Sisekaitseakadeemia

Finantskolledž

Eduard Tšornõi

SOTSIAALMEEDIA ROLL KÜBERKURITEGEVUSE VAHENDAJANA

Lõputöö

Juhendaja:

Helle Koitla,

magistrikraadile vastav kvalifikatsioon

Tallinn 2019

SISEKAITSEAKADEEMIA LÕPUTÖÖ ANNOTATSIOON

Finantskolldež	Juuni 2019

Töö pealkiri eesti keeles: Sotsiaalmeedia roll küberkuritegevuse vahendajana

Töö pealkiri võõrkeeles: The role of social media as an intermediary in cybercrime

Töö on kirjutatud eesti keeles ja koosneb 51 leheküljest. Töös on kasutatud 68 allikat, millele on viidatud. Teema on aktuaalne, kuna sotsiaalmeedia kasutamine on kasvavas trendis. Peaagu kõigil Euroopas elavatel on mingigi kokkupuude sotsiaalvõrgustikega, kes kasutab seda sõprade ja sugulastega ühenduses hoidmiseks kes aga ärilisteks eesmärkideks näiteks müües kaupa või teenuseid. See viimane osa sisaldab ka endas ärilist tegevust, mis läheb vastuollu seadustega, olgu see siis rahavargus, ebaseadusliku sisu levitamine või isiku andmete kasutamine kuritegelikel eesmärkidel. Töö probleemiks on püstitatud küsimus, kuidas vähendada sotsiaalmeedias toimuvate ebaseaduslikude tegevuste mõjud ühiskonnale? Lõputöö eesmärgiks on anda võimalikke meetmeid kuritegevuse ennetamiseks sotsiaalmeedias. Lõputöö eesmärgi saavutamiseks püstitati järgmised uurimisülesanded:

1. Anda ülevaade ebaseadusliku tegevusest sotsiaalmeedias.
2. Anda ülevaade sotsiaalvõrgustikkude funktsionaalsusest.
3. Analüüsida sotsiaalmeedia mõju küberturvalisusele.
4. Analüüsida sotsiaalmeedia kõige levinumaid kuriteo skeeme.

Töös Analüüsitakse kirjalikke dokumente (päevikud, meediatekstid, programmi kirjeldused ja tegevused, kirjalikud intervjuud, meediaväljaanded, koolikirjandid, veebileheküljed). Esitatakse väljavõtted, tsitaadid, dokumentide viited. Andmete analüüsil otsitakse seaduspärasusi. Infovajaduste uurimise viisiks on ekspertintervjuu ja küsitlus. Samuti analüüsitakse ka Küberturvalisuse seaduse ja Euroopa komisjoni õigusakte. Töös kasutatakse kvalitatiivset uurimismeetodit.

Võtmesõnad: sotsiaalmeedia, sotsiaalvõrgustik, küberkuritegevus, küberturvalisus

Võõrkeelsed võtmesõnad: social media, social network, cybercrime, cybersecurity

Säilitamise koht: Sisekaitseakadeemia raamatukogu

Töö autor: Eduard Tšornõi

Olen koostanud lõputöö iseseisvalt. Kõik lõputöö koostamisel kasutatud teiste autorite tööd, seisukohad, kirjalikest allikatest ja mujal allikates saadud info on nõuetekohaselt viidatud. Olen nõus oma lõputöö avaldamisega elektroonilises keskkonnas.

Allkiri:

Vastab lõputöö nõuetele

Juhendaja: Helle Koitla Allkiri:

Kaitsmisele lubatud

Kolledži direktor /
instituudi juhataja: Kerly Randlane Allkiri:

SISUKORD

SISSEJUHATUS

Sotsiaalmeedia on leidmas üha laiemat kasutust igapäevaelus. Tavalisele inimesele on sotsiaalmeedia midagi muud kui sidevahend, uudiste lugemine ja mõtete või ideede avaldamine. Sotsiaalmeedia keskkond on aja jooksul muutunud ka efektiivseteks kauplemisplatvormideks, kus kasutajad saavad oma kaupu ja teenuseid paigutada, hindade üle rääkida või asju osta. Kuid kohas, kus on palju kasutajaid, suhtlemisvõimalusi ning on võimalik oma tegelikku identiteeti varjata, ilmub reeglina ka seadusetus. Infotehnoloogia arendamisega kaasnevad uued küberkuritegevuse viisid, kuid enamik inimesi ei tea, millised ohud sellest tulenevad ja kuidas end internetis kaitsta. Lõputöö keskendub sotsiaalmeedia põhiosale, ehk sotsiaalvõrgustikudele. On teada, et Instagram'is registreeritud kasutajate arv 2018. aastal on 1,1 miljardit ja Facebook'i kasutajate arv on 2,13 miljardit. On ka teisi sotsiaalvõrgustikke, mida kasutavad miljonid kasutajad. Käesolevas töös analüüsitakse neid sotsiaalvõrgustikke, mis on täna kõige asjakohasemad ja populaarsemad, mis võimaldab teha nähtavaks sotsiaalmeedia ebaseadusliku kasutamisega kaasnevad ohud ühiskonnale.

Töö teema on aktuaalne, kuna sotsiaalmeedia kasutamine on kasvavas trendis. Peaagu kõigil Euroopas elavatel on mingigi kokkupuude sotsiaalvõrgustikega, kes kasutab seda sõprade ja sugulastega ühenduses olemiseks, kes aga ärilisteks eesmärkideks, näiteks - müües kaupa või teenuseid. See viimane osa sisaldab ka endas tegevust, mis on vastuolus seadustega, olgu see siis rahavargus, ebaseadusliku sisu levitamine või isiku andmete kasutamine kuritegelikel eesmärkidel.

Lõputöö peamiseks uurimisobjektiks on valitud maailma suurim sotsiaalmeedia platvorm Facebook, kuid vaadeldakse ka teisi platvorme, nagu Twitter, Instagram ja YouTube.

Lõputöö probleemiks on püstitatud küsimus, kuidas vähendada sotsiaalmeedias toimuvate ebaseaduslikude tegevuste mõjusid ühiskonnale?

Lõputöö eesmärgiks on tuvastada võimalikke meetmeid kuritegevuse ennetamiseks sotsiaalmeedias.

Eesmärgi täitmiseks on püstitatud järgmised uurimisülesanded:

1. Anda ülevaade ebaseaduslikust tegevusest sotsiaalmeedias.
2. Anda ülevaade sotsiaalvõrgustikkude funktsionaalsusest.
3. Analüüsida sotsiaalmeedia mõju küberturvalisusele.
4. Analüüsida sotsiaalmeedia kõige levinumaid kuriteo skeeme.

Töös kasutatakse kvalitatiivset uurimismeetodit. Analüüsitakse kirjalikke dokumente (programmi kirjeldused ja tegevused, kirjalikud intervjuud, meediaväljaanded ja tekstid, veebileheküljed). Esitatakse väljavõtted, tsitaadid, dokumentide viited. Andmete analüüsil otsitakse seaduspärasusi. Infovajaduste uurimise viisiks on ekspertintervjuu ja Google docs küsimustik. Samuti analüüsitakse ka küberturvalisuse seadust ja Euroopa komisjoni õigusakte.

Töö esimeses osas antakse ülevaade sotsiaalmeedia olemusest ning funktsionaalsusest. Esimeses alapeatükis antakse ülevaade sotsiaalvõrgustike tehnilisest sisust ning teises alapeatükis antakse ülevaade sotsiaalvõrgustikkude funktsionaalsuse kasutamisest kuritegelikel eesmärkidel.

Töö teises peatükis antakse ülevaade küberkuritegude toimepanemise viisidest ja ennetamise meetmetest. Esimeses alapeatükis analüüsitakse küsitluse ja ekspertintervjuu vastuseid. Samuti käsitleb autor kõige levinumaid küberkuritegevuse liike sotsiaalmeedia kaudu, nende mõjudest ühiskonnale ja küberturvalisusele. Teises alapeatükis tuvastatakse võimalikke meetmeid kuritegevuse ennetamiseks sotsiaalmeedias.

1. SOTSIAALMEEDIA ÜLDINE KONTSEPTSIOON

1.1 Sotsiaalvõrgustike olemus

Üle miljardi kasutaja kogu maailmas on aktiivselt võrgustunud Facebooki kaudu, mis on üks tuntumaid sotsiaalvõrgustiku teenuseid, et edendada kasutajate sotsiaalset internetipõhist olemasolu ja ühendusi. Sotsiaalvõrgustike teenused pakuvad tõhusaid vahendeid sotsiaalse kapitali loomiseks, kuna need võimaldavad kasutajatel arendada uusi ühendusi ja laiendada oma isiklikke võrke. Siinkohal võib püsiva sotsiaalvõrgustiku omamine anda võrgus osalejatele muidu kättesaamatuid ressursse, näiteks juurdepääsu teabele, rahalist kasu ja psühholoogilist heaolu (Kwak & Kim, 2017, pp. 1-16). Inimelu täna on tihedalt seotud sotsiaalmeediaga. Seda on võimalik kasutada erinevatel eesmärkidel, kuid peamiseks on suhtlemine.

