Arvutivõrgus: https://www.europol.europa.eu/newsroom/news/more-900-instances-of-online-terrorist-propaganda-uncovered (02.04.2020)

[81] Council of Europe: Ministers'Deputies. Counter-Terrorism Strategy (2018-2022), p 1.2

kujundamisel koos valitsustega. Konkreetsed koostöövaldkonnad võivad hõlmata ka Interneti kasutamist terroristlikel eesmärkidel.[82]

2.1.2. Euroopa Liidu regulatsioon

Euroopa Liidu Nõukogu võttis 13.06.2002 vastu raamotsuse 2002/475/JSK terrorismivastase võitluse kohta[83], millega määrati terrorikuriteo koosseisu sisustamiseks teatud miinimumnõuded. Tegemist oli kõikidele liikmesriikidele ühise õigusliku raamistikuga terrorismi vastu ning see oli alustalaks kriminaalõiguslike vahenditega terrorismivastaseks reageerimiseks. Seetõttu pandi liikmesriikidele kohustus kriminaliseerida terrorikuriteod, terrorirühmituse juhtimine ning selles osalemine. Raamotsusega 2002/475/JSK kohustati liikmesriike kriminaliseerida lisaks eelnevale ka röövimine, väljapressimine ja dokumentide võltsimine terrorikuriteo toimepanemiseks ning samuti terrorikuriteole üleskutsumine, kihutamine ja kaasaitamine.

28.11.2008 muudeti raamotsusega 2008/919[84] varasemat raamotsust 2002/475/JSK terrorismivastase võitluse kohta. Varasema raamotsuse muutmiseks oli mitmeid põhjuseid. Üheks põhiliseks oli asjaolu, et terrorismioht oli viimaste aastate jooksul kiiresti kasvanud ning terroristide töömeetodite muutuste tõttu oli vajalik muuta terrorismivastast regulatsiooni. Raamotsuses 2008/919 mainiti ära ka asjaolu, et terroristid kasutavad internetti kohalike terrorismivõrgustike ja üksikisikute innustamiseks ning mobiliseerimiseks Euroopas. Lisaks toodi selles raamotsuses välja, et internet on allikaks terroristide vahendite ja meetodite kohta ning et internetis toimub terroristide virtuaalne väljaõppelaager. Seetõttu raamotsusega leiti, et õigusrikkumised, nagu avalik üleskutse panna toime terroriakte või värbamine terroristlike eesmärkidel peaksid olema kõikides liikmesriikides võrdselt karistatavad, sõltumata sellest, kas need pandi toime interneti teel või mitte.

15.03.2017 võttis Euroopa Parlament ja Nõukogu vastu direktiivi 2017/541 terrorismivastase võitluse kohta. Käesoleva direktiiviga asendati nõukogu raamotsus

---

[82] Samas

[83] Euroopa Liidu Nõukogu raamotsus 2002/475/JSK terrorismivastase võitluse kohta. – L 164/3, 13.06.2002.

[84] Euroopa Liidu Nõukogu raamotsus 2008/919/JSK, millega muudetakse raamotsust 2002/475/JSK terrorismivastase võitluse kohta. – L 330/21, 28.11.2008.

2002/475/JSK. Direktiivis on viidatud raamotsusele 2002/475/JSK kui kriminaalõiguslike vahenditega reageerimise alustalana. See raamotsus on siiski kõikidele liikmesriikidele ühiseks õigusraamistikuks ning hilisemate otsustega on seda täiustatud ning ajaga kooskõlla viidud.

Direktiivi 2017/541 artikkel 1 kohaselt nähakse selle direktiiviga ette miinimumnormid, mis käsitlevad terroriaktide, terrorirühmituste ja terroristliku tegevuse vallas kuritegude määratlemist ja karistusi, ning meetmeid terrorismiohvritele kaitse ja toetuse ning abi andmiseks. Direktiivi II jaotis keskendub terroriakti määratlemisele ning on välja toodud terrorirühmitusega seotud kuriteod. III jaotises on terroristliku tegevusega seotud kuriteod. Selle alla kuuluvad avaliku üleskutse panna toime terroriakt, terroristide värbamine, terrorismialase väljaõppe andmine, terrorismialase väljaõppe saamine, terroristlikel eesmärkidel reisimine või sellise reisimise korraldamine või muul viisil hõlbustamine, terrorismi rahastamine ning terroristliku tegevusega seotud muud kuriteod.

Direktiiviga 2017/541 pöörati veel rohkem tähelepanu just terroristlikele tegevustele internetis. Direktiivi preambula punktis 22 on välja toodud, et tõhusaks vahendiks on eemaldada veebisisu, mis kujutab endas avalikku üleskutset panna toime terroriakt. Sama punktiga suunatakse Euroopa Liidu liikmesriike koostööle kolmandate riikidega, mille kaudu oleks võimalik eemaldada kolmandate riikide territooriumil asuvatest serveritest terroristlik veebisisu.

Euroopa Liidu direktiiv 2017/541 üheks põhiliseks valdkonnaks on reguleerida Euroopa Liidus ühtsemaks terroristliku veebisisuga tegelemine ja eemaldamine. Magistritöö alapeatükis 1.2. on kirjeldatud, kuidas terroristlikud rühmitused interneti kasutavad. Kuigi aktiivse võitluse tulemusena on terrorismivastases võitluses tehtud edusamme, toimub siiski interneti vahendusel radikaliseerumine Euroopa riikides. Võrreldes direktiivi 2017/541 varasemate raamotsustega, siis on näha, et direktiiviga antakse liikmesriikidele võimalusi meetmete kohaldamiseks, et tõkestada terroristliku veebisisu levimist.

Direktiivi 2017/541 artikkel 21 käsitleb meetmeid avaliku üleskutse vastu internetis panna toime terroriakt. Selle artikli kohaselt on liikmesriikidel vajalik võtta meetmed, mille kaudu on võimalik tagada nende territooriumil majutatava veebisisu viivitamatu kõrvaldamine internetist. Lisaks on samas artiklis välja toodud, et liikmesriigid püüaksid sellist veebisisu kõrvaldada, kui seda majutatakse väljaspool nende territooriumi. Artikli lõikes 2 on välja toodud, et kui veebisisu algallikat ei ole võimalik eemaldada, siis võivad

liikmesriigid võtta vastu meetmeid, et takistada nende territooriumi asuvate internetikasutajate juurdepääsu sellele veebisisule.

Direktiiv 2017/541 artikkel 7 kohaselt on kuriteoks terrorisimialase väljaõppe andmine. Töö esimeses peatükis on välja toodud, et terroristlikud rühmitused kasutavad internetti erinevate treeninglaagrite korraldamiseks ja koolitamiseks. Kuna väljaõpe peab toimuma terrorismiga seotud eesmärgi ja terroriakti toimepanemise kavatsusega, siis on vajalik sellise käitumise kriminaalvastutuse võtmiseks, et väljaõppe pakkuja oleks teadlik, et nende oskuste kaudu on võimalik toime panna terrorikuritegu.

Kuid selle direktiiviga on pööratud pilk terrorismialase väljaõppe saamisele (Euroopa Liidu direktiiv 2017/541, artikkel 8). Direktiivi preambula punktis 11 on kirjeldatud, et terrorismialase väljaõppe saamine hõlmab teadmiste, dokumentide ja praktiliste oskuste saamist. Lisaks loetakse selle hulka iseõppimist, sealhulgas interneti või muu õppematerjali vahendusel. Selleks peab koolitusest aktiivselt osa võtma, näiteks osalema interneti või muude elektrooniliste meediumite kaudu terroristlike ühenduste või rühmituste juhitavatel treeninglaagritel.[85]

Direktiivi 2017/541 preambula punkti 11 kohaselt ei saa pidada üksnes veebisaitide külastamist või materjalide kogumist õiguspärastel eesmärkidel terrorismialase väljaõppe saamiseks. Terroristide poolt väljaõppe saamisel terrorikuriteo toimepanemiseks võiks piisata üksnes terroristliku teavet sisaldavate veebisaitide külastamisest või sellise suhtluse vastuvõtmisest, mida saaks kasutada terrorismi väljaõppeks ning iseõppimiseks.[86] Seda teemat on täpsemalt analüüsitud käesoleva töö allolevates peatükkides.

Seega on direktiivi alusel võimalik liikmesriikidel tõkestada terroristliku veebisisu levimist ning vastutusele võtta terroristliku veebisisu levitajad, kuid käesolev direktiiv annab võimaluse liikmesriikidele tegeleda terroristliku veebisisu sihtrühmaga ehk inimestega, kes terroristliku veebisisu kaudu näiteks väljaõpet saavad.

Euroopa Liidu terrorismivastase võitluse strateegias on välja toodud punkt, mis käsitleb ennetamist ja terrorismiga võitlemist avaliku provokatsiooni, propaganda, radikaliseerumise, värbamise ja treenimise kohta internetis.[87] Kuna terroristlikud

[85] Paunovic, N. New EU Criminal Law Approach to Terrorist Offences. – EU and Comparative Law Issues and Challenges Series 2, no. 2 (2018), lk 537

[86] Samas

[87] Council of Europe: Ministers'Deputies. Counter-Terrorism Strategy (2018-2022), p 1.2

rühmitused on väga laialdaselt kasutamas ära interneti poolt pakutavaid võimalusi, et levitada enda ideoloogiat, värvata uusi liikmeid ning neid välja koolitada, siis on ääretult oluline, et Euroopa Liidu tasandil oleks paika pandud kindel strateegia ja eesmärgid, kuidas selle probleemiga peaks tegelema ja internetti muuta turvalisemaks ning ohutamaks.

Euroopa Liidus on loomisel õiguslik regulatsioon, mis konkreetselt põhineb terroristlikel eesmärkidel tegutsemisele internetis. Euroopa Parlamendi ja Nõukogu määrus 2018/0331 terroristliku veebisisu levitamise tõkestamise kohta on hetkel veel ettepaneku staadiumis ning läheb veel aega, et see määrus jõustuks. Määruse seletuskirjas on seletatud tausta, miks määrust vajalik oleks. Seletuskirja kohaselt on hiljutised Euroopa Liidu territooriumil toimunud terrorirünnakud näidanud, et terroristlikud rühmitused kasutavad internetti kuritahtlikult. Nende eesmärkideks on interneti kaudu õpetada välja ning värvata uusi toetajaid, lisaks veel valmistada ette ning hõlbustada terroritegevust. Terroristlikud rühmitused kasutavad internetti propaganda jaoks ning kasutavad seda ka ühiskonna hirmutamiseks. Kuna viimaste aastate jooksul on järjest rohkem tähelepanu pööratud just internetis toimuvale, siis on tõendatud, et ebaseaduslik veebisisu on kaasa aidanud üksikute isikute radikaliseerumisele ning ajendanud neid lausa terrorirünnakuid korraldama ning täide viima. Lisaks märgiti veel seletuskirjas ära, et ebaseaduslik veebisisu mõjutab negatiivselt kogu ühiskonda, terroristlik sisuga materjalide levik internetis vähendab usaldusväärsust ning seeläbi kahjustab ettevõtete mainet ning äritegevust.[88]

2.2. Euroopa Liidu liikmesriikide terrorismi vastase võitluse strateegiad ning regulatsioonid

Euroopa Liidu liikmesriikidel on suuresti sarnased vaated terrorismivastasel võitlusel. See väljendub sarnastes ülesehitustes riikide strateegiates, millest on täpsemalt juttu allpool. Euroopa Liidu direktiivide ülevõtmisest tulenevalt on käesolevas magistritöös vaadeldud liikmesriikide õigusaktid suuremas osas sarnased.

Magistritöös on valitud välja Suurbritannia, Saksamaa ning Prantsusmaa, kuna nendes riikides on toimunud suurem osa terrorirünnakuid ning statistika kohaselt on nendes

[88] Seletuskiri. Ettepanek: Euroopa Parlamendi ja Nõukogu määrus terroristliku veebisisu levitamise tõkestamise kohta. 12.09.2018. 2018/0331 (COD). p 1.1 – Arvutivõrgus: https://ec.europa.eu/transparency/regdoc/rep/1/2018/ET/COM-2018-640-F1-ET-MAIN-PART-1.PDF (15.03.2020)

riikides kõige rohkem toimunud terrorismiga seotud isikute arreteerimisi. Sellest tulenevalt võib eeldada, et nende riikide terrorismivastane võitlus on kõige aktiivsem ning seetõttu võib nende riikide õigusaktidest või strateegiatest leida punkte, mis oleksid abiks ka Eesti terrorismivastases võitluses. Lisaks nendele kolmele riigile on magistritöös vaadeldud eraldi alapeatüki all ühiselt ka Soome ning Rootsi terrorismi vastaseid strateegiaid ning õigusakte, kuna tegemist on riikidega, kus on tugev ja hästi organiseeritud heaoluühiskond.

2.2.1. Rootsi terrorismivastane strateegia ning regulatsioon

Rootsi terrorismivastane strateegia põhineb riigi võimete analüüsil, mille tulemusel toodi välja valdkonnad, mida on vaja täiustada Rootsi kaitsmiseks terrorismi eest. Kuigi selles strateegias on välja toodud mitmeid aspekte terrorismivastases võitluses, siis käesolevas magistritöös on keskendutud kohtadele, mis on seotud interneti kasutamisele terroristlikul eesmärgil. Rootsi strateegias on välja toodud, et internet ja sotsiaalmeedia on muutunud peamisteks vahenditeks terroristliku propaganda levitamisel, radikaliseerumisel ja värbamisel ning selline interneti kasutamine on muutunud globaalseks.[89]

Üheks esimeseks eelduseks probleemi lahendamisel on selle probleemi välja toomine. Kui riiklikus terrorismivastase strateegias on välja toodud asjaolu, et internetist tulenevad uued probleemid terrorismivastases võitluses, siis selle põhjal saab eeldada, et see on üks valdkondi, millega hakatakse üha rohkem tegelema.

Rootsi õiguskaitseorganid on samuti tuvastanud, et terroristlikul eesmärgil kasutatakse internetti radikaliseerumiseks ning uute liikmete värbamiseks, mis tõstab uute rünnakute toimumise tõenäosust. Lisaks on Rootsi õiguskaitseorganid täheldanud sotsiaalmeedias teatavaid märke selle kohta, et noorte seas on muutumas kahe terroristliku rühmituse al-Qaeda ja ISIS-e kasutatav retoorika normaalsuseks.[90] Sellised avastused näitavad ning kinnitavad, kuivõrd oluline on tegeleda internetis leiduva terroristliku sisuga materjalide tõkestamisega, et seeläbi vältida uute terrorirünnakute toimumist. Kuna internet on muutunud ääretult oluliseks osaks ühiskonna liikmete igapäevaelus, siis peavad riigid

[89] Sweden. Agreement on counter-terrorism measures. 07.06.2017 – Arvutivõrgus: https://www.government.se/49f005/contentassets/2f681fbd159d451795b744523a96f955/Agreement-on-anti-terrorism-measures.pdf (25.04.2020)

[90] Samas, lk 4

olema suutelised tagama, et internet oleks turvaline ning läbi selle ei ohustataks lääneriikide põhilisi ühiskondlikke alustalasid.

Kui vaadelda Rootsi terrorismivastase strateegiat üldisemalt, siis on üheks olulisemaks kriteeriumiks koostöö nii riigisiseste asutuste vahel kui ka teiste riikide ja organisatsioonidega. Terrorismivastases võitluses, mis keskendub internetis toimuva tõkestamiseks, on Rootsi meedianõukogu spetsiaalselt koostanud digitaalse õppematerjali, mille kaudu üritatakse suurendada inimeste võimet seada kahtluse alla antidemokraatlikke ja vägivaldsed sõnumid internetis ning sotsiaalmeedias. Rootsi meedianõukogu eestvedamisel on korraldatud erinevaid üritusi, mille eesmärgiks on kaitsta demokraatiat vägivaldse ekstremismi eest. Selle raames sooviti suurendada eelkõige noorte, kuid ka täiskasvanute meediateadlikkust, et inimesed suhtuksid kriitilisemalt internetis ning sotsiaalmeedias levivatesse sõnumitesse.[91]

Rootsi terrorismivastase strateegia kohaselt on kuritegevuse vastases võitluses kesksel kohal kriminaalõiguse asjakohane regulatsioonide raamistik.[92] Magistritöö esimeses peatükis on välja toodud, et terrorismi olemus on ajaga muutunud, mistõttu on regulatsioonide asjakohasus olulise tähtsusega terrorismivastases võitluses. Seega tuleb lisaks riiklikule terrorismivastasele strateegiale analüüsida ka terrorismi puudutavaid regulatsioonide.