Ilma veebi ja internetita oleks sotsiaalvõrgustiku saite võimatu kasutada. Seega on vajalik teha arusaadavaks veebi ja interneti mõiste. „Veeb" on termin, mille all mõistetakse üleilmselt jagatud infosüsteemide võrgustikku teabevahetuseks internetis. Interneti ja veebi vahel on suur erinevus, kuid neid tihti samastatakse. Internet on globaalne süsteem omavahel ühendatud arvutivõrkudest ning erinevad nad selles, et veeb on rakendus, mis töötab ühe osana internetis. See on maailma suurim andmebaas ehk kogumik omavahel ühendatud dokumentidest ja teistest ressurssidest, mis on seotud linkide ja URL-ide abil (Priit, 2010). Uniform Resource Locator (URL) on internetis oleva ressursi aadress. URL näitab ressursi asukohta ja sellele ligipääsuks kasutatavat protokolli. Internet ja sotsiaalmeedia on lahutamatu osa, seega tuleb selgeks teha ka interneti olemust.

Internet on laiendanud inimeste võimalusi suhelda. (Ellison, *et al*., 2014, pp. 855). Sotsiaalvõrgustike (Facebook, Twitter, Instagram) kasutamine on viimase kümne aasta jooksul suurenenud. Grieve, Indian, Witteveen, Tolan & Marrington (2013, pp. 604-609) sõnul sotsiaalvõrgustikkude massiivsel kasutamisel arendavad ja säilitavad inimesed sidemeid ja sotsiaalset sidet võrgukeskkonnas, kogedes positiivseid psühholoogilisi tulemusi, näiteks suuremat rahulolu eluga. Sosik & Bazarova (2014, pp. 124-131) leidsid, et sotsiaalvõrgustike kasutamine on inimeste suhete eskaleerumise eelkäija mis on väljendatud erinevat tüüpi vahendatud

kommunikatsioonivõimaluste kaudu, nagu erasõnumid, fotomärgised, seina postitused ja kommentaarid.

Selleks, et mõista sotsiaalvõrgustikude päritolu, tuleb arvestama selle ajalooga. Sotsiaalvõrgustiku juured ulatuvad 20. Sajandi. Esimest sotsiaalvõrgustikku nimetati SixDegrees.com ja see käivitati 1997. Aastal. Sait lubas kasutajatel luua oma sõprade profiile ja loendeid. Kõik need funktsioonid eksisteerisid ka enne SixDegrees'i. Kasutajaprofiilid eksisteerisid enamikes suuremates ja avalikes saitides. AIM ja ICQ näiteks lubasid luua sõprade nimekirju, kuigi need sõbrad ei olnud teistele nähtavad. Classmates.com lubas inimestel luua oma keskkooli või kolledžiga seotud kogukondi. SixDegrees oli esimene koht, kus need funktsioonid ühendati. Friendster'i käivitamisega 2002 aastal, jõudsid sotsiaalvõrgustikud uuele tasemele. Friendster kasutas kontseptsiooni, mis on sarnane nüüdseks kadunud SixDegrees.com kontseptsioonile, parandas seda ja nimetas seda „Circle of Friends". Aasta jooksul pärast käivitamist saavutas Friendster rohkem kui kolm miljonit registreeritud kasutajat ja mitmeid investeerimishuvilisi. Facebook ilmus veidi hiljem. See käivitati 2004. Aastal ja selle peamine eesmärk oli ühendada Ameerika Ühendriikide õpilasi. Mark Zuckerberg alustas Facebooki arendamist Harvardis. Algul oli see ainuõigus ja inimesed said liituda ainult siis, kui nad said teise Facebooki kasutaja kutse. Eksklusiivne funktsioon oli edukas ja enam kui pooled 19 500-st Harvardi õpilast registreeriti esimesel kuul. Kaks aastat hiljem oli võrgustik avalikkusele avatud. 2008. Aastal ületas Facebook MySpace'i ja Friendster'I populaarsust ning sai juhtivaks sotsiaalvõrgustikuks (McFadden, 2018). Tegelikult on sotsiaalvõrgustikud täielikult muutnud inimeste omavahelist suhtlemist. Kõik meediavormid, mis tänapäeval muudavad kohtumisi ja teistega rääkimist kergemaks, eksisteerisid juba 20. sajandil.

Termin „Sotsiaalmeedia" viitab uutele meedia vormidele. Sotsiaalmeedia arengut võib jagada ringhäälinguajaks ja interaktiivseks ajaks. Ringhäälinguajal oli meedia tsentraliseeritud, kus sellised üksused, nagu raadio- või televisioonijaam, ajaleheettevõte või filmitootmise stuudio levitas sõnumeid ühiskonnale. Tagasiside meediaväljaannetele oli sageli kaudne, hilinenud ja isikupäratu. Suhtlemine vana aja meedias toimus isiklike kirjade, telefonikõnede või uudiskirjade kaudu. Digitaalsete ja mobiilsete tehnoloogiate arenemise abil olid loodud uued meediakanalid, kus interaktiivsust asetati uute meediafunktsioonide keskmesse. Uute tehnoloogiate odavus ja juurdepääsetavus võimaldasid inimestele kasutada rohkem sotsiaalmeedia

funktsioone, näiteks saada teavet mitmetest allikatest ja suhelda teiste inimestega sõnumifoorumite kaudu ning postitada oma ideid.
Kõik sotsiaalmeedia kanalid hõlmavad digitaalset platvormi, olgu see siis mobiilne või statsionaarne. Sotsiaalmeedial on kaks ühist omadust. Esimeseks omaduseks on osalemise võimaldamine. Sotsiaalmeedia platvorm tavaliselt ei ole passiivne. Näiteks sotsiaalvõrgustikus Facebook võib passiivselt vaadata, mida teised postitavad, kuid selleks tuleb luua profiili, mis võimaldab sisu vaadata ja suhelda. Teiseks sotsiaalmeedia omaduseks on interaktiivsus (Manning, 2014, p. 1158). Interaktiivsus võib olla loodud sõpradega, perekonnaga, tuttavatega või teiste inimestega.

Käesolevas töös käsitletakse sotsiaalvõrgustikudest nagu sotsiaalmeedia suuremast osast. Sotsiaalvõrgustiku ja sotsiaalmeedia tähendused on vaja omavahel eristada, kuna nende vahel on tegelikult mitmeid erinevusi. Sotsiaalmeedia määratlus on veebipõhiste ja mobiilsete tehnoloogiate kasutamine, mille abil muutub suhtlumise viis interaktiivseks dialoogiks. Sotsiaalmeedia loob ühtse tähenduse kõigi virtuaalsete kogukondade ja võrgustike vahel ning sotsiaalvõrgustikud on üks osa sellest. Sotsiaalvõrgustik on sotsiaalne inimeste struktuur, keda ühendab ühine huvi. Sotsiaalvõrgustike peamine eesmärk on suhelda teiste inimestega. On ka muid sellest tulenevaid lõpptulemusi, näiteks äritegevus. Mõned inimesed väidavad, et sotsiaalvõrgustik tuli enne sotsiaalmeediat ja mõned teised usuvad, et see oli vastupidi. Sotsiaalvõrgustikud on loodud põhimõtteliselt inimeste poolt. Kasutajad täidavad oma profiilid ja inimesed suhtlevad üksteisega, lähtudes isiklikest andmetest, mida nad profiilidest välja loevad. Sotsiaalmeedia eksisteeris ka enne interneti olemasolu ja väljendas ennast sellistes informatsiooni kanalites, nagu televisioon ja ajakirjad. Kui meedia sai veebi kaudu kättesaadavaks, ei olnud meedia enam staatiline. Kõigile said kättesaadavaks tohutud interaktiivsuse võimalused. Sotsiaalmeedia on väga lai mõiste ja see hõlmab tõepoolest mitut erinevat tüüpi meediat, nagu videod, blogid jne. Sotsiaalmeedia on kommunikatsioonivahend, mis võimaldab teavet teistele inimestele edastada. Lisaks sellele võimaldab sotsiaalmeedia kõigil jagada sisu, mida teised inimesed saavad oma võrguga ühendada (Cohn, 2011). Sotsiaalmeediat kasutatakse peamiselt laiema publikuga teabe edastamiseks või jagamiseks, samas kui sotsiaalvõrgustik on ühist huvi pakkuvate inimeste kaasamine ja suhete loomine veebi kaudu. Sotsiaalvõrgustik ühendab erinevaid rahvusi, religioone, elukutseid, ühiskonnarühmi, vanuseid ja sugu. Kõikidel sotsiaalvõrgustiku kasutajatel on võimalus omavahel suhelda otse, ilma lisavahenditeta, kasutades suhtlustarkvara,

kommenteerides postitusi ja väljendades arvamust. Samuti on sotsiaalvõrgustikul vahendid huvipakkuvate kogukondade loomiseks, kus suhtlemine toimub kitsamates ringkondades. Lisaks erinevad rakendused (nt. mängud) muudavad kasutajate jaoks sotsiaalvõrgustikus viibimise huvitavamaks.