Rootsi karistusseadustikus (rootsi keeles Brottsbalken, inglise keeles The Swedish Criminal Code, SFS 1962:700)[93] välja toodud terrorismi puudutavad paragrahvid viitavad edasi terroriaktide kriminaalvastutuse seadusele (rootsi keeles Lag om straff för terroristbrott, inglise keeles Act on Criminal Responsibility for Terrorist Offencese, SFS 2003:148)[94], kus on teises paragrahvis välja toodud terroristi ja terroriakti mõiste. Terroriaktide kriminaalvastutuse seaduse kohaselt on terroristiks isik, kes paneb toime paragrahvis 3 nimetatud teo ning mõistetakse terroriakti eest süüdi, kui see tegu võib tõsiselt kahjustada riiki või valitsustevahelist organisatsiooni. Lisaks on selle punkti all

[91] Samas, lk 10

[92] Samas

[93] Brottsbalken (The Swedish Criminal Code). SFS 1962:700. – Arvutivõrgus: https://www.government.se/government-policy/judicial-system/the-swedish-criminal-code/

[94] Lag om straff för terroristbrott (Act on Criminal Responsibility for Terrorist Offences). SFS 2003:148. – Arvutivõrgus: https://www.government.se/government-policy/judicial-system/act-on-criminal-responsibility-for-terrorist-offences-2003148/

välja toodud, et terroriakt on siis, kui selle eesmärgiks on hirmutada elanikkonda, sundida ametivõime või organisatsioone põhjendamatult tegema toiminguid või hoiduma tegutsemast või tõsiselt destabiliseerima või hävitama põhilisi poliitilisi, põhiseaduslikke, majanduslikke või sotsiaalseid struktuure. Selline säte on vajalik selleks, et mõista, mida konkreetselt on mõeldud terrorirünnakuna, kuna teised sätted viitavad hiljem terroriakti mõistele.

Rootsi õigusaktides on mitmeid erinevaid sätteid, mis puudutavad terrorismi, kuid käesolevas magistritöös keskendutakse eelkõige nendele sätetele, mis puudutavad interneti kasutamist terroristlikul eesmärgil. Lisaks terroriaktide kriminaalvastutuse seadusele on Rootsis seadus[95], mis puudutab konkreetsemalt kriminaalvastutust avaliku provokatsiooni, värbamise ning treenimise terroriaktide ja teiste eriti raskete kuritegude jaoks. Selle seaduse teises paragrahvis on välja toodud eriti rasked kuriteod, mille alla liigitub ka eespool räägitud terroriakti paragrahv. Terroriaktide ja muude eriti raskete kuritegude kriminaalvastutuse seaduses on kriminaliseeritud avalik provokatsioon, värbamine, treenimine, nii treeningu pakkumine kui saamine. Kuigi üheski sättes ei ole selget viidet sellele, et selle paragrahvi alla koonduvad ka internetis toimunud terroristliku sisuga suhtlused, värbamised või erinevate propagandamaterjalide üles laadimised, siis võib eeldada, et need tegevused liigituvad terroriaktide ja muude eriti raskete kuritegude kriminaalvastutuse seaduse paragrahvide alla.

2.2.2. Soome terrorismivastane strateegia ja regulatsioon

Soomes peetakse terrorismi ärahoidmise üheks oluliseks aspektiks ühiskonna polariseerumise ja ebavõrdsuse vältimist erinevates poliitilistes küsimustest, kuna kui selle tõttu mingis ühiskonna grupis tekib võõrandumise tunne, siis see võib kaasa tuua vägivaldse radikaliseerumise ja terrorismi. Selle jaoks võeti Soomes 2016. aastal vägivaldse radikaliseerumise ja äärmusluse ennetamise tegevuskava, mille abil

[95] Lag om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet (Act on Criminal Responsibility for Public Provocation, Recruitment and Training concerning Terrorist Offences and other Particularly Serous Crime). SFS 2010:299. – Arvutivõrgus: https://www.government.se/government-policy/judicial-system/act-on-criminal-responsibility-for-public-provocation-recruitment-and-training-concerning-terrorist-offences-and-other-particulary-serious-crime/

koordineeritakse ametiasutuste tegevust kriminaalkoodeksis määratletud terroriaktide avastamiseks ning nende vastu võitlemiseks.[96]

Sarnaselt Rootsi terrorismivastase võitluse strateegiaga tegeletakse Soomes erinevate koolituste korraldamisega, teadustööde ning teabevahetusega, mille kaudu üritatakse jõuda võimalikult suure hulga inimesteni, et tõsta nende inimeste teadlikkust terrorismi osas. Soomes peetakse oluliseks nii siseriikliku kui ka rahvusvahelist koostööd terrorismivastases võitluses. Terrorismivastane võitlus hõlmab enda alla teatud riskigrupis olevate üksikisikute jälgimise, teabe jagamise ametiasutuste vahel, terrorismi rahastamise vastu võitlemise ja kriminaalvastutuse jõustamise. Terrorismivastase võitluse peamiseks eesmärgiks on kaitsta riigis elavate inimeste elu ja tervist. Soomes on terrorismivastases võitluses oluline, et terrorirünnakute tagajärjed mõjutaksid võimalikult minimaalselt ühiskonna igapäevast elu ning et ühiskonna toimimiseks vajalikud teenused ei katkeks.[97]

Soome kriminaalkoodeksi peatükis 34a on reguleeritud terrorism. Soomes peetakse terroristiks isikut, kes on terroristliku kavatusega ning käitub viisil, mis soodustab tõsise kahju tekitamist riigile või rahvusvahelisele organisatsioonile ning paneb toime kriminaalkoodeksi peatüki 34a esimeses lõigus välja toodud kuriteo. Terrorismi puututavas peatükis on reguleeritud terroristliku kavatsusega toime pandava kuriteo ettevalmistamine, terroristliku rühmitusse kuulumine ning terrorirühmituse tegevuse edendamine, mis omakorda jaguneb veel kolmeks:

1) terrorirühmituse koolitamise pakkumine;
2) reaalne koolitamine terroristliku rühmituse tegevuseks;
3) terroristliku rühmitusse värbamine.

Ehk kokkuvõtvalt on Soome kriminaalkoodeksis reguleeritud terroriaktide loetelu, terroriaktides osalemine ning lisaks veel terroristliku rühmitusse värbamine, selle toetamine, näiteks koolituse pakkumine või sellise koolituse vastuvõtmine ja terroriakti sooritamise eesmärgil reisimine.

11.03.2019 kiitis Soome Parlament heaks valitsuse ettepaneku tsiviilluure seaduse kohta. Selle seadusega soovitakse Soomes parandada võimet kaitsta riigi julgeolekut tõsiste

[96] Ministry of the Interior, Finland. National Counter-Terrorism Strategy 2018-2021. Internal security. Ministry of the Interior publications 28/2018. Helsinki 2018, p 1.4 – Arvutivõrgus: https://julkaisut.valtioneuvosto.fi/handle/10024/161188 (15.04.2020).

[97] Samas, p 3.1- 3.4

ohtude eest ning antakse täiendavaid volitusi terrorismiga võitlemiseks. Tsiviilluure seadus parandab Soome võimet kaitsta riigi julgeoleku tõsiste ohtude eest. Soome julgeolekuinfoteenistusele antakse täiendavaid volitusi näiteks terrorismi vastu võitlemiseks.[98]

Kuna interneti kasutamine terroristlikel eesmärkidel on muutumas järjest suuremaks probleemiks, pööratakse ka Soomes sellele enam tähelepanu. Soomes liigitub interneti kasutamine terroristlikel eesmärkidel küberkuritegude alla. Küberkuritegevus või arvutikuritegevus on kuriteod, mille toimepanijad ründavad või kasutavad infotehnoloogiat või infovõrke.[99]

2.2.3. Prantsusmaa terrorismivastane strateegia ning regulatsioon

Prantsusmaa on üks juhtivaid Euroopa riike terrorismivastases võitluses. 2018. aastal arreteeriti Prantsusmaal 310 terrorismiga seotud süütegude kahtlusega isikut, Euroopas kokku oli 1056 arreteerimist.[100] Nii nagu Euroopa Liidu kui ka teiste käesolevas magistritöös vaatluse all olevate riikide terrorismivastases võitluses keskendub ka Prantsusmaa erinevatele valdkonnale, mille abil terrorismi vastu võidelda. Üheks peamiseks valdkonnaks on ennetustöö, mille eesmärgiks on tõkestada terroristlike rühmituste laienemine ning terrorirünnakute toimumine. Selles valdkonnas on eelkõige tähelepanu suunatud radikaliseerumise poole, kuna radikaliseerunud isikud on potentsiaalne oht uute rünnakute läbiviimiseks.[101]

2016-2018. aastatel Prantsusmaal toimunud terrorirünnakute tõttu koostati 2018. aastal uus terrorismivastane tegevuskava, mille üheks peamiseks eesmärgiks on reageerida

[98] Ministry of the Interior, Finland. Counter-terrorism measures in Finland. – Arvutivõrgus: https://intermin.fi/en/police/counter-terrorism/counter-terrorism-measures-in-finland (24.03.2020)

[99] Ministry of the Interior, Finland. Cybercrime - Information networks and crime. – Arvutivõrgus: https://intermin.fi/en/police/cybercrime (24.03.2020)

[100] European Union Terrorsim Situation and Trend Report 2019, lk 15

[101] French Foreign Policy. Terrorism: France's International Action. – Arvutivõrgus: https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/terrorism-france-s-international-action/ (20.04.2020)

muutuvatele julgeolekuprobleemidele. Strateegias on välja toodud 32 erinevat suuremat punkti, mida tuleb terrorismivastasel võitlusel tähele panna või parandada.[102]

Prantsusmaal pööratakse üha suuremat tähelepanu just terroristlike rühmituste tegevusele internetis. Terrorismivastases tegevuskavas kajastatud statistika pinnalt selgus asjaolu, et Prantsusmaal viibib suurel hulgal radikaliseerunud või potentsiaalset ohtu julgeolekule kujutavaid isikuid. Näiteks said 2016. aastal Prantsusmaa õiguskaitseorganid teateid vägivaldse radikaliseerumise kohta 9300 isikust. Radikaliseerumise tõttu jälgitavate isikute arvu märkimisväärne suurenemine kinnitas fakti, et terroristlikel rühmitustel on suur võimekus propaganda levitamisel internetis.[103] Prantsusmaal tehti uue tegevuskava loomisel selgeks need punktid, mis terrorismivastases võitluses tundusid probleemsed ning vajasid suuremat tähelepanu ja uudsemaid lähenemisi, näiteks on terroristliku sisuga leviva materjali vastu võitlemine internetis üks suurimaid väljakutseid.

Prantsusmaa on terrorismivastases tegevuskavas keskendunud terrorismi propageeriva internetisisu eemaldamisega tegelemisele. Nii nagu ka Soome ja Rootsi terrorismivastase võitluse korraldamises rõhutati koostöö olulisele, on ka Prantsusmaa strateegias välja toodud koostöö tegemine suuremate internetiteenust pakkuvate platvormidega, et seeläbi tuvastada ja eemaldada võimalikult palju terroristliku sisuga materjale.[104] Kuigi sellise koostööga kaasnevad positiivsed tulemused, nagu näiteks Euroopa Liidu terrorismivastase üksuse poolt läbiviidud koolitusel, kuid siiski esinevad ka teatud piirangud, kuna internetiteenust pakkuvatel platvormidel on vabatahtlik selliste materjalide eemaldamine.[105] Selleks on Prantsusmaa koos teiste Euroopa riikidega (sealhulgas Saksamaa ja Suurbritanniaga), võtnud endale kohustuse kehtestada õigusaktid, millega kehtestatakse internetilehekülgedele kohustus terrorismi pooldava sisu avastada ning eemaldada.[106]

---

[102] France Premier Ministre. Action Plan Against Terrorism. 13.07.2018 – Arvutivõrgus: http://www.sgdsn.gouv.fr/uploads/2018/10/20181004-plan-d-action-contre-le-terrorisme-anglais.pdf (20.04.2020).

[103] France Premier Ministre. Action Plan Against Terrorism, p 1.1-1.2

[104] Samas, action p 13 ja 28

[105] Europol, More than 900 instance of online terrorist propaganda uncovered, 16.03.2018. – Arvutivõrgus: https://www.europol.europa.eu/newsroom/news/more-900-instances-of-online-terrorist-propaganda-uncovered (15.03.2020)

[106] France Premier Ministre. Action Plan Against Terrorism, action p 28

2018. aastal oli Euroopa Liidu liikmesriikidest Prantsusmaal kõige rohkem isikuid, kes olid kohtu all terrorismi seonduvalt.[107] Prantsusmaal on suureks probleemiks terrorirühmituse ISIS-meelsed või rühmituse poolt värvatud isikud. Pärast 2015. aastal Pariisis toimunud terrorirünnakut pöördus Prantsusmaa ÜRO liikmesriikide poole, mille eesmärgiks oli koostada rahvusvaheline õigusraamistik, mis paneks internetiteenuse pakkujad jagama vastutust nendega, kes neid platvorme kasutavad terroristlikel eesmärkidel.[108] Seega astus Prantsusmaa juba 2015. aastal samme selle suunas, et internetiplatvormidele kehtestada suuremaid kohustusi, mis aitaks kaasa terroristliku sisuga materjalide eemaldamisele nendelt lehekülgedelt.

Internetiteenuste pakkujatele kohustuse seadmiseks on esmalt vajalik määratleda terrorismi laiemalt.[109] Kuid kuna terrorismile pole rahvusvaheliselt suudetud leida ühtset definitsiooni, mistõttu määratletakse terrorismi terrorikuritegude järgi. Seega tuleks terrorikuritegude ulatust piirate konkreetse loeteluga, mille hulgas on välja toodud ka interneti puudutavad sätted. Riigid on terrorikuritegusid määratlenud küllaltki avaralt, kuigi samaaegselt üritatakse seda loetelu hoida võimalikult kitsalt. See on oluline seetõttu, et loetelus ei oleks välja toodud selliseid kuritegusid, mis on küll ühiskondlikult taunitavad, kuid ei ole terroristlikud.[110]

Prantsusmaa karistusseadustiku[111] neljanda peatüki teises jaotuses on reguleeritud terrorismi puudutavad sätted (prantsuse keeles Code pénal, inglise keeles Penal Code). Sarnaselt teistele eeltoodud riikidele on Prantsusmaal terrorism defineeritud terrorikuriteo kaudu. Prantsusmaa karistusseadustiku artiklis 421-1 on välja toodud loetelu kuritegudest, mille toimepanemist loetakse terroriaktiks, kui need on tahtlikult seotud üksikisiku või kollektiivse rühmitusega, mille eesmärk on avalikku korda tõsiselt häirida hirmutamise või terroriga.

Prantsusmaa karistusseadustiku artikli 421-2-5 kohaselt on kuriteoks terroriaktidele provotseerimine ja avalik üleskutsumine. Selle artikli kolmanda lõigu järgi kohaldatakse

---

[107] European Union Terrorism Situation and Trend Report 2019, lk 21

[108] Yu, J. Regulation of Social Media Platforms to Curb ISIS Incitement and Recruitment: The Need for an International Framework and Its Free Speech Implications. – Journal of Global Justice and Public Policy, vol. 4, no. 1, Spring 2018, lk 16

[109] Samas, lk 19

[110] Samas

[111] Code pénal (Penal Code). – Arvutivõrgus: https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719

artiklis välja toodud kuritegude korral, kui need pannakse toime kirjaliku või audiovisuaalse ajakirjanduse vahendusel või üldsusele internetis edastamise kaudu, vastutavate isikute kindlaksmääramiseks neid küsimusi reguleerivate seaduste erisätteid. Prantsusmaa karistusseadustiku artikkel 421-2-6 reguleerib terroriakti toimepanemise ettevalmistamist. Selle artikli teise lõigu punkti c kohaselt on tegemist terrorikuriteo ettevalmistamisega, kui isik konsulteerib veebis ühe või mitme avaliku kommunikatsiooniteenusega või omab dokumente, mis provotseerivad otseselt toime panna terroriakt või mille abil on võimalik terroriakt toime panna. Lisaks on Prantsusmaa reguleeritud terroristlikku rühmitusse kuulumine, terroristliku rühmituste rahastamine ning rühmitusse värbamine.

Prantsusmaal on seadusega kohustatud internetiplatvorme eemaldama terroristliku sisuga postitused enda lehekülgedelt. Prantsusmaa politseil on võimalik kohtust taotleda terroristliku sisu eemaldamist või terrorismi propageeriva saidi osalist või täielikku sulgemist. Lisaks on võimalik taotleda kohtu kaudu taotleda Prantsusmaa internetikasutajate juurdepääsu takistamist.[112] Prantsusmaa seaduse nr 2004-575[113] artikkel 6-1 kohaselt tuleb internetiplatvormidel terroristliku sisuga materjal eemaldada enda leheküljelt kahekümne nelja tunni jooksul. Kui internetiplatvorm seda kahekümne nelja tunni jooksul ei eemalda, on võimalik nõuda kohtu kaudu sellise lehekülje ajutist või täielikku sulgemist.

05.02.2015 määrus nr 2015-125[114] käsitleb terroriakte provotseerivate või kiitvate saitide blokeerimist. Selle määrusega on välja toodud kindlad kriteeriumid ja reeglid, mida on vajalik enne terroristliku sisu sisaldava lehekülje sulgemist õiguskaitseorganitel teha ning mis tingimustele lehekülg peab vastama.