Sotsiaalvõrgustike tekkimine on muutunud võimalikuks tänu tehnoloogia Web 2.0 loomisele. Seda tehnoloogiat kasutavad veebilehed töötavad ja arenevad mõnevõrra teisiti kui tavalised veebilehed, kuna Web 2.0 tehnoloogia võimaldab kontrollida teavet kasutajate abil. Sellest tulenevalt sõltub sotsiaalvõrgustike täitmine ja arendamine registreeritud kasutajate arvust ja nende aktiivsusest. See sotsiaalvõrgustiku struktuur on muutunud kõige mugavamaks, kuna igal kasutajal on eraldi isiklik ruum, ehk profiil, mida kasutajad saavad täita. Lisaks sotsiaalvõrgustike kasutajalehele hakkasid ilmuma erinevad teenused ja rakendused sotsiaalvõrgustiku omanike või teiste ettevõttete poolt. Kasutajad saavad koguneda kogukondadesse, ühendada huvirühmades, avalikult arutada küsimusi ja teha kollektiivne otsus (Murugesan, 2007, pp. 34-41). Igal aastaga kasvab nii sotsiaalvõrgustikke kasutajate arv, kui ka aeg, mille keskmine kasutaja kulutab sotsiaalvõrgustikus. Uue veebi tehnoloogia abil kasvas sotsiaalmeedia populaarsus.

Sotsiaalmeedia platvormid võivad omada erinevaid vorme. Näiteks e-post, mis tähendab, et kasutajad logivad oma konto sisse, et vastu võtta ja saata sõnumeid teistele kasutajatele. Igaühel, kes saadab või võtab vastu e-kirja, peab olema konto.
Järgmiseks sotsiaalmeedia vormiks on veebipäevikud (blogid). See on veebileht, kus üksikisik või rühm saab interneti kaudu jagada teavet või ideid suure hulga inimestega. Sotsiaalvõrgustikud on suurem sotsiaalmeedia vorm. Selle omaduseks on sõprade nimekiri, kust ühendatakse teiste inimestega. Tavaliselt põhineb see sõprusel, perekonnal või töösuhetel (Manning, 2014, p. 1159-1160).

Sotsiaalvõrgustikud omavad nii kommunikatsiooni funktsioone, kui ka informatiivseid, poliitilisi ja majanduslikke funktsioone. Sotsiaalvõrgustikke informatiivne funktsioon tähendab, et võrgustik on võimeline levitama uudiseid kogu maailmas peaaegu koheselt. Lisaks võivad uudised olla nii isiklikud kui avalikud. Kõige silmapaistvam näide hetkel on Facebook, kus alates 2017 aastast on võrgustikus rohkem kui 2 miljardit kasutajat (Mergel, 2012, pp. 281-292). Poliitiline funktsioon väljendub selles, et paljud poliitikud, poliitilised organisatsioonid ja parteid on

huvitatud sotsiaalvõrgustike kasutamisest oma programmi elluviimiseks ja ideede populariseerimiseks (Shirky, 2011, pp. 28-41). Majanduslik funktsioon tähendab seda, et sotsiaalvõrgustikes on palju võimalusi äritegevuseks ja tulu teenimiseks. Neid võimalusi saavad kasutada nii ettevõtted kui ka üksikud kasutajad (Neumann, Elsenbroich, 2017, pp. 1-15). Erinevad funktsioonid teevad sotsiaalmeediat mugavaks ja produktiivseks vahendiks erinevate eesmärkide täitmiseks. Kasutajatel on võimalus oma ideid avaldada kas kirjalikult, piltidega või videote ja helisalvestiste kaudu. Sotsiaalmeedia on ka erineva informatsiooni allikas, mida saab kasutada isikliku õppevahendina.

Uuringu peamine eesmärk on Facebook. Igal sotsiaalvõrgustikul on oma reeglid, mis piiravad kasutajaid mis tahes toimingute teostamisel. Sotsiaalvõrgustiku kasutustingimuste uurimine võib anda vastuseid, millised toimingud rikuvad kasutustingimusi ja millised mitte. Kasutustingimused on reeglid, millega tuleb nõustuda teenuse kasutamisel, ehk reeglite ja eeskirjade kogum, mida teenuseosutaja lisab tarkvarateenusele või veebipõhisele tootele. Tarbijad peab mõistma kasutusingimuste reegleid ja peab sellega nõustuma sageli enne tarkvarateenuse kasutamist, näiteks uue konto loomise käigus. Facebooki kasutustingimuste kogum reguleerib nii Facebooki kasutamist, kui ka Facebooki poolt pakutavaid tooteid, funktsioone, rakendusi, tehnoloogiaid ja tarkvara.
Kahjuliku käitumise, Facebooki kogukonna kaitsmise ja toetamise punkt kasutustingimustes sätestab, et Facebook kasutab kogu maailmas pühendunud meeskondi ja tehnilise süsteemi arendamist, et avastada Facebooki toodete kuritarvitamist, kahjulikku käitumist teiste kasutajate suhtes. Samuti on välja toodud, et kui Facebook saab teada ebaseadusliku sisust või käitumisest, siis võetakse asjakohaseid meetmeid. Meetmeteks on abi pakkumine, illegaalse sisu eemaldamine, juurdepääsu blokeerimine teatud funktsioonidele ning konto blokeerimine või õiguskaitseorganitega kontakteerumine.

Facebooki teenuseid võib kasutada sel juhul, kui arvamuste ja tegevuste taga on reaalsed inimesed. See reegel aitab suurendada Facebooki kogukonna ohutust ja vastutust. Seega Facebook kohustab kasutajaid kasutada oma reaalse nime, määrata täpsed andmed enda kohta, luua ainult ühe kontot ja isiklikult seda kasutada ning on keelatud jagada oma parooli ja seega andma juurdepääsu oma Facebooki kontole. Eespool toodud reeglite eesmärgiks on luua võimalust tuvastada isikut juhul, kui seda

vajab õiguskaitseasutus või Facebooki administraator. Samuti on üheks Facebooki kasutustingimuseks vanusepiirang, mis keelab luua kontot alla 13-aastastele. Lisaks sellele ka piirang kontot luua nendele, keda süüdistatakse seksuaalkuritegudest või isikule, kellele on keelatud saada Facebooki tooteid ja teenuseid vastavalt kehtivatele seadustele.

Kasutajatel on keelatud kasutada tooteid illegaalse sisu jagamiseks või selliste tegevusteks, mis diskrimineerivad ja eksitavad ning rikkuvad teiste inimeste õigusi (sh. intellektuaalomandi õigusi). Samuti kasutajatel ei ole õigust viiruse või pahatahtlikku koodi levitamiseks ning tarkvara, mis võivad viia Facebooki toodete katkestamise või halvenemise või nende liigse koormuse tekkimiseni.
Kauplemise reeglid Facebookis reguleerivad 17 toodete liiki. Nendest 6 on seotud keelatud ja aktsiisi kaupadega. Keelatud kaupadeks on retseptiravimid ja narkootikumid, sealhulgas kanep ja kanepitooted ning seadmed narkootikumite tarvitamiseks. Samuti on müügiks keelatud kahtlased toidulisandid, näiteks anaboolsed steroidid ja kasvuhormoonid. Järgmiseks keelatud kaubaks on relvad, laskemoon ja lõhkeained. Sinna kuuluvad ka sellised kaubad ja teenused nagu paintball'I relvad, pipragaasi pihustid ja lasketiir. Reeglitega ei ole piiratud ainult enesekaitse ja relva litsentside koolituste reklaamimine. Loomade müük on samuti keelatud, sealhulgas loomade osad ja nahk.
Aktsiisi kaupade puhul on keelatud tubakatoodete või nende tarvikute müük, kuid rõivad tubaka brändi logodega ei ole keelatud. Alkohol ja alkohoolsete jookide valmistamise komplektid on samuti keelatud müügiks, kuid raamatud ja DVD alkoholist ning klaasid alkoholi tarvitamiseks ei ole reeglitega keelatud (Facebook, 2018).

Kokkuvõtvalt võib öelda, et sotsiaalmeedia on veebisaitide, rakenduste ja muude platvormide kogum, mis võimaldab meil jagada või luua sisu ja aitab meil ka sotsiaalvõrgustikus osaleda. Sotsiaalmeedia ei piirdu ainult suhtlemise ja piltide jagamisega, vaid omab ka teatud funktsioone. Sellisteks on informatiivne funktsioon, mis tähendab, et võrgustik on võimeline levitama uudiseid kogu maailmas peaaegu koheselt. Veel üheks funktsiooniks on poliitiline. Näiteks võib tuua seda, et paljud poliitikud, poliitilised organisatsioonid ja parteid on huvitatud sotsiaalvõrgustike kasutamisest oma programmi elluviimiseks ja ideede populariseerimiseks. Lõpuks on ka majanduslik funktsioon, mis väljendub selles, et sotsiaalvõrgustikes on palju

võimalusi äritegevuseks ja tulu teenimiseks. Neid võimalusi saavad kasutada nii ettevõtted kui ka üksikud kasutajad. Sotsiaalmeedia mõju ühiskonnale on täna levinud teema arutlemiseks. Mõned inimesed tunnevad, et sotsiaalmeedia on hävitanud inimsuhteid. Kuid on ka teisi, kes tunnevad, et see on mugav viis suhtlemiseks, mis ühendab inimesi kogumaailmast, ning mis võimaldab levitada teadlikkust. Sotsiaalmeedia olemasolu on ühiskonna elu lihtsamaks muutnud.

1.2 Sotsiaalvõrgustikkude funktsioonaalsuse kasutamine kuritegelikel eesmärkidel

Kuigi sotsiaalmeedia on laiendanud inimestele võimalusi suhelda, on ka sotsiaalmeedia negatiivne mõju. Negatiivne mõju väljendub sellistes kuritegudes nagu ebaseaduslik kaubandus, seksuaalkuriteod, organiseeritud kuritegevus ja terroristlikud organisatsioonide korraldamine. Samuti on sotsiaalmeedia abil nüüd lihtsam toime panna arvutiviiruste ja pahatahtliku tarkvara levitamist, häkkimist, isiklike andmete vargust, autoriõiguse piraatlust ja ebaseadusliku informatsiooni levitamist. Selles peatükis käsitletakse sotsiaalmeedia platvormid ja nende mõjud illegaalsele kauplemisele ja pettustele.