---

[112] Apologie du terrorisme – Provocation au terrorisme. Direction de l'information legale et administrative (Premier minister), Ministere charge de la justice. – Arvutivõrgus: https://www.service-public.fr/particuliers/vosdroits/F32512 (26.04.2020)

[113] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. NOR: ECOX0200175L. – Arvutivõrgus: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164

[114] Décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique. NOR: INTX1502813D. – Arvutivõrgus: https://www.legifrance.gouv.fr/eli/decret/2015/2/5/INTX1502813D/jo/texte

Prantsusmaa kriminaalmenetluse seadustiku[115] artikkel 706-23 kohaselt võib kohtunik Prantsusmaa karistusseadustiku artiklis 421-2-5 sätestatud asjaolude suhtes teha otsuse, millega kohaldada ajutise meetmena internetiteenuse osutamise peatamine, kui on tegemist õigusvastase rikkumisega.

2.2.4. Suurbritannia terrorismivastane strateegia ning regulatsioon

Suurbritannia terrorismivastases strateegias on samamoodi teistele käesolevas magistritöös vaadeldud riikidele välja toodud, et erinevad terroristlikud rühmitused kasutavad interneti enda tegevuste ja eesmärkide propageerimiseks. Euroopas ja Suurbritannias toimunud rünnakud tõestasid veel korda, kuivõrd efektiivselt suudavad terroristlikud rühmitused väravata uusi liikmeid, et neid mõjutada toime panna mõni terrorirünnak.[116] Tehnoloogia arenguga muutub järjest keerulisemaks terrorismi vastu võitlemine, kuna terroristlikud rühmitused saavad tehnoloogia arenguid nende endi eesmärkide täideviimiseks ära kasutada. Seetõttu rõhutatakse ja tuuakse välja nii Suurbritannia kui ka näiteks Prantsusmaa terrorismivastastes strateegiates, et terroristlikud rühmitused kasutavad interneti peamise vahendina propaganda levitamisel ning rünnakute ettevalmistamisel.[117] Loomulikult ainuüksi sellest, et riigid enda strateegiates nendivad selliseid fakte, ei piisa, kuid siiski on oluline välja tuua, et järjest enam märgatakse, kuivõrd suur ohuallikas on riikide julgeolekule see, et terroristlikel rühmitustel on niivõrd mõjuvõimas juurdepääs interneti kaudu Euroopas elavatele isikutele, keda kas värvata või koolitada mõne terrorirünnaku täideviimiseks või ettevalmistamiseks.

Suurbritannias tegeleb luureasutus MI5 terrorismivastase võitlusega. MI5 on tuvastanud enda praktikast, et internetist on saanud üks peamisi vahendeid potentsiaalsete terroristide õpetamiseks ja koolitamiseks. Näiteks toimuvad internetis treeninglaagrid, mille käigus jagatakse nõuandeid või õpetusi rünnakute ettevalmistamiseks ning korraldamiseks. Suur

---

[115] Code de procédure pénale. – Arvutivõrgus: https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071154

[116] Parliament by the Secretary of State for the Home Department by Command of Her Majesty. The United Kingdom's Strategy for Countering Terrorism. 06.2018. Cm 9608, lk 7 – Arvutivõrgus: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf (10.04.2020)

[117] Samas, lk 24

hulk inimesi, kes selliseid veebisaite teevad või informatsiooni sinna üles panevad, on tuvastatud ning Suurbritannias ka süüdi mõistetud. Lisaks on tuvastatud ka selliseid isikuid, kes nendelt veebisaitidelt informatsiooni alla on laadinud ning ka nemad on saanud süüdimõistva kohtuotsuse.[118]

Suurbritannia strateegias on välja toodud mitmeid erinevaid samme, kuidas terrorismi vastu võidelda. Üheks sammuks on suurema tähelepanu pööramine terroristlikul eesmärgil interneti kasutamise vastu võitlemisel, kuna sellega kaasnevad globaalsed riskid mõjutavad otseselt riigi julgeolekut.[119] Seetõttu üritatakse tagada, et terroristlikel rühmitustel puuduks juurdepääs või võimalus turvalistele kohtadele internetis, et seal enda propagandat levitada. Selle jaoks on Suurbritannia järjest enam täiustanud koostööd erinevate tehnikaettevõtetega, mille tulemusel soovitakse luua järjest efektiivsemad arendused, mille abil oleks võimalik tuvastada ning eemaldada internetis leiduv terroristliku sisuga materjal.[120]

Suurbritannias on rõhku pandud ka sellele, et inimesed annaksid nende poolt avastatud terroristliku sisuga materjalidest internetis teade. Selleks on loodud eraldi kampaania ning raporteerimise võimalus internetis.[121] Sellise meetme toimimiseks on vajalik aga põhjalik teavitustöö, et inimesed tunneksid internetis ära terroristliku sisu. See sarnaneb mõningaselt Rootsis ja Soomes korraldatud kampaaniatega, mille käigus üritati inimestele selgeks teha, milline mõju on terroristliku sisuga materjalidel internetis ning kuidas neid tuvastada ja õiguskaitseorganitele teada anda.

Suurbritannia üks põhilisi terrorismi puudutavaid õigusakte on Terrorism Act 2000[122], mida on ajaga muudetud, näiteks seadusega Counter-Terrorism and Border Security Act 2019[123] muudeti teabe kogumise peatükki. Suurbritannias on teabe kogumise all muuhulgas välja toodud, et toime on pandud kuritegu, kui inimene kogub või salvestab internetist teavet, mis võib olla kasulik terroriakti toimepanijale või ettevalmistavale

---

[118] Security Service MI5. International Terrorism - Terrorist training and indoctrination. – Arvutivõrgus: https://www.mi5.gov.uk/terrorist-training-and-indoctrination (15.04.2020)

[119] The United Kingdom's Strategy for Countering Terrorism, lk 12

[120] Samas, lk 28

[121] Counter Terrorism Policing, Report Suspicious Activity. – Arvutivõrgus: https://act.campaign.gov.uk/

[122] Terrorism Act 2000. 2000 c.11. – Arvutivõrgus: http://www.legislation.gov.uk/ukpga/2000/11/contents

[123] Counter-Terrorism and Border Security Act 2019. 2019 c.3. – Arvutivõrgus: http://www.legislation.gov.uk/ukpga/2019/3/contents

isikule. Kuid lisaks on kuritegu toime pandud ka sellisel juhul, kui inimene sellist teavet internetist vaatab või kui tal on sellisele teabele juurdepääs. Kuid vabastavaks asjaoluks sellise tegevuse puhul on mõistlik vabandus, milleks võib näiteks:

- inimene polnud teadlik teabe internetist vaatamise ajal, et see võiks olla kasulik isikule, kes valmistab ette terroriakti või kellel on plaanis toime panna terroriakt;
- kui selle eesmärgiks oli ajakirjaniku töö tegemine või akadeemilise uurimistöö tegemine (Terrorism Act 2000 section 58).

Teiseks oluliseks õigusaktiks Suurbritannias terrorismivastases võitluses on Terrorism Act 2006[124]. Selles seaduses on välja toodud terrorismile õhutamise ning terroristliku väljaannete levitamise peatükid, lisaks on nende kohta eraldi peatükk selle kohta, kui õhutamine ja levitamine on toime pandud internetis.

Counter-Terrorism and Border Security Act 2019 tehti muudatused erinevates terrorismivastastes õigusaktides, mille üheks eesmärgiks oli ajakohastada terroristidele kasuliku teabe hankimise kuritegu. Selle muudatusega sooviti ära katta seaduses see pool, kui internetis vaadatakse terroristlikul eesmärgil teavet, kuid ei laadita püsiva dokumendina alla.

2.2.5. Saksamaa terrorismivastane strateegia ning regulatsioon

Saksamaa terrorismivastases võitluses on sarnased põhimõtted ja eesmärgid Euroopa Liidu strateegiaga. Saksamaal kaardistati vastuäärmusluse projekti raames, kuivõrd suur probleem on äärmuslusel, selle alla liigitub ka terrorism. Vastuäärmusluse projektiga tehti kindlaks, milliseid vahendeid äärmusluse ja terrorismi vastu võitlemisel kasutatakse, mida on selleks juba tehtud ning kuidas selle vastu veel paremini võidelda. Nii nagu eelnevate riikide strateegiates on ka Saksamaal tähelepanu pööratud sellele, et terroristlikud rühmitused kasutavad ühe enam internetti enda eesmärkide täitmiseks. Projekti raames avaldati ka Saksamaal toiminud terrorijuhtumite faktilised asjaolud, mis näitavad, milline oli interneti roll terrorirünnaku ettevalmistamisel. 19.novembril 2019 toimus Saksamaal operatsioon, mille raames arreteeris eripolitsei Süüriast pärit meesterahva, kelle eesmärgiks oli toime panna terrorirünnak. Selle menetluse raames tehti kindlaks, et arreteeritud

[124] Terrorism Act 2006. 2006 c.11. – Arvutivõrgus: http://www.legislation.gov.uk/ukpga/2006/11/contents

meesterahvas oli eelnevalt otsinud veebist informatsiooni pommide ehitamise kohta. Lisaks oli meesterahvas interneti kaudu arutanud rünnakuplaane. Selliseid sarnaseid kaasuseid on Saksamaal veelgi, kus internetis on toimunud vestlused ning juhiste andmised terrorirünnaku korraldamiseks.[125] Selliste kaasuste faktiliste asjaolude üldine avaldamine informeerib avalikkust, kuidas internetti terroristlikul eesmärgil kasutatakse. Terrorismivastases võitluses on üha enam rõhutatud interneti rolli kasvule, mistõttu aitab selline avalikustamine Saksamaal elavatel inimestel paremini mõista, kuidas terrorism internetis toimub. Kuid sellise avalikustamisega näidatakse Saksamaa õiguskaitseorganite heade tööde tulemusi. Selle abil on võimalik vähendada ühiskonnas hirmu, mille külvamine on terrorirühmituste üheks eesmärgiks.

Saksamaa vastuäärmusluse projektiga hinnati äärmusluse ja terrorismi vastu võitlemiseks kasutatud vahendeid. Üheks põhiliseks positiivseks tulemuseks oli spetsiaalsete terrorismivastase võitlusega tegelevate organisatsioonide loomine. Nende organisatsioonide kaudu on terrorismivastane võitlus muutunud efektiivsemaks. Üheks valdkonnaks, millele Saksamaal on suurt rõhku pandud, on terroristlike rühmituste rahastamise tõkestamine. Selles valdkonnas on Saksamaal järjest enam töövõite.[126] Tehnoloogia areng pakub terrorismivastases võitluses uusi võimalusi. Saksamaal on alates 2017. aasta augustist testitud näotuvastustarkvara. Selle tarkvara eesmärgiks on kaasa aidata õiguskaitseorganitel videovalve ja andmebaaside võrdluse abil tuvastada kuriteos ja terrorismis kahtlustatavad.[127]

Saksamaa karistusseadustikus[128] ei ole terrorismivastased regulatsioonid koondatud ühe peatüki alla. Paragrahvis 89c on reguleeritud terrorismi rahastamine, paragrahvis 129a on sätestatud terroristliku organisatsioonide moodustamine ja sellega ühinemine.

2017. aasta sügisel võttis Saksamaa parlament Bundestag vastu seaduse[129], mis piirab vihakõne, kriminaalseid materjale ja väärinformatsiooni sotsiaalmeedia platvormidel. Selle seadusega kohustati sotsiaalmeediaettevõtteid, näiteks Google, Facebook, Twitter,

---

[125] Counter Extremism Project. Germany: Extremism & Counter-Extremism. Report, lk 9 – Arvutivõrgus: https://www.counterextremism.com/countries/germany (26.04.2020)

[126] Samas

[127] Samas, lk 18

[128] Strafgesetzbuch – StGB (German Criminal Code). BGBl. I S. 3322. – Arvutivõrgus: https://www.gesetze-im-internet.de/stgb/StGB.pdf

[129] Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG). BGBl. I S. 3352. – Arvutivõrgus: https://www.gesetze-im-internet.de/netzdg/NetzDG.pdf

eemaldada ebaseaduslik sisu ja vihakõned oma platvormidelt 24 tunni jooksul pärast teate saamist. Kui kohustust sotsiaalmeediaplatvormid ei täida, siis on võimalik seaduse järgi trahvida neid kuni 50 miljoni euro ulatuses. 2020. aastal kiitis Saksamaa valitsus heaks seaduseelnõu, mille kohaselt peavad sotsiaalmeediaettevõtted teavitama koheselt politseid paremäärmusluslikest propagandast, vägivalda, mõrva või vägistamisähvardusi sisalduvatest postitustest ning ka sellistest postitustest, mis viitab sellele, et keegi on ettevalmistamas terrorirünnakut või levitab pilte laste seksuaal väärkohtlemisest. Seda seadust kohaldatakse selliste internetiplatvormide suhtes, mille eesmärk on võimaldada kasutajatel jagada sisu teiste kasutajatega või teha seda sisu üldsusele kättesaadavaks. Platvormid, mis tegelevad ajakirjandusliku või toimetusliku sisu pakkumisega, mille eest vastutab teenuseosutaja ise, ei kuulu selle seaduse alla.[130]

2.3. Eesti terrorismivastane strateegia ja regulatsioon

2.3.1. Eesti strateegia

14.11.2013 kiideti Eesti Vabariigi Valituse poolt heaks Eesti terrorismivastase võitluse põhialused, millega pandi paika Eesti eesmärgid terrorismivastases võitluses, kaardistati terrorismi poolt tekitatud oht maailmas ning Eestis. Lisaks toodi välja konkreetsed meetmed, kuidas peaks terrorismi vastu võitlema. Eesti jaoks on terrorismivastases võitluses märksõnaks terrorismiohu ennetamine, millest tuleneb vajadus tegeleda korraga mitme erineva valdkonnaga.[131]

Kuigi Eestis on terrorismioht siiamaani püsinud madalal tasemel, on ka Eestis vajalik tegeleda aktiivselt terrorismivastase võitlusega. Selleks, et terrorioht püsiks ka edaspidi madalal tasemel, on oluline tegeleda radikaliseerumise ennetamise, terroristlike rühmitusse värbamise tõkestamise ning rühmituste rahastamise tõkestamisega. Nende meetmete abil on võimalik takistada tulevikus toimuvaid potentsiaalseid rünnakuid või rünnakute korraldajaid. Eesti strateegia järgi tuleb rakendada Eestis rahvusvahelisi sanktsioone ning

[130] Counter Extremism Project. Germany: Extremism & Counter-Extremism. Report, lk 17

[131] Eesti Vabariigi Valitsus. Eesti terrorismivastase võitluse põhialused (2013). Heaks kiidetud Vabariigi Valitsuse poolt 14.11.2013 istungi protokollilise otsusega nr 47 pp nr 5. – Arvutivõrgus: https://www.siseministeerium.ee/sites/default/files/dokumendid/tvv_pohialused_2013.pdf, lk 1

tõkestada strateegiliste kaupade[132] salakaubandust. Nii nagu eeltoodud Euroopa Liidu liikmesriikides pööratakse ka Eestis terrorismivastases võitluses olulist tähelepanu suure rünnakuriskiga objektide ja suure rünnakuriskiga isikute kaitsmisele ning valmisolekule hädaolukordade lahendamiseks. Selle kõige tõhusaks elluviimiseks on vajalik tagada usaldusväärne koostöö kõigi terrorismivastase võitlusega seotud avalik-õiguslike ja eraõiguslike juriidiliste isikute vahel. Oluliseks on ka avalikkusele ajakohase terrorismivastase tegevusega seonduva informatsiooni edastamine.[133]

Terrorismivastaseks võitluseks on Eestis loodud nõukogu, kuhu kuuluvad Siseministeeriumi, Justiitsministeeriumi, Kaitseministeeriumi, Majandus- ja Kommunikatsiooniministeeriumi, Riigikantselei, Rahandusministeeriumi, Välisministeeriumi, Kaitsepolitseiameti, Kaitseväe, Teabeameti, Maksu- ja Tolliameti ning Politsei- ja Piirivalveameti esindajad.[134] Terrorismivastases võitluses on erinevate riikide strateegiates mitmel korral rõhutati erinevate asutuste koostööle just riigisiseselt. Eestis puutuvad vähemalt 12 asutuse esindajad kokku terrorismivastase võitlusega, see tähendab, et kõigi nende 12 asutuse vahel peab olema võimalik tõhus ja toimiv koostöö, et terrorismivastane võitlus oleks jätkusuutlik ning edukas. Selle saavutamine nõuab kõigi asutuste poolset avatust koostööle ning ühist arusaamist probleemist. Lisaks on vajalik ka piisava ressursi tagamine asutustele, et terrorismivastane võitlus oleks üldse võimalik.