Küberkuritegevus on kuritegu, milles kuriteo objektiks on interneti sidevõrgud ja infosüsteemid (häkkimine, andmepüük, rämpspost ja terroristliku tegevuste korraldamine) või mida kasutatakse kuriteo toimepanemise vahendina (illegaalse sisu levitamine ja illegaalne kaubandus). Küberkuritegevuse oht suureneb, kuna üha rohkem inimesi ühendatud internetiga, kasutades sülearvuti ja nutitelefoni. Samuti on see üks kõige tulusamaid viise, kuidas saavad kurjategijad raha teenida. Küberkuritegevuse viise on palju, ning neid võib üldjoontes paigutada kahte kategooriasse: ühekordsed kuriteod, ehk näiteks isikuandmeid varastava pahatahtliku tarkvara paigaldamine, ja käimasolevad kuriteod, nagu väljapressimine, laste pornograafia levitamine või terrorirünnakute korraldamine (*Anon*, 2016). Sotsiaalmeedia kasutamine interneti ühenduseta ei ole võimalik. Hoolimata kasutuses oleva seadmest tuleb interneti ja sotsiaalmeedia kasutamisega ettevaatlik olla.

Kui käsitleda keelatud kaupade leviamisest sotsiaalmeedias, siis on nii otsene mõju narkootikumide pakkumisele kui ka kaudne moju narkootikumide nõudlusele. Esiteks võib sotsiaalmeedia mõjutada narkootikumide pakkumist, näiteks pakkudes võimalusi

narkootiliste ainete ja ravimite ostmiseks ja müümiseks. Teiseks võib sotsiaalmeedia mõjutada turgu, näiteks nõudluse suurendamisega, narkootikumidega seotud kogemuste jagamisega, narkootikumidega seotud fotode ja videote jagamisega ning narkootikumidega seotud arvamuste kujundamisega.

Uimastite tarnimist võib hõlbustada samuti mitmel viisil. Üks võimalus on, et sotsiaalmeedia platvormide kasutajad saavad otseselt aineid müüa. Näiteks 2014. aastal avaldas narkootiliste ainete teabekeskus „DrugAbuse“ infograafilise dokumentatsiooni narkootiliste ainete kauplemise kohta Instagramis. Uuringu käigus tuvastasid teadlased ühe päeva jooksul 50 narkootikumide edasimüüja kontot. Paljud sisaldasid müüdavate ainete fotosid. Instagrammi kasutati müüdavate ravimite reklaamimiseks, kuid müügi tehingud toimusid muude sidekanalite kaudu, näiteks sõnumirakenduses WhatsApp, mis võimaldab kasutajatel anonüümseks jääda.

Narkootilis aineid reklaamitakse nii piltide, kui ka videote abil. Kui Instagramis reklaamitakse fotode abil, siis YouTube’is kasutatakse videot. YouTube on kõige populaarsem videote jagamise sotsiaalmeedia platvorm. Manning (2013) uuris YouTube’i ja narkootikumitega seotud videote vahelist seost. Uuring hõlmas 750 uimastivideo sisu analüüsi. Uuringu käigus leiti suur hulk videod, mis andsid juhiseid kuidas kasvatada oma kanepit (European Monitoring Centre for Drugs and Drug Addiction, 2016, pp. 115-118).
Sotsiaalmeedia platvormid liiguvad üha enam reaalsest maailmast digitaalsele maailmale, ning selle järel liigub ka narkootikumide turg. Kuigi sotsiaalmeedia võib hõlbustada narkootikumide pakkumist, peab toote vahetamine siiski toimuma reaalses elus, kas postiteenuse kaudu või käest kätte.

Küberkuritegevus omab sageli rahvusvahelist mõõdet. Ebaseadusliku sisuga e-kirjade ülekandmisel läbivad nad sageli mitmeid riike. Küberkuritegevuse uurimise käigus on on oluline saavutada tihe koostöö asjaomaste riikide vahel. Menetluste loomine eesmärgiga kiirelt reageerida vahejuhtumitele ning rahvusvahelise koostöö päringud seisavad seega väga olulisel positsioonil (Sofaer & Goodman, 2001, pp. 6-7). Mitmed riigid toetavad oma vastastikuse õigusabi süsteemi „Double criminality“ põhimõttel, ehk kahtlustatavat võidakse välja anda ühest riigist, et kohtusse pöörduda teise riigi seaduste rikkumise eest ainult siis, kui väljaandvas riigis on olemas sarnane seadus. Ülemaailmsed uurimised piirduvad üldjuhul kuritegudega, mis on kõikides osalevates

riikides kriminaliseeritud (Williams, 1991, pp. 581-624). Üheks näiteks on vihakõne. Kuna ebaseadusliku sisu kriminaliseerimine erineb erinevates riikides, siis materjal, mida võib ühes riigis seaduslikult levitada, võib teises riigis olla seadusega piiratud. Tuleb märkida, et praegu kasutatav arvutitehnoloogia on põhimõtteliselt ühesugune kogu maailmas. Aasias müüdavate arvutite ja mobiiltelefonide ning Euroopas müüdavate mobiiltelefonide vahel eksisteerib vähe erinevusi. Seega on sotsiaalmeedia põhised kuriteod aktuaalsed kõikides riikides. Analoogne olukord tekib seoses internetiga. See võimaldab kasutajatel kasutada Internetis sama teenuseid üle maailma. Kui me mõistame Internetti mitte kui tehnoloogiat, vaid tehnoloogiliselt aktiivsete sotsiaalsete tavade muutuva kogumina, hakkame me mõistma, kuidas e-keskkond muutub, ehk kuidas see toimib ja kuidas inimesed tavaliselt kasutavad seda teistega suhtlemiseks. Sellest tulenevalt võib muutuda ka kuriteo ja ohvriks langemise olemused. Käesolevas alapeatükis on oluline uurida, kuidas Web 2.0 ja seejärgi sotsiaalvõrgustike esilekerkimine mõjutas küberkuritegevust ning aitas luua uusi pettuse vorme ja seeläbi luua uusi e-kuritegevuse vorme.

Selleks, et saada aru kuidas tekkisid kuriteod sotsiaalmeedias, on kõigepealt vaja kindlaks teha, kuidas uute kommunikatsioonitehnoloogiate arendamine on muutnud suhete iseloomu. Mõistet uus meedia kasutatakse paljude infotehnoloogiate tähistamiseks, mis kasutavad digitaliseerimist, paljundamist ja edastamist sisu genereerimisel (Jenkins, 2008, p. 282). Nende arengute keskmes on selliste tehnoloogiate ühendamine ja integreerimine elektroonilistesse sidevõrkudesse, nagu Internet ja veeb. Veeb (World Wide Web-WWW) on omakorda Interneti-põhine infosüsteem, mis võimaldab dokumente ühendada teiste dokumentidega hüpertekstilinkide abil, võimaldades kasutajal teavet otsida, liikudes ühest dokumendist teise. Nende uute meediakanalite puhul on väidetavalt eristusvõime, et need ei ole ühesuunalised, vaid võimaldavad pigem kahesuunalist suhtlemist (Miller, 2011, pp. 12–14). Teisisõnu, meedia igapäevased kasutajad saavad nüüd ise meediasisu luua ja jagada seda globaalselt. Tuleb märkida ka seda, et vaatamata sellele, et Interneti kasutajate võimalused on tänapäeval ümberkujundanud, Interneti algusaastad kippusid reprodutseerima varasema meediatehnoloogiaga seotud suhtlusmudeleid.

Peale Web 1.0, mis lõppes it-mulli lõhkemisega, hakkas vaikselt tekkima uus ja läbimõeldum kontseptsioon: Web 2.0. Seda terminit mainiti esmakordselt O Reilly

Media poolt 2004. aasta konverentsil ja see kannab endas nn. WWW uue versiooni mõtteviisi. Web 2.0 on ärirevolutsioon IT-tööstuses mille põhjustas Interneti kui platvormi teadvustamine ja proov mõista selle uue platvormi edukuse reegleid. Web 2.0 lahendused lasevad kasutajatel sisu loomisse ise panustada tõstes sellega veebikeskkonna väärtust (näiteks kommentaariumid, tootearvamused, wikid, videod, foorumid jne). Web 2.0 kohta on kasutatud ka termineid osalusveeb ja kollektiivne intelligents (Kalda, 2009).

Termin „Web 2.0" kasutatakse selleks, et tähistada suurt Interneti kommunikatsiooni, mis iseloomustab kasutajate kõrge interaktiivsuse määra ja sisu genereerimist samade kasutajate poolt. See kasutaja poolt loodud sisu võib sisaldada erinevaid informatsiooni vorme, nagu video, muusika, fotograafia, artikel, raamat ja blogi. Meedia kasutaja ei ole enam lihtsalt sisu tarbija, vaid ka selle tootja, keda haarab selline mõiste nagu tootev tarbija. (Ritzer & Jurgenson, 2010, pp.13-36). Võttes arvesse kõiki eespool nimetatud asjaolusid on oluline keskenduda selle uue maastiku ühele konkreetsele mõõtmele, nimelt sotsiaalvõrgustike tõusule. Need on Interneti-põhised rakendused, mis võimaldavad inimestel end teistega tutvustada (oma elu, tegevused, huvid ja arvamused). Nende hulka kuuluvad sellised sotsiaalmeedia platvormid nagu Facebook, YouTube, MySpace, Twitter, Tumblr ja LinkedIn (Miller, 2011, pp. 171–173). Kõigi selliste uute meediumiruumide keskmes on viisid, kuidas nad võimaldavad kasutajatel ennast esitleda avalikkusele, kuvades oma identiteete teistele ning võimaldades neid vaadata ja kommenteerida.