Eestis on konservatiivne kodakondsus- ja migratsioonipoliitika ning elatustase on maailma kontekstis keskmisest kõrgem. Need tunnused võivad meelitada üha rohkem immigrante Eestisse elama tulema. Seetõttu on oluline jälgida Eestisse tulevaid välisüliõpilasi ning töölisi ja välja selgitada, mis on nende peamised eesmärgid ja soovid seoses Eestisse tulemisega, kuna välismaalt Eestisse saabujate hulgas võib olla ka terroristlike rühmitustega seotud või nende vaateid omavaid isikuid. Nende isikute puhul tuleb koheselt reageerida, kuna nad on potentsiaalseks ohuks julgeolekule ning lisaks võivad hakata levitama oma vaateid, värbama uusi liikmeid ning abistama terrorismialase väljaõppe korraldamises.[135] Kaitsepolitseiameti sõnul on välisvõistlejatest tulenev oht Eestis siiski

---

[132] Terrorismivastases võitluses loetakse strateegilisteks kaupadeks eelkõige tulirelvi ning muud relvastust, millega on võimalik potentsiaalselt suuri terrorirünnakuid teostada.

[133] Eesti Vabariigi valitus. Eesti terrorismivastase võitluse põhialused, lk 1-2

[134] Siseministeerium. Terrorismivastane võitlus. – Arvutivõrgus: https://www.siseministeerium.ee/et/eesmark-tegevused/sisejulgeoleku-tagamine/terrorismivastane-voitlus (25.03.2020)

[135] Eesti terrorismivastase võitluse põhialused, lk 6

madal. Alates 2013. aastast on tuvastatud paarkümmend Eestiga seotud isikut, kes on viibinud või viibivad konfliktikolletes ning omavad sidemeid äärmusrühmitustega. Üheks näiteks on Eestist pärit välisvõistleja Abdurrahman Sazanakov, kuid Kaitsepolitseiameti hinnangul on nende isikute naasmine Eestisse ebatõenäoline. Probleemiks on muutunud hoopis kohalike radikaalide huvi konfliktipiirkonda sõitmise vastu. Kuna Eesti on Euroopa Liidus transiitriik, mistõttu on Eestit läbinud sellised isikud, kes on seotud terroriorganisatsioonidega.[136] Näiteks 2019. aasta märtsis Uus-Meremaal terrorirünnaku korraldanud meesterahvas külastas 2018. aasta detsembris ka Eestit. Lisaks oli tema sotsiaalmeedia postitustes mitmel korral mainitud Eestit. See ilmestab praegust olukorda, et kuigi terrorioht Eestis on madal, siis on Eesti terrorismiga seotud ning vajalik on aktiivne terrorismivastane võitlus ka Eestis, et vältida võimalikke terrorirünnakuid.

Radikalism ja ekstremism ei saa pidada probleemiks, millega tegelevad ainult julgeolekuasutused. Eestis on julgeolekuasutused reageerivaks jõuks, kui on toimunud mingisugune rünnak või mõned äärmuslikud liikumised on alustanud oma tegevust. Eestis ning ka mujal maailmas on radikalismi ja ekstremismi ennetamisel väga suureks rolliks sotsiaal- ja haridusvaldkonnal.[137] Viimase paari aasta jooksul on vihkamise teema järjest rohkem ühiskonnas esile kerkinud. Olukorra parandamiseks on tehtud erinevaid kampaaniad, millega kutsutakse üles inimese olema rohkem sallivamad. Selliseid kampaaniaid tehakse ka teistes Euroopa Liidu liikmesriikides, näiteks Rootsis seoses terrorismivastase ennetustööga, kuna selle kaudu tõstetakse ühiskonna üldist teadmist aktuaalsetest probleemist ning ühiskond oskab paremini potentsiaalseid ohte näha ja nendest teada anda.

Nii nagu eespool toodud riikide strateegiates rõhutati asjaolu, et järjest enam kasutatakse terroristlikul eesmärgil ära internetti, on see ka Eesti strateegias välja toodud. Mitmed Euroopas tegutsevad äärmuslikud liikumised on huvitatud oma tegevusele uue ja laiema kandepinna leidmisest ning üritavad laieneda ka Eestisse.

Kaitsepolitseiameti hinnangul toimub radikaliseerumine suuresti internetikeskkonnas, millele on kõige vastuvõtlikumad konvertiidid, kelle seos islamiga on värske ning

[136] Eesti Kaitsepolitseiamet. Kaitsepolitseiameti aastaraamat 2018. Tallinn: Kaitsepolitseiamet 2018, lk 30

[137] Siseministeerium. Terrorismivastane võitlus. – Arvutivõrgus: https://www.siseministeerium.ee/et/eesmark-tegevused/sisejulgeoleku-tagamine/terrorismivastane-voitlus (25.03.2020)

motivatsioon järgida usutõlgendust suurem kui sünnijärgsetel moslemitel.[138] Eesti terrorismivastase võitluse strateegias on välja toodud, et Eestis tuleb suuremat tähelepanu pöörata küberjulgeolekule ning küberruumi kuritarvitamisele terroristlike rühmituste poolt. Selle tagamiseks on vajalik valdkonnaga seotud asutuste koostöö ning ressursside jagamine Strateegias on sarnaselt Rootsi, Soome strateegiatele mainitud, et küberturvalisuse tõstmisel, mille hulka kuulub ka terrorismi leviku piiramine internetis, on vajalik elanikkonna ning infosüsteemide haldajate teadlikkuse parandamine küberruumi ohtudest.[139] Kuna küberruum on üleilmne ning riikide küberruumide turvalisus ei sõltu ainult konkreetselt riikide enda pingutustest, vaid ülemaailmsest stabiilsest küberruumist, siis on oluline selles vallas rahvusvaheline koostöö.

Teabe ja kogumuste vahetamine, vastastikuse usalduse kasvatamine ning inimõiguste kaitse küberruumis on meetmed, mis aitavad luua ohutut küberruumi. Eesti panustab järjest enam rahvusvaheliste organisatsioonide ning uute algatuste raames kokku lepitud tegevustesse. Kuna kõikides riikides ei ole küberruumi turvalisuse tagamise võimekus kuigi kõrge, siis on vajalik ka Eesti poolne abi turvaliste e-lahenduste ellu viimisel. Eesti on pikka aega olnud küberjulgeoleku teemadel üks eestkõnelejatest, mida ilmestavad Eesti osalus paljudes rahvusvahelistes algatustes, mida on hiljem küberjulgeoleku valdkonnas tegutsevad organisatsioonid omaks võtnud.[140] Kuna Eestit teatakse maailmas kui ühte tugevat e-riiki, kus on palju IT-spetsialiste, siis sellisel juhul võiks Eesti olla veelgi rohkem seotud terrorismivastases võitluses just internetis toimuvaga. Eestis asuvad NATO küberkaitsekoostöö keskus ning Euroopa Liidu IT-amet, mis kinnitab ainult seda, et Eestit peetakse tugevaks infotehnoloogiaga tegelevaks riigiks. Kuigi Eesti portaalides ei ole suuremat probleemi terroristliku sisuga materjalide osas, siis võiks Eesti roll olla pigem heade lahenduste väljapakkumises, kuidas probleemi võiks kõige paremini lahendada. Kuna tegelikkuses on võimalik ka juhused, kus Eestis elavatel inimestel, on võimalik poolkogemata sattuda terroristliku sisuga saitidele või propagandavideotele, mis on üles laaditud populaarsete sotsiaalmeedia platvormidele. Seetõttu võiks Eesti ka enda terrorismivastases strateegia veelgi rohkem suunata pilku just sellele asjaolule, et

[138] Kaitsepolitseiameti aastaraamat 2018, lk 30

[139] Eesti terrorismivastase võitluse põhialused, lk 7-8

[140] Välisministeerium. Julgeolekupoliitika – küberjulgeolek. – Arvutivõrgus: https://vm.ee/et/tegevused-eesmargid/julgeolekupoliitika/kuberjulgeolek (26.03.2020)

terroristlikul eesmärgil kasutatakse interneti järjest rohkem ning seeläbi ohustatakse nii küberruumi kui ka Eesti ning muu maailma julgeolekut.

Eesti on terves maailmas tuntud eduka IT-riigina, millele tuginedes on võimalik sarnaselt Prantsusmaaga teha tihedat koostööd suuremate internetiplatvormidega, et leida lahendus probleemile. Eesti terrorismivastases võitluses on küll rõhutatud koostöö tegemise olulisust ning Eesti julgeolekupoliitika alustes on välja toodud, et küberruumi kuritarvitamine suureneb, mille hulgas peetakse silmas ka terrorirühmituste poolt tehtavat,[141] kuid siiski ei tundu see olevat Eestis prioriteetsete teemade hulgas. Kuigi Eestis on terrorioht senimaani olnud madal, siis on näiteks Välisluureameti koostatud aastaraamatus siiski välja toodud, et Eestis ei saa täielikult välistada internetis levitava propaganda mõjul radikaliseerumist.[142]

Eestile on terrorismivastases võitluses oluline radikaliseerumise ennetamist erinevate meetmete kaudu, muu hulgas abinõude kasutusele võtmist internetiradikaliseerumise peatamiseks. Liikmesriikide infovahetuse parandamiseks tuleks tõhusamalt rakendada Europoli, Eurojusti ning Interpoli vastavaid süsteeme. Toetame samuti Euroopa Liidu välispiiri tugevdamise meetmeid. Ühtlasi tuleb tõhustada kompensatsioonimeetmeid Schengeni piirkonnas. Esmaoluline on Euroopa Liidu PNR-süsteemi rakendamine. Toetame tõhusate regulatsioonide loomist ebaseadusliku relvakaubanduse tõkestamiseks, sealhulgas interneti kaudu, nt Europoli tulirelvade andmebaasi laiemat kasutamist.[143]

2.3.2. Eesti terrorismivastane regulatsioon

Eesti karistusseadustiku 15. peatüki 3. jaos on reguleeritud süüteod riigivõimu vastu, mille alla kuulub ka terrorism. §-is 237 on defineeritud terrorikuriteo mõiste:

Rahvusvahelise julgeoleku vastase, isikuvastase, elu või tervist ohustava keskkonnavastase, välisriigi või rahvusvahelise organisatsiooni vastu suunatud või üldohtliku kuriteo toimepanemise, keelatud relva tootmise, levitamise või kasutamise või vara ebaseadusliku hõivamise või olulises ulatuses rikkumise või hävitamise või arvutiandmetesse sekkumise

[141] Riigikogu. Eesti julgeolekupoliitika alused. - RT III, 06.06.2017, 2. Riigikogu otsuse „Eesti julgeolekupoliitika alused“ heakskiitmine. Lisa, lk 5

[142] Välisluureamet. Eesti rahvusvahelises julgeolekukeskkonnas 2019, lk 64

[143] Välisministeerium. Eesti Euroopa Liidus. – Arvutivõrgus: https://vm.ee/et/eesti-euroopa-liidus (26.03.2020)

või arvutisüsteemi toimimise takistamise eest, samuti selliste tegude toimepanemisega ähvardamise eest, 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.

KarS § 237 puhul on tegemist blanketse deliktiga, mis tähendab seda, et koosseisupäraste tegude sisustamisel tuleb pöörduda teiste karistusseadustikus sätestatud kuriteokoosseisude poole.[144] Nii nagu Euroopa Liidu direktiivis ning liikmesriikide regulatsioonides on ka Eesti karistusseadustikus terrorismi defineeritud terrorikuriteo kaudu.

Terrorikuriteo defineerimine on karistusõiguslikus väga oluline teiste karistusseadustiku terrorismi kohta käivate paragrahvide jaoks. Näiteks KarS § 237[1] on viidatud terrorikuriteo paragrahvile:

Kolmest või enamast isikust koosnevasse püsivasse isikutevahelise ülesannete jaotusega ühendusse kuulumise eest, mille tegevus on suunatud käesoleva seadustiku §-s 237 sätestatud kuriteo toimepanemisele, samuti sellise ühenduse loomise, juhtimise või sinna liikmete värbamise eest.

Seega on KarS § 237[1] koosseis täidetud, kui koosseisus välja toodud tegevus on suunatud ka terrorikuriteo toimepanemisele. Seetõttu on vajalik kõikvõimalikud kuriteokoosseisud, mis võiksid terroristlike rühmituste eesmärkidega samastuda või nende tegevust rünnakute korraldamisel abistada, vajalik välja tuua.

KarS § 237[1] kohaselt on Eestis kriminaliseeritud sellisesse ühendusse kuulumine, lisaks veel sellise ühenduse loomine, juhtimine või liikmete värbamine. Koosseisutüübilt on on tegemist formaalse süüteokoosseisuga, mis tähendab, et tagajärje saabumine ei kuulu koosseisuliste tunnuste hulka ehk ei ole oluline, kas vastav terrorikuritegu pannakse toime või mitte.[145]

Käesoleva magistritöö esimeses peatükis on välja toodud erinevad viisid, kuidas terroristlikul eesmärgil kasutatakse interneti. Põhiliselt kasutatakse interneti terrorirühmituste poolt propaganda levitamiseks, uute liikmete värbamiseks ning

[144] Kiris, R. KarS § 237/2.

[145] Kiris, R. KarS § 237[1]/2.

koolitamiseks. Paljudel juhtudel propaganda levitamine ei ole suunatud mõne konkreetse terrorikuriteo toimepanemisele, vaid pigem hoopis levitatakse radikaalseid vaateid ning pakutakse erinevaid võimalusi terrorirühmitusega liitumiseks, mida ei saa samastada värbamisega. Sellise propaganda levitamise eesmärgiks on tekitada uutes potentsiaalsetes liikmetes teatav huvi nende veendumuste osas.

KarS § 237^2 lg-s 1 on sätestatud terrorikuriteo ettevalmistamine ja üleskutse selle toimepanemisele:

Käesoleva seadustiku §-s 237 sätestatud kuriteo toimepanemiseks väljaõppe korraldamise või saamise või isiku värbamise või muul viisil sellise kuriteo ettevalmistamise eest, samuti sellise kuriteo toimepanemisele avaliku üleskutsumise eest.

Selles paragrahvis on välja toodud 3 erinevat valdkonda. Esimene nendest hõlmab §-s 237 sätestatud kuriteo toimepanemiseks väljaõppe korraldamist. Terrorismi ennetamise Euroopa Nõukogu konventsiooni (TerEnEKonv) artikkel 7 kohaselt hõlmab väljaõppe pakkumine eeskätt terrorikuriteo täideviimiseks või kaasaaitamiseks juhiste andmist lõhkeainete, tuli- või muude või mürgiste või ohtlike ainete valmistamise või kasutamise kohta või muude eriliste meetodite või tehniliste võtete kohta.[146]

Teine valdkond käesolevas paragrahvis on KarS §-s 237 sätestatud kuriteo toimepanemiseks väljaõppe saamine. Direktiivi 2017/541 preambula 11 punkti kohaselt hõlmab terrorismialase väljaõppe saamine teadmiste, dokumentide ja praktiliste oskuste saamist. Terrorismi Ennetamise Euroopa Nõukogu Konventsiooni lisaprotokolli artikkel 3 kohaselt tuleb sätestada kuriteona ka teistelt isikult terrorikuriteo toimepanemiseks või sellele kaasaaitamiseks juhiste saamine, sealhulgas teadmiste või praktiliste oskuste omandamine lõhkeainete, tuli- või muude relvade või mürgiste või ohtlike ainete valmistamise või kasutamise kohta või muude erimeetodite või tehniliste võtete kohta.[147]

Käesoleva magistritöö esimeses peatükis on välja toodud, et üheks põhjuseks, miks terroristlikul eesmärgil kasutatakse internetti, on juhiste edastamine või informatsiooni jagamine terrorirünnaku korraldamiseks. See tähendab üldiselt seda, et näiteks kuskil Euroopa Liidu liikmesriigis asuv radikaliseerunud isik soovib saada terrorirünnaku läbiviimiseks vajalikke teadmiseid. Terroristlik rühmitus, näiteks ISIS, edastab erinevaid

[146] Terrorismi ennetamise Euroopa Nõukogu konventsioon. – RT II 2009, 10, 24.

[147] Terrorismi ennetamise Euroopa Nõukogu konventsiooni lisaprotokoll. – L 159/17, 22.10.2015

kanaleid pidi isikule informatsiooni. Seega, kui selline teadmiste jagamine õiguskaitseorganite poolt avastatakse, siis tuleb analüüsida, millised koosseisud karistusõiguslikus mõttes on täidetud.

Terrorismi ennetamise Euroopa Nõukogu konventsiooni lisaprokolli seletuskirjas on välja toodud, mida üldse väljaõppe saamine tähendab. Üheks kriteeriumiks on see, et väljaõppe saamine võib toimuda isiklikult. Selle alla liigituvad terroristliku rühmituse poolt korraldatud treeninglaagrites osalemine. Kuid väljaõppe saamise alla läheb ka elektrooniliste vahendite kaudu treeninglaagris osalemine, kuid oluline on see, et isik võtaks aktiivselt treeningust osa. See tähendab aga seda, et selliste veebilehtede kasutamine, mida küll kasutatakse terrorismi eesmärkidel treenimiseks, ei ole piisav, et § 237^2 koosseis väljaõppe saamise osas oleks täidetud. Üheks põhjuseks on õiguspärastel eesmärkidel selliste veebisaitide külastamine või materjalide kogumine, näiteks akadeemilise või teadustöö eesmärgil, ei tuleks pidada terrorismialase väljaõppe saamiseks käesoleva direktiivi tähenduses.