Need platvormid üha enam integreeritakse seadmetega, näiteks nutitelefonid, mis võimaldavad kasutajate poolt pildi, video ja teksti kohest salvestamist ja reaalajas jagamist. See võimalus on kasutajatele atraktiivne, kuna need võimaldavad meil luua sotsiaalse kohaloleku laiendatud kaasvastajate kogukonna hulgas ja vastupidi saada intiimseid teadmisi teiste inimeste igapäevaelust ja tegudest. Lapsed ja noored võivad muutuda üha haavatavamaks kurjategijatele, mis tuleneb uute sotsiaalmeedia ulatuslikest kasutamistest. Facebook, maailma kõige populaarsem sotsiaalvõrgustik lubab kontot luua igaühel, kes on 13-aastane või vanem (Mann, 2008, p. 255).
Tegelikult seda vanusepiirangut tihti ignoreeritakse. Näiteks võib tuua seda, et USAs on 7,5 miljonit alla 12-aastast last Facebook'I kasutajat (Bazelon, 2011). On samuti teada, et Ameerika ühendriikides 40% 12-aastastest lastest kasutab sotsiaalvõrgustikke (vanuse piiranguid rikkudes) ning sarnaseid rikkumisi on leitud Euroopa laste seas,

kus 10-aastaseid oli 31%, 11-aastaseid 44% ja 12-aastaseid 55%); 10-aastaste seas oli 78% vanematest abistanud neid konto loomisel Facebook'is. Ainult 50% vanematest, kes soovisid lubada oma lastel selliseid veebilehekülgi kasutada, nende järelevalve all (Hargittai, *et al*., 2011).

Need asjaolud on põhjustanud juhtumeid, kus noored teevad end kättesaadavaks teadmata isikutele kontakteerumiseks ilma tõhusa vanemate järelevalveta. Eelkõige on tekkinud mure, et sotsiaalvõrgustikud pakuvad seksuaalkurjategijatele lihtsat võimalust endale ohvrit leida. Selline kuritarvitamine võib hõlmata olukordi, kus üksikisik (tavaliselt täiskasvanu, kuid mitte ainult) leiab võimaluse võrgukeskkonnas alaealisega suhelda. Need suhted võivad sisaldada selgesõnalise seksuaalse olemuse stsenaariumi, seksuaalse iseloomuga küsimuste esitamine ja alaealiste õhutamine seksuaalseks käitumiseks, ehk ettevalmistused järgnevaks kontaktiks reaalses elus (O'Connell, 2003, p. 9). Näiteks laste hooldamine, võites nende usalduse, et korraldada järgnevaid koosolekuid, kus võib juhtuda füüsiline väärkohtlemine.

Arvestades, et selliste veebilehtede eesmärk on julgustada kasutajaid ühendusi luua ja teistega suhtlema, hõlbustavad nad kerget ligipääsu pakutavate teenuste kaudu teiste leidmisel ja nende poole pöördumisel. Lisaks loovad kasutajad avalikke profiile, mis sisaldavad isiklikku informatsiooni, nagu vanust, elukohta ja sageli ka fotot. Samuti on petliku profiili loomine lihtne, võimaldades näiteks täiskasvanutel ennast internetis tutvustada lastena, et alaealisi suhtluses paremini kaasata (Ybarra & Mitchell, 2008, pp. 350–357). Kõik eeltoodud näited suurendavad oluliselt kuritegijate võimet tuvastada ja sihtida ohvreid.

Pöördume alaealiste sotsiaalvõrgustikus ohvriks langemise eest täiskasvanute ohvriks langemisele, mida on ümber kujundanud sotsiaalmeedia tekkimine. E-suhtluse arendamine on toonud kaasa tavapäraste õigusrikkumiste vormide laienemise, mis on rännanud uude elektroonilisse side valdkonda. Sellised kuriteod nagu ahistamine ja jälitamine on võtnud uue elu Internetis (Mullen, *et al*., 2001, p. 9). Jälitamist iseloomustab korduv käitumine, sealhulgas: ohvritele telefonikõnede tegemine, nende mitmesuguste kirjade, kingituste või solvava materjali saatmine, jälgides ohvrit, ähvardades ohvri vara, lähedasi ja töökaaslaseid (McGuire & Wraith, 2000, p. 317). Jälitamine võib saada füüsilise ja seksuaalse rünnaku ja tapmise tagajärjeks. Küber jälgimist saab määratleda kui Interneti, e-posti või sellega seotud digitaalsete

elektrooniliste sidevahendite korduvat kasutamist, et häirida või ähvardada konkreetset isikut (D'Ovidio & Doyle, 2003, p. 10). Kõigil sellistel käitumistel ei ole seksuaalset eesmärki, kuid märkimisväärne osa ahistamisest sotsiaalmeedias on seksuaalse iseloomuga (Alexy, *et al*., 2005, pp. 279–289). Tavaliselt need toimingud kujutavat ennast püsiva seksuaalse selgesõnalist väljendamist, mida levitatakse e-posti, kiirsõnumite ja erinevate sotsiaalvõrgustike kaudu. Sellised kogemused võivad ohvritele tekitada emotsionaalset ja psühholoogilist stressi, põhjustades alandustunnet, hirmu ja ärevuse tundeid. Anonüümsuse tunne, mida pakkub interneti tehnoloogia, aitab vähendada agressiivse, ähvardava ja antisotsiaalse suhtluse pärssimist seeläbi julgustades veebikasutajaid tegelema seksuaalse ja muu ahistamisega (Kabay, 1998, p. 8).

Palju juhtumeid on pööranud tähelepanu ka „trollimise" nähtusele sotsiaalmeedia veebilehtedel. Trollimine viitab nende isikute tegevusele, kes tahtlikult otsivad võimalusi kuritahtlike kommentaaride postitamiseks võrgus, kavatsusega tekitada häireid ja stressi (Morris, 2011). Sotsiaalvõrgustiku kõrgendatud nähtavuse ja kommunikatiivse kättesaadavuse tase võimaldab, et üksikisikud puutuvad kokku ähvardava, kuritahtliku ja häiriva kontaktiga.

On mitmeid teisi valdkondi, kus sotsiaalvõrgustikude kasutamine loob võimalusi kurjategijatele. Eriti identiteedivargusega seoses tekivad ohud, mis toovad kaasa nn. Eraelu teabe ebaseadusliku kasutamise, nagu isiku sünniaeg, sünnikoht, kodune aadress, perekonnaseis ja perekonnaliikmete nimed (Smith, 2010, p. 277). Sellist teavet kasutavad sageli sellised finantsteenuste pakkujad nagu pangad ja laenuandjad, eesmärgiga identiteeti tõestada. Selliste andmete jagamine sotsiaalvõrgustikude kaudu võimaldab kurjategijatel seda kasutada. Üks uurimus näitas, et umbes 40% sotsiaalvõrgustikude kasutajatest avalikustab oma koduse aadressi, hoolimata sellest, et sellise isiklikku teabe jagamine võib tagada turvariski (*Anon*, 2010).

Teises uuringus leiti, et selliste sotsiaalvõrgustiku kasutajad nagu Facebook ja Twitter, said tõenäolisemalt identiteedivarguse ohvriks kui need, kes sotsiaalvõrgustikuid ei kasuta ning ohvriks langemise oht suureneb, kui isikud kasutasid sotsiaalvõrgustikuid pikema aja jooksul (*Anon*, 2011). Sarnased riskid tulenevad kasutajate postitamisest sellist tundlikku teavet, nagu sotsiaalkindlustuse numbrid ja sünniaeg. Näiteks võivad

üksikisikud, kes avaldavad oma reisiplaane, pakkuda kurjategijatele võimalusi koduse vara varguseks.

Kokkuvõtlikult öeldes on uue põlvkonna tehnoloogia tagajärjel tulnud vana veebi asemele uus Web 2.0. Uus veebi tehnoloogia võimaldas luua laiemaid funktsioone sotsiaalmeedias. Nende funktsioonide kasutamine toob nii mugavust kasutajatele, kui ka kurjategijatele. Seega saab sotsiaalmeedia funktsioone kasutada ebaseaduslikel eesmärkidel. Sotsiaalvõrgustikus osalemine koos isikliku elu avalikustamisega, mida see tingimata eeldab, toob endaga suurema hulga kuritegude ohvriks langemise määra kui varem.

Teaduse ja tehnika arengu saavutused mõjutavad ühiskonnaelu nii positiivselt, kui ka negatiivselt. Peamine negatiivne suundumus on kuritegelike ohtude tungimine info- ja telekommunikatsioonikeskkonda.