Ehk kui tulla tagasi näite juurde, kus terroristlik rühmitus teadmiseid vahendab radikaliseerunud isikule läbi interneti, siis on Eesti karistusseadustiku mõttes täidetud nii väljaõppe korraldamine kui ka väljaõppe saamine[148] KarS § 237 lg-s 1 sätestatud terrorikuriteo toimepanemiseks. Direktiivi 2017/541 preambula punkti 11 kohaselt tuleb arvesse võtta kõiki juhtumi konkreetseid asjaolusid. Nii võiks terrorismialase väljaõppe saamisena käsitada lõhkeainete valmistamise õpetuse allalaadimist terroriakti toimepanemise eesmärgil. Terrorismialase väljaõppe saamisena tuleb käsitada ka iseõppimist. See tähendab siis näiteks interneti või mingi muu õppematerjali vahendusel teadmiste omandamist, kui eesmärgiks on panna toime terrorirünnak või sellise rünnaku toimumisele kuidagi kaasa aidata.[149]

KarS § 237^2 kolmandaks valdkonnaks on TerEnEKonv artikkel 6 kohaselt on värbamine aga ettepanek panna toime terrorikuritegu või liituda selle toimepanemisele suunatud terroristliku ühendusega.

---

[148] Väljaõppe saamine lisati karistusseadustiku 04.01.2019 jõustunud karistusseadustiku muudatustega.

[149] Karistusseadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seadus (terrorismivastase võitluse direktiivi ülevõtmine) 642 SE. Seletuskiri karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse (terrorismivastase võitluse direktiivi ülevõtmine) eelnõu juurde. Lk 8 – Arvutivõrgus: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/af992ccb-58f7-4a6e-bef5-d8f82772b3b7/Karistusseadustiku%20muutmise%20ja%20sellega%20seonduvalt%20teiste%20seaduste%20muutmise%20seadus%20(terrorismivastase%20v%C3%B5itluse%20direktiivi%20%C3%BClev%C3%B5tmine) (10.04.2020).

Eestis ei ole kriminaliseeritud sellise propaganda sisuga üleskutsed. KarS § 237^2 koosseisu puhul on välja toodud, et avalikuks üleskutsumise jaoks on vajalik, et see oleks suunatud konkreetselt KarS § 237 sätestatud kuriteo toimepanemiseks. Karistusseadustiku kommenteeritud väljaande kohaselt on *terrorikuriteole avalik üleskutsumine määramatule adressaatide ringile suunatud tahteavaldus, mille kohaselt peaks adressaat vm isik panema toime täideviijana või osavõtjana terrorikuriteo koosseisule vastava teo. Üleskutse vorm ei ole oluline, küll aga peab see olema objektiivselt tõsiselt võetav ning äratuntavalt suunatud adressaatide motiveerimisele teataval määral konkretiseeritud terrorikuriteole. Samas terrorikuriteo toimepanemise konkreetse ohu teket koosseis ei nõua; avaliku üleskutse abstraktne ohtlikkus tuleneb aga määratlemata adressaatide ringist.*[150]

KarS § 237^2 koosseis ei hõlma aga olukorda, kus internetis levitatakse terroristliku sisuga propagandat, mis ei sisalda üleskutset toime panna KarS § 237 sätestatud kuritegu. Kuna terrorismivastases võitluses on oluline, et ka sellise sisuga propagandat internetis ei levitataks ning sellise materjalide levitajad vastutusele oleks võimalik võtta. Kuna terrorismi olemus on ajaga muutunud ning praegusel juhul on järjest enam terrorirünnakuid toime pannud üksiküritajad, siis lisaks ennetamise meetmetele on vajalik karistusõiguslik lähenemine olukorra parandamiseks. Terrorismivastases võitluses ennetamiseks kasutatavate meetmetega on võimalik tõkestada sellise propaganda levitamine internetis, kuid karistusõiguslikult ei tohiks sellised üleskutsed, mis ei sisalda konkreetse kuriteo toimepanemist, välja jääda vastutusele võtmisest.

Eestis ei ole kriminaliseeritud KarS § 237^2 välja toodud väljaõppe korraldamiseks jagatavate juhiste ning materjalide omamine. Selle paragrahvi alusel saab vastutusele võtta isiku, kes sellist väljaõpet pakub. *Väljaõppe pakkumine hõlmab eeskätt terrorikuriteo täideviimiseks või kaasaaitamiseks juhiste andmist lõhkeainete, tuli- või muude relvade või mürgiste või ohtlike ainete valmistamise või kasutamise kohta vm eriliste meetodite või tehniliste võtete kohta. Värbamine on ettepanek toime panna terrorikuritegu või liituda selle toimepanemisele suunatud terroristliku ühendusega.*[151] Terrorismivastase võitluse seisukohalt oleks aga selliste materjalide omamise kriminaliseerimine aitaks kaasa ka tõkestada levitamist. Paralleeli saaks tõmmata propaganda, mis ei sisalda terrorikuriteole suunamist, levitamisega. Kui on selgelt tuvastatud, et kusagil veebiplatvormil on üles

[150] Kiris, R. KarS § 237^2/3.2.

[151] Kiris, R. KarS § 237^2/3.1.

laetud terroristliku sisuga video või materjal, mille eesmärk ei ole otseselt õpetada või suunata inimesi terrorikuritegusid toime panema, vaid hoopis terrorirühmituste veendumusi jagada, tasuks karistusõiguslikult vaadelda selliste tegude kriminaliseerimist. Kui riikide õiguskaitseorganid on välja selgitanud, et konkreetne isik omabki terroristliku sisuga materjale, oleks terrorismivastase võitluse seisukohalt olemas veel üks meede juures, mis takistaks terrorismi levitamist.

KarS § 237^3 keskendub terrorikuriteo rahastamise ja toetamisele. Kui terrorismi rahastamise kriteeriumid on üsna selged, mida selle all mõeldakse, siis terrorismi toetamise sisustamine on keerulisem. Terrorismi toetamiseks võib pidada sellist tegu, mille abil on võimalik toetavat objekti või adressaati füüsiliselt, vaimselt või aineliselt kasutada. Vaimse abi all tuleks eelkõige mõelda nõuandeid või ründeobjektide kohta mingisuguse teabe avaldamist. Ainelise abi hulka kuulub terrorikuriteo varustamine vahenditega. Teise koosseisualternatiivi objektiivsed tunnused seisnevad vahendite kättesaadavaks tegemises või nende kogumises. Vahendite all tuleb mõista kõikvõimalikke objekte, siin ei saa tuua välja konkreetset loetelu, mis tooks välja konkreetsed vahendid. Samamoodi nagu ei ole oluline üleskutsumise osas viis või vorm, ei ole ka vahendite kättesaadavaks tegemisel määratud, millisel viisil see toimuma peaks. Selle alla kuulub ka internetti üles laetud juhised.[152]

KarS § 237^4 on välja toodud kuritahtlik sisenemine Eesti Vabariiki. KarS §-id 237^5 ja 237^6 on kõige uuemad terrorismi puudutavad sätted. Nende sätete alusel on karistatav terroristlikul eesmärgil reisimine ning sellise reisi korraldamine, rahastamine ja toetamine.

2.4. Võimalikud lahendused

Käesoleva magistritöö esimeses peatükis on välja toodud, milliseks on terrorism tänapäeval muutunud ning kui suurel hulgal terroristlikud rühmitused internetti enda eesmärkide täideviimiseks ära kasutavad. Sellega seoses on oluline üle vaadata, kas ja kuidas on regulatsioonid terrorismi arengutega kaasas käinud ning kas Eestil oleks käesolevas magistritöös vaadeldud Euroopa Liidu liikmesriikidelt midagi õppida või üle võtta.

[152] Kiris, R. KarS § 237^3/3.1.3 ja 3.2.

Euroopa Liidu terrorismivastase võitluses on järjest enam rõhku pööratud internetis toimuva tõkestamiseks. Kuna tehnoloogia ning interneti areng on loonud terrorirühmitustele hea pinnase, kus enda eesmärke levitada või uusi liikmeid värvata ja koolitada, siis on selle vastu võitlemiseks vajalik ajakohased õigusaktid ning strateegiad. Sarnaselt Euroopa Liidule on Prantsusmaa, Suurbritannia, Saksamaa, Soome ja Rootsi terrorismivastases võitluses rõhutatud internetist tulenevat probleemi. Kui võrrelda neid strateegiaid Eestiga, siis üheks esimeseks probleemkohaks on asjaolu, et Eesti terrorismivastase võitluse põhialused on paika pandud 2013. aastal. Selles dokumendis on välja toodud, et terroristlikud organisatsioonid kasutavad küll internetti värbamiseks, kuid täpsemad vastumeetmed selle probleemiga tegelemiseks puuduvad. Arvestades tehnoloogia ja interneti kiiret arengut, tõstatuvad terrorismivastases võitluses uued probleemid, näiteks tekivad terroristlikel rühmitustel uued võimalused, kuidas enda eesmärke täide viia. Seetõttu on oluline uuesti kaardistada Eesti terrorismivastase võitluse põhialused, et välja selgitada, kas Eestis on terrorismivastases võitluses mõnes valdkonnas probleeme või puudujääke.

Kõikide käesolevas töös vaadeldud riikide strateegiates nähtub, et selle probleemi lahendamisel on vajalik ennetustöö, kuid riigid on seda mõnevõrra erinevalt sisustanud. Ennetamise abil on võimalik ära hoida suuremaid terrorirünnakuid, kuid ka radikaliseerumist ning terroristlike rühmituste uute liikmete värbamist. Töö esimeses peatükis on välja toodud, et terroristlikud rühmitused kasutavad internetti uute liikmete värbamiseks. Nende peamiseks sihtrühmaks on radikaliseerunud persoonid, keda on võimalik lihtsamini mõjutada. Selleks, et terroristliku sisuga postitused selliste inimesteni ei jõuaks, on Rootsis ning ka Soomes üha enam rõhku pandud avalikkuse koolitamisse, et inimesed oskaksid kriitiliselt suhtuda internetis leiduvatele postitustele. Selliste koolitamiste kaudu suudetakse suuremale osale ühiskonnast teadvustada, millised potentsiaalsed ohud internetis leiduvad. Suurbritannias on loodud lehekülg, kus inimesed saavad teada anda terroristliku sisuga postitustest. Kui panna need kaks külge kokku, kus ühelt poolt riigid koolitavad ning teadvustavad üha rohkem enda inimesi internetis toimuvast ning teiselt poolt loovad võimaluse, kus inimesed saavad teada anda. Sellest tulenevalt on võimalik avastada veelgi rohkem terroristliku sisuga materjalide levimist internetis, mis omakorda aitab kaasa sellele, et terroristlikel rühmitustel on keerulisem leida uusi liikmeid, kelle kaudu enda eesmärke täide viia. Kui inimestel on oskus näha ning avastada internetis terroristliku sisuga postitus ning on võimalus sellest koheselt

õiguskaitseorganitele teavitada, vähendab see olulisel määral tõenäosust, et see postitus oleks jõudnud radikaliseerunud isikuni.

Eesti Küberturvalisuse 2019-2022 strateegias on välja toodud, et Eestis muudetakse küberteadmised ja -oskused üldhariduse läbivaks osaks ning viiakse süsteemselt ellu teavituskampaaniad ja täiendkoolitusi ning tõstetakse teadlikkust nii ohtudest kui ka õiguspärasest ja õigusvastasest käitumisest.[153] Lisaks on Eestis järjest enam korraldatud kampaaniaid, mille abil üritatakse avalikkust teavitada eelkõige küberruumides levivatest petuskeemidest. Kuid terrorismivastase võitluse seisukohalt on selliste

Euroopa Liidu terrorismivastases võitluses on võetud konkreetseid meetmeid, kuidas tegeleda just eelkõige internetis toimuva terroristlike materjalide levitamisega. Üheks näiteks on terrorismivastase üksuse loomine. Võrreldes Euroopa Liidu terrorismivastast strateegiat Eesti terrorismivastase strateegia, siis selgub, et Eesti koostatud strateegias on palju vähem rõhutatud terroristlikul eesmärgil interneti kasutamist ning kuidas selle vastu võidelda.

Analüüsides lisaks Euroopa Liidu strateegiale ka teiste magistritöös välja toodud riikide ja Eesti terrorismivastase võitluse strateegiaid ning vaadates läbi nende riikide seadused, mis puudutavad terrorismi, on näha, et järjest enam teadvustatakse suurenevat ohtu, mis tuleneb interneti kasutamist terroristlikel eesmärkidel. Siiski nähtus nendest dokumentidest probleem, millele pole veel kõikides riikides, sealhulgas ka Eestis, lahendust leitud. Magistritöö alapeatükis 1.3 on kirjeldatud olukorda, kus küll avastatakse internetiplatvormidelt terroristliku sisuga postitusi või materjale, kuid selliste postituste mahavõtmine on platvormidele vabatahtlik. Kuigi õiguskaitseorganitel on kasutuses piisavalt võimekas ressurss, mille abil jälgida ja tuvastada internetis terroristliku sisuga materjal, siis puudub neil seaduse järgi õigus kohustada mõnda internetiplatvormi sellise sisuga materjal maha võtta. Probleemseks kohaks ei ole suured internetiplatvormid, neil on üldiselt olemas enda programmid, mille abil näiteks terroristliku sisuga postitusi tuvastada. Näiteks suudab Instagram tuvastada platvormile üles pandud postituse sisu, mille kaudu on tuvastada ka terroristliku sisuga postitusi. Lisaks on suured IT-ettevõtjad (Facebook, Microsoft, Twitter, YouTube, Instagram, Google+, Snapchat ja Dailymotion) ühinenud vihakõnevastase võitluse tegevusjuhendiga, millega tekkis ettevõtetel kohustus

[153] Majandus- ja Kommunikatsiooniministeerium. Küberturvalisuse strateegia 2019-2022, lk 5 – Arvutivõrgus: https://www.mkm.ee/sites/default/files/kuberturvalisuse_strateegia_2019-2022.pdf (10.04.2020).

ebaseadusliku sisu hindamine ning eemaldamine.[154] Siiski puudub seadusest tulenev kohustus sellistel platvormidel, mille eesmärk on võimaldada kasutajatel jagada sisu teiste kasutajatega või teha postitusi, mis on üldsusele kättesaadavad, terroristliku sisuga postitused eemaldada. Sellised platvormid on terroristlike rühmituste sihtmärgid, kuna eesmärgiks on jõuda võimalikult paljude inimesteni. Seetõttu võib kujunda olukord, kus terroristliku sisuga postitus on tuvastatud, aga internetiplatvorm ei eemalda seda, mistõttu jääb see siiski avalikkusele kättesaadavaks. Kui õiguskaitseorganitel oleks seadusest tulenev õigus kohustada selliseid postitusi eemaldama, kuid internetiplatvormide enda kohustust ei täida, annaks see õiguskaitseorganile võimaluse kasutada erinevaid sunnimeetmeid internetiplatvormi vastu.

Selle probleemi lahendamiseks võiks Eestile eeskujuks olla Saksamaa ning Prantsusmaa, kuna nende riikide strateegiatest ning regulatsioonides on probleemile lahendust leitud. Prantsusmaa terrorismivastase võitluse strateegiast nähtub, et suuremate internetiplatvormidega tuleb veelgi rohkem teha koostööd, millest lõpuks võiks välja kooruda kohustus teha selliste terroristlike sisuga postituste ja materjalide eemaldamine.

Prantsusmaal on seaduse järgi kohustatud internetiplatvormid terroristiliku sisuga postitused internetis eemaldama kahekümne nelja tunni jooksul. Kui internetiplatvormid seda ei tee, on võimalik nõuda platvormi ajutist peatamist. Lisaks on võimalik nõuda sellise internetilehekülje blokeerimist või konkreetse terroristliku sisu sisaldava postituse blokeerimist. Sellega tõkestatakse terroristliku sisuga materjali levimist internetis.

Saksamaal kohustab seadus NetzDG internetiplatvorme eemaldama terroristliku sisuga postitused kahekümne nelja tunni jooksul. See seadus puudutab konkreetselt selliseid internetiplatvorme, kus on Saksamaal registreeritud vähemalt kaks miljonit kasutajat. Terroristlikud rühmitused soovivad enda postitustega jõuda võimalikult suure hulga inimesteni, mistõttu tuleb esmalt tähelepanu pöörata just suuremate kasutajate arvuga platvormidel toimuvale. Pärast seaduse jõustumist on koostatud erinevate suuremate platvormide (Google, Facebook, Twitter) poolt analüüse, mille kaudu nähtub, et seaduse alusel eemaldatud postituste arv on märkimisväärselt väiksem nende platvormide enda

[154] Euroopa Komisjon, Euroopa Liidu olukord 2018 – komisjon esitab terroristliku veebisisu eemaldamise uute eeskirjade ettepaneku. – Arvutivõrgus: http://europa.eu/rapid/press-release_IP-18-5561_et.htm (20.04.2020).

seatud reeglite alusel eemaldatud postituste arvust.[155] Kuigi sellise statistika valguses võib jääda esmapilgul mulje, et seaduse loomine polnud vajalik ning suurtel platvormidel on olemas reeglid, mille alusel ka terroristlikud postitused avastatakse ning eemaldatakse. Kuid sellest hoolimata on vajalik seadusega selliseid kohustusi internetiplatvormidele seada, et vältida olukordi, kus terroristliku sisuga postituste eemaldamine poleks vabatahtlik.

Saksamaal vastu võetud seadus NetzDG kohustab internetiplatvorme eemaldama terroristliku sisuga postitused kahekümne nelja tunni jooksul. Eestis hetkel seadustes sellist õiguslikku alust ei ole. Elektroonilise side seaduse[156] § 111^1 järgi on sideettevõtjad, telefoni-ja mobiiltelefoniteenuse, telefonivõrgu ja mobiiltelefonivõrgu teenuse osutajad, interneti-ühenduse, elektronposti ja Interneti-telefoni teenuse osutajad kohustatud säilitama andmeid, §-s 112 on sätestatud teabe andmise kohustus ning § 113 sidevõrgule juurdepääsu võimaldamise kohustus. Kõik need kohustused on abiks õiguskaitseorganitele terroristliku sisuga postituste ja materjalide tuvastamisel, kuid teenuseosutajatel ei ole kohustust internetis leiduva terroristliku sisu eemaldamiseks.

Eestis pole terroristliku sisuga materjalide levimine veel suureks probleemiks, kuid siiski on Eesti terroristlike organisatsioonide jaoks potentsiaalne sihtmärk, kuna Eesti toetab terrorismivastast võitlust. Eesti Kaitsepolitsei aastaraamatust tuleneb, et terroriohu vaates mõjutavad Eesti turvalisust nii radikaliseerunud kui ka Eestit külastavad radikaliseerunud inimesed. Kaitsepolitseiamet on tuvastanud paarkümmend Eestis elavat või Eestiga tihedalt seotud inimest, kes edasi radikaliseerudes võivad kujuneda ohuks Eesti riigi julgeolekule.[157] Seega nende isikute eestvedamisel võib ka Eestis terroristlikul eesmärgil internetti kasutada. Saksamaa ja Prantsusmaa näitel on seadusega loodud internetiplatvormidele kohustus sellise sisuga postitused ja materjalid eemaldada, mis aitab otseselt kaasa terrorismi ennetamisele, kuna mida kiiremini need postitused ja materjalid eemaldatakse, seda väiksem on inimeste arv, kelleni postitustes olnud informatsioon jõudis.

---

[155] Tworek, H. Leerssen, P. An Analysis of Germany's NetzDG Law. 15.04.2019 – Arvutivõrgus: https://www.ivir.nl/publicaties/download/NetzDG_Tworek_Leerssen_April_2019.pdf (20.04.2020)

[156] Elektroonilise side seadus. – RT I, 08.01.2020, 4.

[157] Kaitsepolitsei aastaraamat 2019, lk 41

Euroopa Liidus on loomisel määrus 2018/0331 terroristliku veebisisu levitamise tõkestamise kohta, mis on hetkel ettepaneku staadiumis. Selle määrusega kohustataks internetiplatvormide sarnane kohustus nagu Saksamaal vastu võetud seadusega. Euroopa Komisjon on välja pakkunud mitmed erinevad eeskirjad, mille eesmärgiks on tagada veelgi kiirem terroristliku veebisisu eemaldamine:

- *ühe tunni reegel: terroristlik veebisisu teeb enim kahju esimestel tundidel pärast veebi ilmumist oma levikukiiruse tõttu. Seetõttu esitab komisjon ettepaneku õiguslikult siduvaks ühetunniseks tähtajaks sisu eemaldamiseks liikmesriigi pädeva asutuse poolsest eemaldamiskäsust arvates;*

- *terroristliku veebisisu selge määratlus materjalina, milles kutsutakse üles terroriaktide sooritamisele või õigustatakse seda, reklaamitakse terrorirühmituse tegevust või antakse juhtnööre terroriaktide sooritamise tehnika kohta;*

- *hoolsuskohustus kõigi platvormide puhul, et vältida nende kuritarvitamist terroristliku veebisisu levitamiseks. Sõltuvalt nende platvormide kaudu terroristliku veebisisu levitamise ohust, nõutakse teenusepakkujatelt ka ennetavaid meetmeid, näiteks uute vahendite kasutamist, et oma platvorme ja nende kasutajaid terroristliku kuritarvitamise eest paremini kaitsta;*

- *tihedam koostöö: ettepanekuga luuakse tugevam koostöövõrgustik veebimajutusteenuste pakkujate, liikmesriikide ja Europoli vahel. Teenusepakkujad ja liikmesriigid peavad nimetama 24/7 kättesaadavad kontaktpunktid, et lihtsustada eemaldamiskäskude ja esildiste täitmise jälgimist;*

- *tugevad kaitsemeetmed: sisuteenuse pakkujatel on võimalik tugineda tõhusatele kaebuste esitamise mehhanismidele, mille kõik teenusepakkujad peavad kehtestama. Kui veebisisu eemaldati põhjendamatult, peavad teenusepakkujad selle võimalikult kiiresti taastama. Liikmesriikide ametiasutused pakuvad ka tõhusaid õiguskaitsemeetmeid ning platvormidel ja sisuteenuse pakkujatel on õigus eemaldamiskäsk vaidlustada. Põhjendamatu eemaldamise vältimiseks peaksid automaatseid avastamisvahendeid kasutavad platvormid kasutama ka inimjälgimist ja -kontrolli;*

- *suurem läbipaistvus ja aruandekohustus: läbipaistvus ja kontroll tagatakse iga-aastaste läbipaistvusaruannetega, mida teenusepakkujad ja liikmesriigid peavad esitama selle kohta, kuidas nad võitlevad terroristliku veebisisuga, samuti korrapärase aruandlusega võetud ennetavate meetmete kohta;*

- *ranged ja hoiatavad rahatrahvid: liikmesriigid peavad kehtestama tõhusad, proportsionaalsed ja hoiatavad karistused terroristliku veebisisu eemaldamiskäsu täitmata jätmise eest. Veebisisu eemaldamiskäskude korduva täitmata jätmise eest võidakse teenusepakkujale määrata rahaline karistus kuni 4% tema viimase majandusaasta kogukäibest.*[158]

Selline määrus toetaks terrorismivastast võitlust, kuna sellisel juhul oleks Euroopa Liidu liikmesriikides ühine õiguslik raamistik internetis leviva terroristliku sisu eemaldamiseks. Internetiplatvormidel oleks suurem vastutus ja kohustus sellist sisu enda platvormilt eemaldada ning seeläbi muutuks internet tavakasutaja jaoks turvalisemaks. Kuid selle määrusega võidakse riivata internetiplatvormide ettevõtlusvabadust, mistõttu on vajalik kaaluda määrusega seatud eeskirjade mõju ettevõtlusele. Terroristliku sisu levitamise tõkestamisel internetis on oluline selle võimalikult kiire avastamine ning eemaldamine, seega määrusega seatud kohustus see ühe tunni jooksul pärast avastamist internetiplatvormide poolt eemaldada on mõistlik. Kuid üheks ohuks võib kujuneda see, et selliseid internetiplatvorme võidakse hakata võtma vastutusele selle eest, et nende platvormil terroristliku sisuga postitusi. Näiteks on määruse üheks eeskirjaks ranged ja hoiatavad rahatrahvid. Kui veebisisu eemaldamiskäske korduvalt täitmata jäetakse on määruse järgi võimalik määrata kuni 4% rahaline karistus viimase majandusaasta kogukäibest. Kuigi terrorismivastase võitluse seisukohalt oleks selline kohustus ja vastutus vajalik, et internetis levivat terroristliku sisu tõkestada, siis tuleb esmalt teha koostööd, et kõikidel internetiplatvormidel oleks võimekus ja vajalik ressurss, et ühe tunni jooksul terroristlik veebisisu enda lehelt eemaldada. Lisaks tuleb selle määruse puhul kaaluda, milliseid internetiplatvormi see käsitleb, kas määrusega seatavad kohustused on suunatud kõigile internetplatvormidele või ainult suurematele. Saksamaa näitel on kohustus seatud platvormidele, kus on üle 2 miljoni kasutaja.

Määrusega soovitakse suuremat läbipaistvust ning aruandekohustust. Selline kohustus väiksematele platvormidele võib tekitada neile liiga palju lisakohustusi ning väljaminekuid. Näiteks on määruses välja toodud hoolsuskohustuse suurendamine, millega soovitakse platvormide suunata võtma kasutusele uusi tehnoloogilisi meetmeid, et ennetada terroristliku sisu enda leheküljel. Kuigi määrusega soovitakse tõkestada

[158] Euroopa Komisjon, Euroopa Liidu olukord 2018 – komisjon esitab terroristliku veebisisu eemaldamise uute eeskirjade ettepaneku

terroristliku sisu levimist internetis, peavad internetiplatvormidele seatud kohustused olema proportsionaalsed, et ei tekiks olukordi, kus liiga karmid nõudmised sunnivad ettevõtlusest loobuma.

Selle määrusega võib tekkida probleeme sõnavabadusega, mistõttu tuleb selgelt määratleda terroristlik sisu mõiste. See mõiste ei saa olla liiga avar, kuna sellisel juhul võib tekkida olukordi, kus selle määrusega seatud kohustust kasutatakse ära mõne muu elu valdkonna eesmärgi täideviimiseks.

Võrreldes Eesti karistusseadustiku terrorismi kohta käivaid sätteid teiste töös vaadeldud riikide sätetega, on näha, et suuresti kõikide riikide sätted on sarnased. Euroopa Liidu liikmesriigid on üle võtnud direktiiviga 2017/541 kehtestatud sätted. Eesti seadustes puuduvad sätted sellise olukorra kohta, kui inimene külastab internetis lehekülge, mis sisaldab terroristliku sisuga materjali. KarS § 237^2 käsitleb terrorismialase väljaõppe saamist, mille alla liigitub ka iseõppimine. Iseõppimise all tuleb mõista olukordi, kus isik saab terroristlikult rühmitustelt interneti või mõnda muud moodi õppematerjali, mille abil omandada teadmisi terrorirünnaku toimepanemiseks või sellele kaasaaitamiseks. Seega eeldab iseõppimine terroristliku rühmitustega eelnevat suhtlemist.

Suurbritannia on seaduse Terrorism Act 2000 kohaselt kriminaliseeritud selliste saitide külastamine või vaatamine, kus on terroristliku sisuga materjale. Seadusega on välja toodud vabandavateks asjaoludeks, kui inimene polnud teadlik teabe internetist vaatamise ajal, et see võiks olla kasulik terrorkuritegu ettevalmistavale või toime panna soovivale isikule. Lisaks on Suurbritannias lubatud selliseid lehekülgi külastada, kui selle eesmärgiks on ajakirjaniku töö tegemine või akadeemilise uurimistöö tegemine.

Terroristliku sisu sisalduval veebilehe külastamine ei tähenda koheselt iseõppimist. Kuigi selle kaudu on võimalik õppida näiteks pommivalmistamist, siis tuleb kõigepealt selgeks teha külastamise eesmärk. Üldjuhul võib inimene sellisele lehele sattuda juhuslikult, arusaamata, et seda sisu võiks terrorikuriteo toimepanemiseks kasutada. Ehk Suurbritannias on seaduses välja toodud kaks võimalust, mis vabastavad kuriteo koosseisu realiseerumist, kuid ülejäänud juhtudel on inimestel mingi kindel eesmärk, miks seda lehekülge külastati või vaadati. Kuna terrorioht Euroopas püsib jätkuvalt kõrge eelkõige internetis toimuva radikaliseerumise tõttu, siis tuleb kõikvõimalikke meetmete abil terroristlike sisuga postituste levimist internetis takistada. Seega lisaks ennetavatele meetmetele on võimalik seeläbi võtta vastutusele isikuid, kes terroristliku sisuga lehekülge on külastanud.

Kokkuvõte

Terrorioht Euroopas on jätkuvalt kõrge ning lähiaastate jooksul ei ole näha, et terrorioht Euroopas väheneks. Kuigi terroristlikud rühmitused on nõrgestatud, siis omavad nad rahvusvahelist võrgustikku, mille abil jätkuvalt Euroopa riike ohustada.

Terrorismile ei ole 21. sajandiks veel leitud ühist definitsioon, mis kõiki riike ning rahvusvahelisi organisatsioone rahuldaks. Selleks on tehtud mitmeid püüdlusi ajaloo vältel ning erinevaid uuringuid, kuid ikka pole terrorismile ühtsed definitsiooni. Terrorismi defineeritakse suuresti läbi terrorikuriteo mõiste. See tähendab, et õigusaktides on välja toodud kindlad kriteeriumid ja kuriteod, mille täitumisel on tegemist terroriaktiga. Terrorismi defineerimine õigusaktides on seetõttu oluline, et mõista terrorikuriteoga kaasnevaid kuritegusid. Näiteks on käesolevas magistritöös analüüsitud riikide õigusaktides kriminaliseeritud terrorikuriteo ettevalmistamine. Kuid selleks, et õiguslikus mõttes oleks võimalik hakata ettevalmistamise paragrahvi käsitlema, tulebki kindlaks teha terrorikuriteo mõiste sisu.

Terrorismi olemus on ajas muutunud ning see on globaalne probleem. Suuresti on sellele kaasa aidanud tehnoloogia kiire areng, mis võimaldab terroristlikel rühmitustel luua paremaid ja tugevamaid rahvusvahelisi võrgustikke. Terroristlikud rühmitused kasutavad interneti, et levitada seal enda veendumusi ja propagandat ning värvata uusi potentsiaalseid liikmeid. Nii sotsiaalmeediasse kui ka teistesse suuremate kasutajate arvuga platvormile lisatakse erinevaid propaganda videoid ja pilte, mille eesmärgiks on jõuda oma ideedega võimalikult suure arvu inimesteni. Interneti vahendusel toimub Euroopas radikaliseerumine, mille tulemusena püsib Euroopas terrorioht jätkuvalt kõrgena. Näiteks CEP poolt korraldatud uuringuga tuvastati paari kuu jooksul Youtube keskkonnas üle tuhande terroristliku sisuga video. Internet pakub terroristlikele rühmitustele anonüümset kohta, kus on võimalik üksteisega suhelda krüpteeritud teid pidi. Selle kaudu värvatakse nii uusi liikmeid kui ka jagatakse informatsiooni ning teadmisi. Lisaks toimuvad internetis erinevad treeningud, mille eesmärgiks on koolitada Euroopas elavaid isikuid terrorirünnaku toimepanemiseks. Seega kui varasemalt toimusid terroristlike organisatsioonide kontrolli all olevatel territooriumidel sellised treeningud ja koolitamised, siis nüüd tehakse seda interneti vahendusel, edastades erinevaid käsiraamatuid, juhendeid või videoid. See tähendab, et radikaliseerunud isikul ei ole vajalik enam reisida.

Kuigi tehnoloogia areng aitab terroristlike rühmitusi, siis samamoodi kasutatakse tehnoloogia arengut ära terrorismivastases võitluses. Euroopas on loodud erinevaid organisatsioone ning üksusi, mis tegelevad konkreetselt terroristliku sisuga postituste ja materjalide avastamisega internetis. Suur roll terrorismivastases võitluses on lisaks riikidele ja rahvusvahelistele organisatsioonidele suurtel internetiplatvormidel, näiteks Facebook, Instagram või Google. Need internetiplatvormid suudavad iseseisvalt tuvastada ning eemaldada nendel lehtedel olevaid terroristliku sisuga postitusi. Selleks investeerivad platvormid üha rohkem tuvastamistarkvaradesse, et nende lehtedel poleks terroristliku sisuga postitusi või et sellised postitused võimalikult kiiresti oleks võimalik avastada. Käesoleva magistritöö esimeses peatükis on välja toodud statistika, kui palju terroristliku sisuga materjali internetist on leitud ja eemaldatud.

Euroopa Liidu ja liikmesriikide terrorismivastase võitluse strateegiatest nähtub, et järjest rohkem rõhutatakse terroristlikul eesmärgil interneti kasutamise tõkestamise olulisust. Strateegiates on välja toodud erinevad meetmed, mille abil tõkestada terroristliku sisuga postituste levimine. Näiteks Suurbritannias on loodud avalikkuse jaoks eraldi lehekülg, kus saavad inimesed teada anda, kui nad on leidnud mõnelt internetilehelt terroristliku sisuga materjali. Soomes ja Rootsis viiakse läbi erinevaid koolitusi ja kampaaniaid, mille eesmärk on avalikkuse teadvust internetis leiduva osas parandada. Selliste koolituste kaudu on võimalik ennetada veel enam olukordi, kus terroristliku sisuga postitused või materjalid jõuavad radikaliseerunud isikuteni. Eesti terrorismivastane strateegia on aastast 2013 ning seetõttu oleks vajalik seda strateegiat uuendada, et selles oleksid kajastatud terrorismivastase võitluse kõige uuemad meetmed ja võimalused.

Kuigi terrorismivastases võitluses on järjest paranenud võimekus tuvastada terroristliku sisuga postitusi internetis, siis ilmnes selliste postituste eemaldamise osas probleem, kuna internetiplatvormide jaoks oli vabatahtlik sellised postitused enda leheküljelt eemaldada.