Infotehnoloogia valdkonnas tekivad uued kuriteod, näiteks elektrooniliste andmete terviklikkuse, kättesaadavuse ja konfidentsiaalsuse rikkumine. Samas ei vaja kuriteo toimepanemine sotsiaalmeedias palju pingutusi ja kulusid, vaid piisab arvutist, pahatahtliku tarkvarast ja internetiühendust. Tänapäeval pole vajalik omada sügavaid tehnilisi teadmisi, kuna internetis on loodud spetsiaalsed foorumid, kus saab osta tarkvara kuritegude toimepanemiseks, näiteks sotsiaalvõrgustiku kasutaja identifitseerimisandmete varguseks ja arvutisüsteemide rünnakute korraldamiseks.

Kuritegevuse ulatust sotsiaalvõrgustikudes on raske hinnata. Eelkõige seetõttu, et infotehnoloogiliste vahendite abil toime pandud kuritegude tuvastamine muutub keerulisemaks.

2. KURITEGEVUSE TOIMEPANEMINE JA ENNETAMINE SOTSIAALMEEDIAS

2.1 Sotsiaalvõrgustike levinumad kuriteoliigid

Töös kasutatakse kvalitatiivset uurimismeetodit ning andmete kogumiseks viis autor läbi küsitlust ja ekspertintervjuud, et saada andmeid ebaseadusliku kaubanduse ja küberkuritegevuse kohta Facebookis. Käesolevas alapeatükis analüüsib autor nii küsitluse vastuseid, kui ka intervjuu andmeid. Samuti käsitletakse levinumad kuriteoliigid sotsiaalmeedias.

Küsitlus koosnes kahest osast. Esimese osa küsimused olid seotud illegaalse kaubandusega Facebookis. Lisaks küsiti ka teadmised illegaalsetest kaupadest. Ilma teadmisi kasutajad ei pruugi müügis olevaid illegaalseid kaupu ära tunda, seega püüdis autor hinnata vastajate teadmisi selles osas. Kõik küsimused olid kohustulikud. Küsimustele vastasid 146 isikut, neist 77 (52,7%) olid mehed ja 69 (47,3%) naised. Kõik vastajad täitsid küsimustiku eesti keeles. Kuna küsimustele vastamine oli täiesti anonüümne, siis polnud võimalik kindlaks teha, millisest valimi allikast keegi osales.

Vastanute vanuseline jaotus oli järgmine:

- noorem kui 18 – vastanuid ei olnud (0%)
- 18-30 – 121 vastaja (82,9%)
- 31-40 – 17 vastajat (11,6%)
- 41-50 – 7 vastajat (4,8%)
- 51-60 – 1 vastaja (0,7%)
- Vanem kui 61 – vastanuid ei olnud (0%)

Järgmiselt selgus, et vastanute Facebooki kasutamise kestus on:

- Vähem kui 1 aastat – 9 vastajat (6,2%)
- 1 kuni 5 aastat – 32 vastajat (21,9%)
- 6 kuni 10 aastat – 95 vastajat (65,1%)
- Rohkem kui 10 aastat – 10 vastajat (6,8%)

Neist 92 (63%) vastajaid mitte kordagi ei ostnud või müünud kaupa Facebookis. Vastajate arv, kes ostavad või müüvad kaupa harva on 45 (30,8%). Sageli kauplevad

Facebookis 9 (6,2%) vastajaid ning ühtegi vastanutest ei tegele kauplemisega Facebookis põhitegevusena.

Järgmisel küsimusel autor püüdis välja selgitada kasutajate teadlikkuse sellest, millised kaubad on ebaseaduslikud müümiseks Facebookis eraisiku poolt ning tõi välja näited (alkohool, tubakas, tubakatooted, e-sigarettid ja nende täitevedelikud, relvad, narkootikumid, ravimid). Selline küsimus on oluline, kuna teadmised kujundavad turvalisust selles valdkonnas.

Tabel 1. Vastanud Facebooki kasutajate teadmised illegaalsetest kaupadest (autori koostatud)

Kas te olete teadlik, millised kaubad on ebaseaduslikud müümiseks Facebookis eraisiku poolt?	**Vastajate arv**	**Vastajate arv protsentides**
Jah	56	38,1%
Jah, kuid mitte piisavalt	59	40,1%
Ei	14	9,6%
Ei, aga ma tahaksin sellest rohkem teada saada	17	11,6%

Tabelist on näha, et 56 (38,4%) vastajatest on sellest teadlikud, kuid enamikul vastajatel, ehk 59 (40,4%) isikutel, puuduvad piisavad teadmised sellest. 14 (9,6%) vastajatel on teadmiste täielik puudumine ning 17 (11,6%) vastajatel lisaks teadmiste puudumisele on soov sellest teada saada.

Esimese osa eelviimase küsimuse eesmärgiks oli saada ülevaade olukorrast, kus vastajad on ise olnud tunnistajaks ebaseaduslike kaupade müümisel Facebookis. Vastajatel oli võimalus märkida mitu kaupa, seega on tunnustatud kaupade arv suurem, kui tunnistajate arv.

Tabel 2. Vastanud illegaalse kaupade tunnistajad Facebookis (autori koostatud)

Tunnistatud kaup	**Vastajate arv**	**Vastajate arv protsentides**
Mul ei olnud juhust	117	79,6%
Tubakas ja tubakatooted	23	15,6%
Alkohol	15	10,2%
Ravimid	4	2,7%
E-sigarettide vedelikud	1	0,7%
Narkootikumid	1	0,7%
Pürotehnika	1	0,7%

Tabelist selgub, et enamik isikutest, ehk 117 (79,6%), ei olnud kunagi näinud ebaseaduslike kaupade müümist Facebookis. Ebaseaduslike kaupade müümise tunnistajateks olid 26 isikut. Kõige levinum kaup vastajate hulgas oli tubakas ja tubakatooted, mis sai 23 (15,8%) vastuseid. Teisel kohal oli alkoholi tooted 15 (10,2%) vastustega. Kolmandal kohal olid ravimid 4 (2,7%) vastustega. Ühe vastuse said sellised kaubad, nagu narkootikumid, e-sigarettide vedelikud ja pürotehnika.

Viimane küsimus esimese osas väljendas vastajate arvamust selle kohta, kas kauba müük ja/või ost Facebookis on turvaline või mitte. Enamiku vastajate arvamus oli negatiivne, ehk 82 (56,2%) vastajatest arvavad, et kauplemine Facebookis ei ole turvaline. 44 (30,1%) vastajatest ei tunne ennast täiesti turvaliselt ning 20 (13,7%) vastajaid arvavad, et kauplemine Facebookis on turvaline.

Küsitluse teise osa eesmärgiks oli välja selgitada Facebooki kasutajate käitumist oma andmete jagamisel ja profiili kaitsmisel, teadlikkust küberkuritegevuse ohtudest ning ohvriks langemise määra vastajate hulgas.

Küsimustiku teises osas selgus, et enamik vastajatest, ehk 94 (64,4%), muudavad oma konto parooli harva. Samuti 27 (18,5%) vastajatest kunagi ei vaheta oma konto parooli, kuna puudub vajadus selleks. Ainult 11 (7,5%) vastajatest vahetavad oma parooli regulaarselt.

Järgmise küsimusega püüti selgitada välja, kui tihti vastajad kasutavad asukoha jagamise funktsiooni Facebookis. Selgus, et 73 (49,7%) vastajatest ei kasuta seda kunagi ning 69 (46,9%) vastajatest peaaegu ei kasuta seda funktsiooni. Ainult 5 (3,4%) vastajat sageli jagavad oma asukoha.

Samuti oli küsitud isiklikute andmete paljastamisest (sünnipäev, elukutse, elukoht, telefoni number). Tulemuseks selgitati välja, et 84 (57,1%) vastajatest paljastavad osaliselt oma andmeid Facebooki profiilis ning 57 (38,8%) vastajatest ei näita avalikkusele oma isiklikke andmeid. 6 (4,1%) vastajaid omakorda jagavad oma andmeid Facebookis.

Üheks küsimustiku eesmärgiks oli välja selgitada Facebooki kasutajate teadlikkust sellistest küberohtudest, nagu isiklike andmete vargus, jälitamine, ahistamine ja

pahavara levitamine. Selgus, et 109 (74,1%) vastajatel on piisavad teadmised küberohtudest. 14 (9,5%) vastajaid teavad sellest pealiskaudselt ning sooviksid sellest rohkem teada saada. Samuti 5 (3,4%) vastajatest ei oma teadmisi küberohtudest, kuid tahaksid sellest teadma.

Teise osa eelviimase küsimuse eesmärgiks oli saada ülevaade olukorrast, kus vastajad on ise saanud küberkuritegevuse ohvriks Facebookis. Vastajatel oli võimalus märkida mitu kuritegevust, seega on tunnustatud kaupade arv suurem, kui tunnistajate arv.

Tabel 3. Vastanud küberkuritegevuse ohvrid (autori koostatud)

Kas te olete kunagi langenud pettuse ohvriks Facebookis? Kui jah, siis millise pettuse?	**Vastajate arv**	**Vastajate arv protsentides**
Ei olnud	131	89,1%
Pahavara (nt. viirused)	11	7,5%
Isiklike andmete vargus	4	2,7%
Ahistamine	4	2,7%
Jälitamine	3	2%

Eelviimases küsimuses selgitati välja, et enamik vastajatest ei ole kunagi langenud pettuse ohvriks Facebookis, neid oli 131 ehk 89,1%. Kõige levinumaks pettuseks sai pahavara levitamine. Selle kuriteo ohvreid oli 11 (7,5%) vastajat. Isiklike andmete varguse ja ahistamise ohvriks said 4 (2,7%) vastajat. Lisaks sellele oli ka 3 (2%) jälitamise ohvrit.

Teise osa viimases küsimuses püüti välja selgitada Facebooki kasutajate teadlikkust sellest, kuidas kaitsta ennast pettustest Facebookis (privaatsusseaded, turvaline parool, funktsioonide hoolikas kasutamine). Tulemuseks tuli välja, et suurem osa vastajatest, ehk 98 (66,7%), oskavad kasutada turvameetmeid. Samuti 22 (15%) vastajatest teadsid sellest pealiskaudselt ja sooviksid sellest rohkem teada. 9 vastajatel puudusid sellest teadmised ja sooviksid teada saada.

Kokkuvõteks võib öelda, et sellised pettused nagu jälitamine, ahistamine ja isiklike andmete vargus sotsiaalvõrgustikus Facebook ei ole levinud nähtus, kuid pahavara levitamine sai kõige levinumaks pettuseks vastajate hulgas. Kokku neid juhtumeid on 22, neist 11 on pahavara levitamise juhtumid. Töö teises osas autor annab ettepanekuid selle kohta, kuidas kaitsta ennast pettuste vastu.

Lähtuvalt vastustest on illegaalne kaubandus rohkem levinud nähtus võrreldes pettustega. Kokku oli 45 juhtumeid, kus kasutajad olid ebaseadusliku kaubanduse tunnistajaks. Sellest suurem osa oli tubaka ja tubakatoodete illegaalne müük (23 juhtumit) ning alkoholi illegaalne müük (15 juhtumit). Ravimite illegaalse müügi tunnistajateks said 4 vastajat.

Samuti selgus, et enamikul vastajatel (40,4%) puuduvad piisavad teadmised sellest, millised kaubad on illegaalsed Facebookis müümiseks.

Teisest osast võib järeldada, et enamik kasutajatest (63,9%) ei pööra piisavalt tähelepanu oma konto parooli regulaarsele vahetusele.

Selgus, et vastajad kasutavad asukoha jagamise funktsiooni ettevaatlikult ning enamus neist loobuvad selle kasutamisest. Isiklikke andmete jagamise osas on sama olukord, ehk enamik vastajatest ei paljasta oma andmeid avalikkusele.

Vaatamata sellele, et enamik vastajatest on teadlikud sellest, kuidas kaitsta ennast pettustest, on ka selliseid, kes vajavad rohkem teadmisi selles osas. Illegaalse kaubanduse osas oli teine olukord. Suurem osa vastajate teadmised olid nende arvates mitte piisaval tasemel.

Teiseks andmete kogumise meetodiks oli ekspertintervjuu. Intervjuu eesmärgiks oli saada ülevaade kuritegevuse olukorrast sotsiaalvõrgustikudes. Püüti välja selgitada, millised on aktuaalsed kuriteod Eestis ning milliseid meetmeid on võimalik kasutada nende tõkkestamiseks. Lisaks olid küsimused tänapäevaste väljakutsete kohta kuritegevuse ennetamisega sotsiaalvõrgustikudes, et uurida praegused Eesti arengu kohad selles valdkonnas. Esimeseks eksperdiks oli Maarja Punak, PPA kommunikatsiooni büroo, sotsiaalmeedia ja veebiturvalisuse valdkonna spetsialist.

Lähtudest Maarja Punaki sõnadest pannakse toime läbi sotsiaalmeediat erinevaid kuritegusid. Intervjuust selgus, et enne kõike võib rääkida identiteedivargusest, mis on tõusvas trendis. Identiteedivargusest käsitletakse nii töö teooria osas 17 leheküljel, kui ka praktilises osas. Identiteedivargus tähendab isikute andmete vargust ja libakontode loomist. Eesmärgiks on panna toime kuriteod libakontode abil, ehk teise isiku nimel. Siit võivad tulla ostu-müügi pettused või valeinfo jagamine. Vihakõne tehakse tihti kas võõralt kontolt või libakontolt. Kui üks isik loob võltsitud kontod kasutades teise isiku andmeid, siis see on juba identiteedivargus. Kontode ülevõtmine oli ka kunagi populaarne kuriteo liik, mis samamoodi läheb häkkimise paragrahvi alla. Kui saadi aru, kuidas need kontod üle võeti, siis see võimalus likvideeriti. Selline nähtus

sotsiaalmeedias nagu „Trolling“ (teisele inimesele stressi tekitamine) ei ole seadusega piiratud, kui ta ei kvalifitseeru ähvarduse, väljapressimise, vihakõne või mingi muu alla, mis on seadusega väga selgelt ära seletatud. Kuid tülitamine läheb tsiviilasja alla. Oli juhtumeid, kus keegi saatis isiku kontole sada korda vägisõnu ja seega rikkus ta selle isiku eraelu nii, et viimasel oli võimalus asja kohtusse anda. Praegu on valimistejärgne aeg, seega kasutatakse tuntuid isikute pilte ja nende põhjal solvatakse. Pettusskeemid toimuvad igapäevaselt. Identiteedivargus toimub tihti nii, et suhted inimeste vahel purunevad ning nad lähevad lahku, seejärgi mehed teevad naistele libakontosid erinevates portaalides, kus pakutakse seksuaalse sisuga teenuseid. Samuti toimub ka illegaalse kauba müük. Kõige populaarsem on ravimite müük (müüakse need ravimid mis on endal alles või mis on välisriigis ostetud edasimüümise eesmärgil), sealhulgas viagra müük, mis kuulub ravimiseaduse alla. Sellel juhul annab politsei info edasi Ravimiametile. On ka teada, et detsember on pürotehniliste asju müügi põhihooaeg. Toimub ka alkoholi, mokatubaka, sigarettide (sh. e-sigarettide vedelikud) ja külmrelvade müük.

Samuti intervjuust Maarja Punakiga selgus, et küberkuritegude menetlemine on keeruline protsess, kuid politseil on võimalik teada anda, et keegi oli toime pandud väljapressimist ning paluda lõpetada sellist tegevust.

Üldjuhul pettuse kontod likvideeritakse ja asi lõpetatakse. Ennetuse mõttes ikkagi hoiakse silma selle peal, mis toimub mujal politsei kontodel ehk millist infot jagatakse. Eestisse jõuavad asjad hiljem. Näiteks lapsi hirmutav „Momo“ nimeline konto, mille kaudu tehti kuriteod. See jõudis välismaale enne, aga Eesti politsei oli juba teadlik, et see võib ka Eestisse jõuda. Seega meil oli hea võimalus selleks valmis olla. Veel oli sotsiaalmeedias selline enesetapumäng, mida nimetati „sinivaal“ kus mängija peab 50 päeva jooksul tegema ülesandeid, mis on määratud administraatorite poolt. Ülesanneteks oli enesevigastamine ning viimaseks ülesanneks oli enesetapp. Politsei teavitas lapsevanemaid läbi sotsiaalmeedia ja e-kooli, et nad oleksid sellest paremini informeeritud. Politsei oli teinud e-kooliga sellise kokkuleppe, et kui tulevad sellised ohtlikud asjad ette, siis teavitab politsei sellest ka e-kooli keskkonda kaudu.

Kui on teada, et isik postitab illegaalseid asju müügiks, siis on võimalik välja selgitada kes selle taga on ning teda otseselt karistada. Samamoodi kui keegi pidevalt tüütab, siis ohvrile soovitatakse sotsiaalmeedias kasutada privaatsusseadeid.

Samuti ekspert oli märkinud, et sotsiaalmeedias toimub ka lapspornograafia levitamine. Laps ise ei tea, mis on lubatud ja keelatud ning võib oma otsusel postitada

sellist sisu, mis meie seaduse alusel läheb lapspornograafia alla. See tähendab seda, et politsei peab teostada rohkem selgitustööd.
Intervjuust selgus, et sotsiaalmeedia keskkondi , kus inimesed omavahel suhtlevad, on palju ning iga päev tuleb neid juurde. On palju keskkondi, kus üldse ei tehta koostööd politseiga. Näiteks võib tuua sotsiaalvõrgustiku Vkontakte ja Odnoklassniki, nad ei anna politseile andmeid välja. Läbi sotsiaalmeediat pannakse toime erinevaid kuritegusid ja kõige levinumaks kuriteoks on identiteedivargus, mis on tõusvas trendis. Võib järeldada, et oluliseks ülesanneks on elanikke teavitamine võimalikest ohtudest sotsiaalmeedias, kuna sellest sõltub kasutajate turvalisus.