Saksamaal ja Prantsusmaal on seadustega sätestatud kohustus internetiplatvormidele terroristliku sisu eemaldamiseks. Seda tuleb teha kahekümne nelja tunni jooksul alates terroristliku sisuga postituse avastamisest. Kuna internetis toimuva tõkestamiseks on vajalik, et terroristlik sisu internetis võimalikult kiiresti eemaldatakse, on oluline, et internetiplatvormid teeksid koostööd õiguskaitseorganitega. Kuid näiteks Prantsusmaal on seadustega antud võimalus õiguskaitseorganitel pöörduda kohtu poole, kui internetiplatvorm ei eemalda kahekümne nelja tunni jooksul terroristliku sisu oma leheküljelt. Prantsusmaal on võimalik meetmetena kasutada sellise lehekülje ajutist

sulgemist või täielikku blokeerimist. Eestis internetiplatvormidele sellist kohustust seadustest ei tulene. Kuigi Eestis on terrorioht üsna madal ning terroristliku sisuga materjale Eesti internetilehekülgedel on vähe, siis on oluline, et õiguskaitseorganitel oleks siiski olemas võimalused, kui peaks sellised olukorrad tekkima. Kuna Eesti toetab terrorirühmituste vastast võitlust, on ka Eesti potentsiaalne sihtmärk terroristlike rühmituste jaoks.

Euroopa Liidus on hetkel ettepaneku staadiumis määrus 2018/0331 terroristliku veebisisu levitamise tõkestamise kohta, millega kohustataks internetiplatvorme terroristliku sisu eemaldama. Lisaks kavatsetakse määrata selle määruse ettekirjutiste kohaselt internetilehekülgedele lisakohustused ning vastutused, mille tulemusena oleks võimalik paremini tõkestada terroristliku sisu levimine internetis. Näiteks luuakse internetilehekülgedele kohustus üha rohkem investeerida sellise sisu avastamist abistavatesse tarkvaradesse, lisaks on plaanis luua kohustus

Euroopa Liit on järjest rohkem rõhku pannud terroristlikul eesmärgil interneti kasutamise tõkestamiseks. Selle jaoks on loodud eraldi üksused, mis konkreetselt tegelevad terroristliku veebisisu tuvastamisega. Lisaks on Euroopa Liit on uuendanud terrorismivastaseid regulatsioone ning järjest enam viidanud interneti kasutamisele. Euroopa Liidu direktiiviga 2017/541 pöörati veel rohkem tähelepanu just terroristlikele tegevustele internetis ning selle direktiiviga reguleeritakse Euroopa Liidus ühtsemaks sellevastane võitlus. Lisaks on direktiiviga 2017/541 kriminaliseeritud terrorismialase väljaõppe saamine, mille hulka kuulub ka interneti vahendusel toimuvad treeninglaagrid ja koolitamised. Kuna terrorismi olemus on ajaga muutunud ning terroristlikud rühmitused on järjest enam hakanud uusi liikmeid värbama ja koolitama interneti vahendusel, on vajalik, et kas terrorismialase väljaõppe saamine oleks kriminaliseeritud.

Direktiivi 2017/541 mõjul on käesolevas magistritöös käsitletud Euroopa Liidu liikmesriikide terrorismi puudutavad regulatsioonid sarnased. Kõikides töös analüüsitud riikides on terrorism defineeritud terrorikuriteo kaudu. Lisaks on nende riikides kriminaliseeritud terroristlikusse ühendusse kuulumine, värbamine ning terrorikuriteo ettevalmistamine ja selle toetamine. Kuid siiski on osade sätete osas mõningaid erinevusi.

Prantsusmaal on karistusseadustikus terroriaktidele provotseerimise ja avaliku üleskutsumise sätte juures välja toodud eraldi lõige, mille kohaselt sättes välja toodud kuritegude korral, kui need pannakse toime kirjaliku või audiovisuaalse ajakirjanduse vahendusel või üldsusele internetis edastamise kaudu, kohaldatakse vastutavate isikute

kindlaksmääramiseks neid küsimusi reguleerivate seaduste erisätteid. Lisaks on Prantsusmaa karistusseadustikus välja toodud, et on tegemist terrorikuriteo ettevalmistamisega, kui isik konsulteerib veebis ühe ühe või mitme avaliku kommunikatsiooniteenusega või omab dokumente, mis provotseerivad otseselt toime panna terroriakt või mille abil on võimalik terroriakt toime panna.

Suurbritannias on terroristliku teabe kogumise all muuhulgas välja toodud, et toime on pandud kuritegu, kui inimene kogub või salvestab internetist teavet, mis võib olla kasulik terroriakti toimepanijale või ettevalmistavale isikule. Kuid Suurbritannias on kuriteoks ka terroristliku sisuga teabe vaatamine või kui isikul on juurdepääs sellisele teabele. Sellise kuriteo vabandatavateks asjaoludeks on, kui inimene polnud teadlik, et seda teavet võiks keegi kasutada terrorikuriteo toimepanemiseks või ettevalmistamiseks. Terroristliku sisuga teavet võib internetis vaadata ka ajakirjaniku töö tegemiseks või akadeemilise uurimistöö tegemiseks. Lisaks on Suurbritannias terrorismile õhutamise ning terroristliku väljaannete levitamise peatükis eraldi säte selle kohta, kui selline tegevus on toime pandud internetis.

Seega on Prantsusmaal ja Suurbritannias karistusseadustike sätetes välja toodud selged viited, et selliste tegevuste tegemine internetis on samuti kuriteoks. Eesti karistusseadustikus ei ole terrorismi puudutavate sätete juures välja toodud konkreetseid viiteid, et sellise tegevuse toime panemine internetis on samuti kuritegu, kuid see ei tähenda, et näiteks internetis tehtud üleskutse terrorikuriteo toimepanemiseks ei oleks Eestis karistatav. Kuid Eestis ei ole kriminaliseeritud terroristliku veebisisuga lehekülje külastamine või vaatamine, nagu on näiteks Suurbritannias. Karistusseadustiku § 237^2 kohaselt on karistatav terrorikuriteo toimepanemiseks väljaõppe korraldamine ning saamine. Selline tegevus on karistatav ka juhul, kui väljaõppe korraldamine või saamine toimub interneti vahendusel. Kuid see säte ei hõlma selliseid olukordi, kus isik külastab terroristliku sisuga internetilehekülge ning ta on teadlik, et tegemist on terroristliku rühmituse poolt postitatud sisuga. Kuna selline käitumine võib samuti olla terrorikuriteo ettevalmistamine, siis võimaldaks see õiguskaitseasutustel veelgi varem ning efektiivsemalt terroriohule reageerida.

Problems Originating from the Internet in the Fight Against Terrorism

Terrorism is a current problem for European and global security in the 21st century. The number of terrorist attacks in Europe has increased in recent years and the terrorist threat in Europe remains high. In 2015, there were counted a total of 211 terrorist attacks in Europe, including failed or prevented attacks in addition to those completed. There were 142 of such attacks in 2016, 205 in 2017 and 129 in 2018. The largest number of attacks occurred in Great Britain and France. Despite the fact that terrorist groups have weakened as a result of the active fight against terrorism, they have large international networks via which to continue their operations. It is important for the combat against terrorism to understand the ongoing situation and the primary challenges.

The aim of the hereby Master's thesis is to identify how the Internet is instrumentalised for terrorist purposes, how it is battled and whether and how the use of the Internet for terrorist purposes is regulated in Estonian law. In order to achieve the set goal, the following research questions have been posed:

1. To what extent do terrorist groups use the Internet to fulfil their own purposes?
2. What are the reasons for which terrorist groups use the Internet?
3. What problems does the use of the Internet by terrorist groups cause?
4. Is there a fight against terrorist groups on the Internet and to what extent?
5. What are the legal options for preventing the use of the Internet by terrorist groups?
6. Does Estonia have anything to learn or take over from the law of the European Union member states on the fight against terrorism examined in this master's thesis?

In addition to Estonian counter-terrorism strategy and regulations, the work will also analyse the counter-terrorism regulations and strategies set by the European Union and the European Union member states, such as Sweden, Finland, France, Great Britain and Germany.

Cooperation between countries and organisations is a crucial criterion in the fight against terrorism. For cooperation to work successfully, it is required to find a joint definition of terrorism. The definition of terrorism dates back to the first half of the 20th century, but so far it has not been possible to find an internationally common definition of terrorism. The legislation of the European Union and the Member States of the European Union defines

terrorism by explaining the concept of a terrorist offense. The legislation sets out specific criteria and a list of crimes that are considered terrorist offenses.

The essence of terrorism has changed throughout history and terrorist groups are striving to adapt to changing conditions in society. Terrorist organizations have been deprived of large territories under their control due to the fight against terrorism. As a result, it is no longer the territory that is important to terrorist groups, but their ideology. Terrorist groups in Europe are progressively launching attacks to prove to Western countries that they are still capable of executing such operations. Terrorist attacks in Europe have become simplistic, using less complex means, while they are carried out by radicalized individuals living in Europe.

Technological progress offers new opportunities for terrorists. With the development of technology, chances have been created to produce more and more powerful and dangerous weapons. However, the Internet is the most widely abused instrument by terrorist groups. The Internet is a fast, easy, cheap and anonymous environment where members of terrorist groups can interact with each other. Terrorists do not use the Internet mainly as a weapon to attack targets, but rather as a resource. In conjunction with communication purposes, terrorist groups use the Internet to disseminate violent propaganda, recruit new members, train them and provide guidance. With the help of the Internet, terrorist groups can mobilise new members from Europe and train novel members to commit a terrorist attack via the Internet. Terrorists have developed sophisticated encryption tools that allow them to interact between them. As a consequence, they are able to operate an international network, which means that the terrorist threat, both in Europe and on a global basis, stays constantly high.

There is an active fight against the activities of terrorist groups. In the Middle East, they have managed to reduce the territories controlled by terrorist organizations, which has undermined the activities of such groups. In the fight against terrorism, great attention has been paid to restricting the use of the Internet for terrorist purposes. To this end, international entities and organizations have been created to actively combat terrorism on the web. With the help of technology and in cooperation with online platforms, it is possible to quickly identify terrorist content on the Internet. Net platforms have software that allows them to detect posts with terrorist content and remove them as promptly as possible. One important criterion in the fight against terrorist content on the Internet is that such posts be identified and removed at the earliest opportunity. The longer a post with

terrorist content is on a website, the more people will be able to view it. Terrorist groups use the Internet to engage new members and spread their propaganda and therefore, these posts are intended to reach as large an audience as possible.

In the European Union's fight against terrorism, there has been a growing emphasis on blocking certain Internet activities. A separate unit has been set up in the European Union, the utmost task of which is to battle radicalization on the Internet more effectively. As technology and the development of the Internet have created a fertile ground for terrorist groups to divulge their opinions to achieve their goals or employ and train new members, up-to-date legislation and strategies are needed to defeat it. The strategies of all the countries examined in this work show that prevention is appropriate to solve this issue, but the countries have arranged it somewhat differently. Prevention may avoid major terrorist attacks, but also radicalization and the recruitment of new members of terrorist groups. In Sweden, the Media Council has specifically prepared digital learning material that seeks to boost people's ability to challenge anti-democratic and violent messages on the Internet and social media. Similar trainings are held in Finland too. In Great Britain, a separate webpage has been established, where people can report terrorist posts. Such preventive measures contribute to the war against terrorism on the Internet. Major public attention to the distribution of terrorist content on the Internet will help to discover and spot even more such content. The more and quicker terrorist content is singled out and removed on the Internet, the fewer people it will address.

The anti-terrorism provisions in the European Union have changed over time. In 2017, the Directive 2017/541 on combating terrorism was adopted, replacing the Council Framework Decision 2002/475 / JHA. One of the aims of this directive was to harmonise the definition of terrorist attacks, terrorist groups and criminal offenses relating to terrorist activity and further states that such activities should be punishable even if they are committed via the Internet, including social media. Directive 2017/541 refers to the Internet to greater extent. For example, Article 5, which governs public provocation to commit a terrorist offense, cites that such conduct is punishable if it is committed in any way whatsoever, whether it is online or offline.

In the battle against terrorism, the problem of blocking terrorist content on the Internet was raised, as Internet platforms did not have a legal obligation to remove terrorist content from their site. To this reason, France and Germany have introduced legislation allowing for the removal of terrorist content from online platforms within 24 hours of the discovery

of such content. If this obligation is not complied with, in France, for instance, the law allows the temporary closure of an online platform or the removal of a specific post as a temporary measure. In both France and Germany, fines have been imposed for non-compliance with such an obligation. The NetzDG law requires German internet platforms to remove posts within twenty-four hours which contain terrorism-related content. The law concerns internet platforms that have a minimum of two million registered users in Germany. Terrorist organisations strive to reach as many people as possible with their posts, which is why it is primarily important to concentrate on platforms with larger user bases.

No similar legal basis currently exists in Estonia. § 111^1 of the Electronic Communications Act requires communications companies and providers of telephone and mobile phone services, telephone and mobile phone network services, internet access, electronic mail services, and internet telephony services to preserve data; § 112 stipulates the obligation to provide information, and § 113 the obligation to grant access to communications networks. These obligations help law enforcement authorities to detect posts and material which contain terrorism-related content, but service providers are not obliged to remove terrorism-related content that is found online. The spread of terrorism-related information is currently not a significant problem in Estonia but, given that Estonia supports counterterrorism activities, the country is a potential target for terrorism-related organisations. The Estonian Security Police yearbook indicates that both radicalised people in Estonia and those who visit the country pose a terrorist threat to Estonian security. The Internal Security Service has identified around twenty people who are living in or who are tightly connected to Estonia who, if further radicalised, could pose a threat to national security. Led by such people, the internet could be used to further the terrorist agenda in Estonia. Germany and France are examples of countries in which internet platforms are required by law to remove such posts and material to help prevent terrorism. The faster such posts and material is removed, the fewer people the information in the posts reaches.

Regulation 2018/0331 on the prevention of the distribution of terrorist online content is being drafted in the European Union. The goal of this regulation is to ensure even faster elimination of terrorist online content, and the Member States of the European Union would have a common legal framework for removing terrorist content on the Internet. This regulation would give Internet platforms a greater responsibility and obligation to discharge such contents from their own platform, thus making the internet safer for the

average user. However, in the context of this regulation, the proportionality of all obligations to online platforms must be considered, as such obligations may infringe on freedom of establishment and that of expression.

A comparison of the anti-terrorism provisions in the Estonian Penal Code and the provisions of other countries which have been observed in the thesis reveals that provisions in all countries deal with similar activities that have been criminalised in those countries. Estonian law contains no provisions for situations in which an individual visits an online website that contains terrorism-related materials. §237^2 of the Penal Code concerns terrorist training, including self-study, which refers to situations in which an individual receives educational materials that are geared towards committing or aiding in a terrorist attack by a terrorist organisation via the internet or other means. As such, self-study presumes prior communication with a terrorist organisation.

The UK Terrorism Act 2000 criminalises visiting or viewing a site with terrorist content. There are two exculpatory criteria. First, if the person was not aware of the contents of the page, it could be used by a member of a terrorist organization to commit or prepare for a terrorist offense. Secondly, such webpages may be viewed for journalistic or academic research writing purposes.

Visiting a website that contains terrorism-related content does not necessarily mean self-study. Although the website may be used in such areas as, for example, learning to manufacture explosives, it is important to determine the aim of visiting the website. People generally find themselves on such websites by accident, without understanding that the website's content could be used to commit a terrorism-related crime. Since the terrorist threat remains high in Europe - primarily due to online radicalisation - the spread of posts with terrorism-related content must be impeded with the help of all available measures.

Kasutatud materjalid

Kasutatud kirjandus

1. Bertram, L. Terrorism, the Internet and the Social Media Advantage: Exploring how terrorist organizations exploit aspects of the internet, social media and how these same platforms could be used to counter-violend extremism. – Journal for Deradicalization, Summer 2016 nr 7.
2. Biller, J.T. Cyber-Terrorism: Finding a common starting point. – Journal of Law, Technology & The Internet, Vol 4, No 2, 2013.
3. Bruce, G. Definition of Terrorism – Social and Political Effects. – Journal of Military and Veterans' Health, Volume 21 No. 2. 2013.
4. Cohen-Almagor, R. The Role of Internet Intermediaries in Tackling Terrorism Online. – Fordham Law Review 86, no. 2, November 2017.
5. Ganor, B. Defining Terrorism: Is One Man's Terrorist Another Man's Freedom Fighter? – Police Practice and Research: An International Journal. Volume 3, 2002
6. Hoffman, B. Inside terrorism. New York; Columbia University Press, 2013.
7. Holms, J.P. Burke, T. Terrorism: Tänapäeva suurim oht vabadusele. Tallinn: Ersen 2002.
8. Klabbers, J. Rahvusvaheline õigus. Tallinn: Juura 2018.
9. Levitt, G. Is Terrorism Worth Defining. – Ohio Northern University Law Review 13, no. 1. 1986.
10. Mockaitis, T.R. The "New" Terrorism: Myths and Reality. London: Praeger Security International, 2007.
11. Paunovic, N. New EU Criminal Law Approach to Terrorist Offences. – EU and Comparative Law Issues and Challenges Series 2, no. 2. 2018.
12. Rapoport, D.C; Cronin, A.K.; Ludes, J.M. Four Waves of Modern Terrorism. – Attacking Terrorism: Elements of a Grand Strategy. Washington DC: Georgetown University Press 2004.
13. Sedgewick, M. Inspiration and the Origins of Global Waves of Terrorism. – Studies in Conflict & Terrorism, Volume 30. 2007.
14. Schmid, A. P. The Way Forward on Counter-Terrorism: Global Perspectives. – Strathmore Law Journal 2. 2016.

15. Sootak, J. Pikamäe, P (koostajad). Karistusseadustik. Kommenteeritud väljaanne. 4 vlj. Tallinn: Juura 2015.
16. Värk, R. Riikide enesekaitse ja kollektiivse julgeolekusüsteemi võimalikkusest terroristlike mitteriiklike rühmituste kontekstis. Doktoritöö. Juhendaja Raul Narits. Tartu Ülikooli Kirjastus, 2011.
17. Weimann, G. Terror on the Internet: The New Arena, the New Challenges. Washington, DC: Endowment of the United States Institute of Peace, 2006.
18. Yu, J. Regulation of Social Media Platforms to Curb ISIS Incitement and Recruitment: The Need for an International Framework and Its Free Speech Implications. – Journal of Global Justice and Public Policy, vol. 4, no. 1, Spring 2018.

Kasutatud õigusaktid

19. Brottsbalken (The Swedish Criminal Code). SFS 1962:700. – Arvutivõrgus: https://www.government.se/government-policy/judicial-system/the-swedish-criminal-code/
20. Code pénal (Penal Code). – Arvutivõrgus: https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719
21. Code de procédure pénale. – Arvutivõrgus: https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071154
22. Counter-Terrorism and Border Security Act 2019. 2019 c.3. – Arvutivõrgus: http://www.legislation.gov.uk/ukpga/2019/3/contents
23. Décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique. NOR: INTX1502813D. – Arvutivõrgus: https://www.legifrance.gouv.fr/eli/decret/2015/2/5/INTX1502813D/jo/texte
24. Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG). BGBl. I S. 3352. – Arvutivõrgus: https://www.gesetze-im-internet.de/netzdg/NetzDG.pdf
25. Elektroonilise side seadus. – RT I, 08.01.2020, 4.

26. Euroopa Parlamendi ja Nõukogu direktiiv (EL) 2017/541 terrorismivastase võitluse kohta, millega asendatakse nõukogu raamotsus 2002/475/JSK ning muudetakse nõukogu otsust 2005/671/JSK – ELT L 88/6, 15.03.2017
27. Euroopa Liidu Nõukogu raamotsus 2002/475/JSK terrorismivastase võitluse kohta. – L 164/3, 13.06.2002
28. Euroopa Liidu Nõukogu raamotsus 2008/919/JSK, millega muudetakse raamotsust 2002/475/JSK terrorismivastase võitluse kohta. – L 330/21, 28.11.2008
29. Karistusseadustik – RT I, 28.02.2020, 5.
30. Lag om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet (Act on Criminal Responsibility for Public Provocation, Recruitment and Training concerning Terrorist Offences and other Particularly Serous Crime). SFS 2010:299. – Arvutivõrgus: https://www.government.se/government-policy/judicial-system/act-on-criminal-responsibility-for-public-provocation-recruitment-and-training-concerning-terrorist-offences-and-other-particulary-serious-crime/
31. Lag om straff för terroristbrott (Act on Criminal Responsibility for Terrorist Offences). SFS 2003:148. – Arvutivõrgus: https://www.government.se/government-policy/judicial-system/act-on-criminal-responsibility-for-terrorist-offences-2003148/
32. League of Nations. Convention pour la prévention et de la répression du terrorisme/ Convention for the Prevention and Punishment of Terrorism, 1937.
33. Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. NOR: ECOX0200175L. – Arvutivõrgus: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164
34. Strafgesetzbuch – StGB (German Criminal Code). BGBl. I S. 3322. – Arvutivõrgus: https://www.gesetze-im-internet.de/stgb/StGB.pdf
35. Terrorism Act 2000. 2000 c.11. – Arvutivõrgus: http://www.legislation.gov.uk/ukpga/2000/11/contents
36. Terrorism Act 2006. 2006 c.11. – Arvutivõrgus: http://www.legislation.gov.uk/ukpga/2006/11/contents
37. Terrorismi ennetamise Euroopa Nõukogu konventsioon. – RT II 2009, 10, 24.
38. Terrorismi rahastamise tõkestamise rahvusvaheline konventsioon – RT II 2002, 12, 45.

Kohtupraktika

39. RKKKo 10.04.2017, 3-1-1-101-16

Muud kasutatud materjalid

40. Apologie du terrorisme – Provocation au terrorisme. Direction de l'information legale et administrative (Premier minister), Ministere charge de la justice. – Arvutivõrgus: https://www.service-public.fr/particuliers/vosdroits/F32512 (26.04.2020)
41. Council of Europe: Ministers'Deputies. Counter-Terrorism Strategy (2018-2022). 04.07.2018. – CM (2018)86
42. Counter Extremism Project. Germany: Extremism & Counter-Extremism. Report. – Arvutivõrgus: https://www.counterextremism.com/countries/germany (26.04.2020).
43. Counter Extremism Project, The Eglyho Web Crawler: ISIS Content on Youtube, 2018 – Arvutivõrgus:https://www.counterextremism.com/sites/default/files/eGLYPH_web_crawler_white_paper_July_2018.pdf (15.03.2020).
44. Counter Terrorism Policing, Report Suspicious Activity. – Arvutivõrgus: https://act.campaign.gov.uk/
45. Daily Mail, Terrorism 2018: Al Qaeda uses Google Maps to plan a terrorist attack in new propaganda video that features a former Guantanamo prisoner. 21.04.2018. – DailyMail. Arvutivõrgus: https://www.dailymail.co.uk/news/article-5642361/Al-Qaeda-appears-use-Google-Maps-plan-terrorist-attack-new-propaganda-video.html (10.02.2020).
46. Eesti Kaitsepolitseiamet. Kaitsepolitseiameti aastaraamat 2019. Tallinn: Kaitsepolitseiamet 2019.
47. Eesti Kaitsepolitseiamet. Kaitsepolitseiameti aastaraamat 2018. Tallinn: Kaitsepolitseiamet 2018.
48. Eesti Kaitsepolitseiamet. Olukord Eestis. – Arvutivõrgus: https://kapo.ee/et/content/olukord-eestis-1.html (27.02.2020).
49. Eesti Kaitsepolitseiamet. Terrorismi mõiste. – Arvutivõrgus: https://kapo.ee/et/content/terrorismi-mõiste.html (27.02.2020).
50. Eesti Kaitsepolitseiamet. Terrorismi liigid – Arvutivõrgus: https://www.kapo.ee/et/content/terrorismi-liigid.html (13.01.2020).

51. Eesti Vabariigi Valitsus. Eesti terrorismivastase võitluse põhialused (2013). Heaks kiidetud Vabariigi Valitsuse poolt 14.11.2013 istungi protokollilise otsusega nr 47 pp nr 5. – Arvutivõrgus: https://www.siseministeerium.ee/sites/default/files/dokumendid/tvv_pohialused_2013.pdf
52. Euroopa Komisjon, Euroopa Liidu olukord 2018 – komisjon esitab terroristliku veebisisu eemaldamise uute eeskirjade ettepaneku. – Arvutivõrgus: http://europa.eu/rapid/press-release_IP-18-5561_et.htm (20.04.2020).
53. Euroopa Parlament. Terrorism Euroopa Liidus: arvud ja faktid. – Arvutivõrgus: https://www.europarl.europa.eu/news/et/headlines/priorities/terrorism/20180703STO07125/terrorism-euroopa-liidus-arvud-ja-faktid (27.02.2020).
54. Euroopa Ülemkogu, Euroopa Liidu Nõukogu. ELi terrorismivastane võitlus. – Arvutivõrgus: https://www.consilium.europa.eu/et/policies/fight-against-terrorism/ (10.04.2020).
55. European Union Agency for Law Enforcement Cooperation. European Union Terrorism Situation and Trend Report 2019. Haag: European Union Agency for Law Enforcement Cooperation 2019 – Arvutivõrgus: https://www.europol.europa.eu/activities-services/main-reports/terrorism-situation-and-trend-report-2019-te-sat (10.04.2020).
56. European Union: Council of the European Union. The European Union Counter-Terrorism Strategy. 30.11.2005. – 14469/4/05 REV 4.
57. Europol: EU Internet Referral Unit. Year one report – highlights. – Arvutivõrgus: https://www.europol.europa.eu/publications-documents/eu-internet-referral-unit-year-one-report-highlights (20.04.2020).
58. Europol. European Counter Terrorism Centre. – Arvutivõrgus: https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc (30.03.2020).
59. Europol. Europol’s internet referral unit to combat terrorist and violent extremist propaganda. – Arvutivõrgus: https://www.europol.europa.eu/newsroom/news/europol%E2%80%99s-internet-referral-unit-to-combat-terrorist-and-violent-extremist-propaganda (30.03.2020).
60. Europol. More than 900 instances of online terrorist propaganda uncovered. (16.03.2018). – Arvutivõrgus:

https://www.europol.europa.eu/newsroom/news/more-900-instances-of-online-terrorist-propaganda-uncovered (02.04.2020).

61. Finnish Security Intelligence Service. Supo Year Book 2018. – Arvutivõrgus: https://www.supo.fi/instancedata/prime_product_julkaisu/intermin/embeds/supowwwstructure/77291_WWW_SUPO_Juhlakirja_70_2019_ENG.pdf?52e507f9e2d6d788 (15.04.2020).
62. France Premier Ministre. Action Plan Against Terrorism. 13.07.2018 – Arvutivõrgus: http://www.sgdsn.gouv.fr/uploads/2018/10/20181004-plan-d-action-contre-le-terrorisme-anglais.pdf (20.04.2020).
63. French Foreign Policy. Terrorism: France's International Action. – Arvutivõrgus: https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/terrorism-france-s-international-action/ (20.04.2020).
64. Interpol. Analysing social media. – Interpol. Arvutivõrgus: https://www.interpol.int/Crimes/Terrorism/Analysing-social-media (20.03.2020).
65. Kaplan, E. Terrorists and the Internet – Council on Foreign Relations. Arvutivõrgus: https://www.cfr.org/backgrounder/terrorists-and-internet (15.03.2020).
66. Karistusseadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seadus (terrorismivastase võitluse direktiivi ülevõtmine) 642 SE. Seletuskiri karistusseadustiku ja sellega seonduvalt teiste seaduste muutmise seaduse (terrorismivastase võitluse direktiivi ülevõtmine) eelnõu juurde. – Arvutivõrgus: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/af992ccb-58f7-4a6e-bef5-d8f82772b3b7/Karistusseadustiku%20muutmise%20ja%20sellega%20seonduvalt%20teiste%20seaduste%20muutmise%20seadus%20(terrorismivastase%20v%C3%B5itluse%20direktiivi%20%C3%BClev%C3%B5tmine) (10.04.2020).
67. Katz, R. How Terrorists Slip Beheading Videos Past YouTube's Censors. – Arvutivõrgus: https://motherboard.vice.com/en_us/article/xyepmw/how-terrorists-slip-beheading-videos-past-youtubes-censors (14.04.2020).
68. Majandus- ja Kommunikatsiooniministeerium. Küberturvalisuse strateegia 2019-2022. – Arvutivõrgus: https://www.mkm.ee/sites/default/files/kuberturvalisuse_strateegia_2019-2022.pdf (10.04.2020)

69. Ministry of the Interior, Finland. Counter-terrorism measures in Finland. – Arvutivõrgus: https://intermin.fi/en/police/counter-terrorism/counter-terrorism-measures-in-finland (24.03.2020).
70. Ministry of the Interior, Finland. Cybercrime - Information networks and crime. – Arvutivõrgus: https://intermin.fi/en/police/cybercrime (24.03.2020).
71. Ministry of the Interior, Finland. National Counter-Terrorism Strategy 2018-2021. Internal security. Ministry of the Interior publications 28/2018. Helsinki 2018 – Arvutivõrgus: https://julkaisut.valtioneuvosto.fi/handle/10024/161188 (15.04.2020).
72. North Atlantic Treaty Organization. Combined Joint Chemical, Biological, Radiological and Nuclear Defence Task Force. – Arvutivõrgus: https://www.nato.int/cps/en/natohq/topics_49156.htm (15.02.2020).
73. North Atlantic Treaty Organization. Defence Against Terrorism Programme of Work. – Arvutivõrgus: https://www.nato.int/cps/en/natohq/topics_50313.htm (15.02.2020).
74. North Atlantic Treaty Organization. Weapons of mass destruction. – Arvutivõrgus: https://www.nato.int/cps/en/natohq/topics_50325.htm (15.03.2020).
75. Office of the United Nations. High Commissioner for Human Rigts. Human Rights, Terrorism and Counter-terrorism. Fact Sheet no. 32. – Arvutivõrgus: https://www.refworld.org/docid/48733ebc2.html (10.02.2020).
76. Parliament by the Secretary of State for the Home Department by Command of Her Majesty. The United Kingdom's Strategy for Countering Terrorism. 06.2018. Cm 9608. – Arvutivõrgus:https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf (10.04.2020).
77. Postimees. Mošeeründaja: radikaliseerusin pärast Marine Le Peni lüüasaamist. 15.03.2019. – Postimees. Arvutivõrgus: https://www.postimees.ee/6545788/moseerundaja-radikaliseerusin-parast-marine-le-peni-luuasaamist (20.03.2020).
78. Postimees. Süürias andsid alla tunnelitest välja ilmunud džihadistid (24.03.2019). – Postimees. Arvutivõrgus: https://www.postimees.ee/6552732/suurias-andsid-alla-tunnelitest-valja-ilmunud-dzihadistid (20.03.2020).

79. Riigikogu. Eesti julgeolekupoliitika alused. – RT III, 06.06.2017, 2. Riigikogu otsuse „Eesti julgeolekupoliitika alused“ heakskiitmine. Lisa.
80. Ritchie, H.; Hasell, J.; Appel, C.; Roser,M. Terrorism. – Arvutivõrgus: https://ourworldindata.org/terrorism (15.02.2020).
81. Security Service MI5. International Terrorism - Terrorist training and indoctrination. – Arvutivõrgus: https://www.mi5.gov.uk/terrorist-training-and-indoctrination (15.04.2020).
82. Seletuskiri. Ettepanek: Euroopa Parlamendi ja Nõukogu määrus terroristliku veebisisu levitamise tõkestamise kohta. 12.09.2018. 2018/0331 (COD). – Arvutivõrgus: https://ec.europa.eu/transparency/regdoc/rep/1/2018/ET/COM-2018-640-F1-ET-MAIN-PART-1.PDF (15.03.2020).
83. Siseministeerium. Terrorismivastane võitlus. – Arvutivõrgus: https://www.siseministeerium.ee/et/eesmark-tegevused/sisejulgeoleku-tagamine/terrorismivastane-voitlus (25.03.2020).
84. Sweden. Agreement on counter-terrorism measures. 07.06.2017 – Arvutivõrgus: https://www.government.se/49f005/contentassets/2f681fbd159d451795b744523a96f955/Agreement-on-anti-terrorism-measures.pdf (25.04.2020).
85. Teabeamet. Eesti rahvusvahelises julgeolekukeskkonnas 2017. (Tallinn: Teabeamet 2017) – Arvutivõrgus: https://www.valisluureamet.ee/pdf/TA_raport_2017_EST.pdf (15.04.2020).
86. Terrorismi ennetamise Euroopa Nõukogu konventsiooni lisaprotokoll. – L 159/17, 22.10.2015.
87. The NYU Dispatch. Is technology helping or hindering the fight against terrorism? (15.12.2017) – The NYU Dispatch. Arvutivõrgus: https://wp.nyu.edu/dispatch/2017/12/15/is-technology-helping-or-hindering-the-fight-against-terrorism/ (14.03.2020).
88. Tworek, H. Leerssen, P. An Analysis of Germany’s NetzDG Law. 15.04.2019 – Arvutivõrgus: https://www.ivir.nl/publicaties/download/NetzDG_Tworek_Leerssen_April_2019.pdf (20.04.2020).
89. Välisministeerium. Eesti Euroopa Liidus. – Arvutivõrgus: https://vm.ee/et/eesti-euroopa-liidus (26.03.2020).

90. Välisministeerium. Julgeolekupoliitika – küberjulgeolek. – Arvutivõrgus: https://vm.ee/et/tegevused-eesmargid/julgeolekupoliitika/kuberjulgeolek (26.03.2020).
91. Välisluureamet. Eesti rahvusvahelises julgeolekukeskkonnas 2019. Tallinn: Välisluureamet 2019 – Arvutivõrgus: https://www.valisluureamet.ee/pdf/raport-2019-EST-web.pdf (14.04.2020).