Teine ekspertintervjuu oli korraldatud Maksu- ja Tolliameti uurimisosakonna ametnikuga Andreas Sõlega kes tegeleb sotsiaalmeedia ebaseadusliku sisu jälgimisega ja monitooringu kanalitega.
„MTA roll on nii legaalse kui ka illegaalse ja keelatud kaubanduse kontroll. Samuti on meie oluliseks rolliks informatsiooni kogumine ja selle töötlemine“ (Sõlg, 2019).
Intervjuus selgus, et praegu aktuaalsed kuriteod on seotud kahe suure valdkonnaga - illegaalne aktsiisi ja keelatud kauba müük. Seda tõestavad ka korraldatud küsitluse tulemused töö praktilises osas. Facebookis luuakse spetsiaalsed gruppid, kus müüakse ja ostetakse illegaalseid kaupu. Seal võib müügis olla nii aktsiisi kaubad kui ka ravimid. MTA tegeleb nende gruppide jälgimisega.
Kui rääkida ennetamisest, siis gruppile ligipääsu saamiseks luuakse lisakonto Facebookis ja taotletakse gruppi administraatori luba. Enamik gruppi osalejatest samuti loovad lisakontosid, et ei oleks võimalik isikut tuvastada. Isikut võetakse vastutusele kui on võimalik teda tuvastada. Samuti kui isik müüb illegaalseid asju, siis võib teha kontrolltehingu, et teha kindlaks isiku tegevust. Need gruppid võib kinni panna kirjutades Facebooki haldurile. Tavaliselt vastab haldur nädala jooksul. Probleem seisneb selles, et gruppi kinni panemisel luuakse uued gruppid, kuna see ei ole Facebooki kasutustingimustega piiratud.
Peamiseks väljakutseks praegu on võltskontod ja sellega seotud isiku tuvastamine ja vastutusele võtmine. Neid kontod Facebook ei sulge, kuna ei ole võimalik tuvastada isikut ning tõestada, et see on võltskonto ja sellega illegaalselt kaubeldakse. Samuti raskendab olukorda see, et isik võib võltskontod uuesti luua. Teiseks väljakutseks on inimeste teadmiste tõstmine selles valdkonnas. Enamik inimesi ei ole teadlikud milliseid kaupu ei saa müüa Facebookis. Näiteks võib tuua ravimid retseptiga.

Eksperdi arvates läheb tulevikus olukord raskemaks, kuna illegaalsed kauplejad saavad Facebooki privaatsusseade abil oma profiili teiste jaoks kinni panna.

Küberintsidentide arv kasvab üle maailma ja Eesti ei ole erand. Aastal 2017 oli nii maailmas kui ka Eestile tervikuna katsumusterohke, avastati laialt kasutuses olevate nuti- ja digiseadmete nõrkusi, lekkisid miljonite inimeste isikuandmed ning paroolid. Esiteks kasutavad meie digitaalse eluviisi sõltuvust ära rohkem kurjategijad, ehk ründeid ise on rohkem. Teiseks on paranenud intsidentide avastamise võimekus. Siin kehtib reegel - mida rohkem uuritakse, seda enam avastatakse.

Üheks näiteks on kasutajainfo (kasutajanimede ja paroolide) lekked 2016. aastal, kus oli registreeritud 1,1 miljardit juhtumit. Teiseks näiteks on 2017. aasta lõpul avaldatud 1,4 miljardi kasutaja infot sisaldav andmebaas. Lisaks ka lunavaraintsidentide hulk maailmas kasvas aastaga 36 protsenti ja pahavara levitavate e-kirjade osakaal kasvas aastaga kolmandiku võrra. Tõusuteel on ka teenustõkestusrünnete arv – 2017. aastal registreeriti üle maailma 7,5 miljonit DDoS-rünnet ja maksimaalne ründemaht on paari aastaga pea kahekordistunud. Mobiilseadmetele mõeldud pahatarkvara levik kasvab endiselt – nende arv on aasta jooksul kahekordistunud ning tuvastatud pahatarkvara levik ulatub ligi paarikümne miljoni. Ohustatud on ka järjest lisanduvad nutikad seadmed. Statistiliselt kulub keskmisel ettevõttel oma infosüsteemi kompromiteerumise avastamiseks 168 päeva (Riigi Infosüsteemi Amet, 2018). Avastamise aeg võib väheneda mitu kordselt, kui ettevõted organiseerivad oma võrkude monitooringut.

Sellised kübermaailma väljakutsed aina suurenevad ning meil tuleb selleks hästi valmis olla. Kurjategijad või ka vaenulikud riigid, kelle soov on manipuleerida infoga, teenida kuritegelikul teel hõlptulu või õõnestada vastase usaldusväärsust, kasutavad ära iga võimaluse. Sotsiaalmeedia kasutajatel tuleb olla sammuke eespool – teha kõigepealt ise kõik selleks, et talitada digimaailmas võimalikult läbimõeldult ning hoolikalt, kaitsta enda süsteeme ning vajadusel riigilt abi küsida.

Üheks sotsiaalmeedia probleemiks on seksuaalne kuritarvitamine, mille puhul varieerub ohvrite vanus alates väikestest lastest kuni täiskasvanuteni. Teooria osa 16 leheküljel käsitletakse seksuaalkuritegu probleemist. Sotsiaalmeedia roll seksuaalsel ahistamisel on iga juhtumi puhul erinev. Paljud ohvrid on oma sotsiaalvõrgustiku

kaudu ründajaga kohtunud. Seda probleemi raskendab ka noorte Interneti kasutajate valmisolek suhelda võrgus. Tavaliselt noored internetikasutajad suhtlevad võõrastega läbi sotsiaalvõrgustiku, ning pärast kohtuvad nendega isiklikult reaalses elus.
Seksuaalkuritegevus sotsiaalmeedia kaudu on üheks levinumaks kuriteoliigiks ja sotsiaalmeedia probleemiks üldiselt. See probleem põhjustas muutusi mitmes riigis. Üheks näiteks on sotsiaalvõrgustiku MySpace otsus oma teenusest 90 000 USA-s asuvat kasutajat, keda on identifitseerinud seksuaalkurjategijateks (Jones, 2009). Teiseks näiteks on Ühendkuningriigi siseministeerium 2008. aastal kasutusele võetud meetmed, mis kohustuvad kõiki politsei andmebaasis registreeritud seksuaalkurjategijaid esitada ametiasutustele oma e-posti andmeid. Politsei omakorda edastab neid sotsiaalvõrgustike teenuste pakkujatele, et võimaldada blokeerida seksuaalkurjategijate juurdepääsu platvormidele (BBC News, 2008). Sotsiaalmeedia kasutamiseks vastuvõtmine paljude kurjategijate poolt on tekitanud väljakutseid kuritegude ennetamisega tegelevatele ametnikele.

Küberrünnakud ja küberterrorism on samuti levinud kuriteoliigid sotsiaalmeedias. Küberrünnak on arvutisüsteemide, tehnoloogiast sõltuvate ettevõtete ja võrkude pahatahtlik kasutamine. Küberründajad kasutavad pahatahtlikku koodi andmete kahjustamiseks või muutmiseks, mille tagajärjeks on sellised küberkuriteod, nagu identiteedivargus. Küberrünnakute arv on viimastel aastatel suurenenud ja on tekkinud küberjulgeoleku probleemid nii inimestele, kui ka maailmale. Sotsiaalmeedia võimaldab suhelda inimestega, kellel on sotsiaalmeedia kontod. Teabe levitamine sotsiaalmeedia kaudu on kiirem ja lihtsam võrreldes mis tahes muu meediaga.

Maailmas kasutavad sotsiaalmeediat umbes 2,67 miljardit inimest ja eeldatakse, et 2020. aastaks muutub see 2,95 miljardit (Kirichenko, *et al*., 2018). Küberterrorism on samuti rünnak arvutisüsteemi, arvutiandmete, programmide ja muu teabe vastu, kuid erinevus küberrünnaku ja küberterrorismi vahel on selles, et küberterrorismi eesmärgiks on teatud piirkonna või inimrühmade vastu suunatud kuritegevus. Janczewski ja Colariki määratlevad küberterrorismi kui: „alamrühmade või salajaste isikute rünnakuid, mis on poliitiliselt motiveeritud ja mida suunatakse teabe- ja arvutisüsteemide, arvutiprogrammide ja andmete vastu, mis omakorda põhjustab vägivalda süütud isikute vastu" (Janczewski & Colarik, 2008, pp. 13–14).
Sotsiaalmeedia on küberterrorismi jaoks sobiv ala. Tänu sotsiaalsete platvormide laialdase kättesaadavusele, kasutavad terrorirühmitused sotsiaalmeediat oma

eesmärkide saavutamiseks riigi piires ja väljaspool. Tänapäeval toimub 90% küberrünnakutest sotsiaalmeedia kaudu (Aly, *et al*., 2016, pp. 1-9).

Küberrünnakute ja küberterrorismi paremaks mõistmiseks on loodud rünnaku mudel, mis võimaldab tuvastada praegust olukorda ja tulevasi küberrünnakuid. LockheedMartin Intrusion Kill Chain (IKC) mudel näitab neid etappe, mida ründaja rünnaku planeerimiseks ja elluviimiseks tavaliselt järgib. Esimeseks etapiks on sihtmärgi teabe kogumine.

Teise etappina järgneb relvastus, mis häkkerite mõistes tähendab haavatavuste jaoks pahatahtliku tarkvara arendamine.

Kolmas etapp on toimetamine, mis tähendab pahatahtliku tarkvara ülekandmist sihtkeskkonda. Neljas ja viies etapp hõlmab endas pahatahtliku tarkvara instaleerimist ja kasutamist (Galinec, *et al.,* 2017, pp. 273-286).

Sotsiaalmeedia on poliitiline vahend küberterroristide jaoks. Küberterroristid ja nende organisatsioonid hakkavad sotsiaalmeediat kasutama oma tegevuse laiendamiseks ja organiseerimiseks, kuna sotsiaalmeedia platvormid võimaldavad terroristidele oma sõnumit kiiremini ja tõhusamalt levitada. UNODC organisatsioon kirjeldas sotsiaalmeedia ohtusid ning klassifitseeris neid kategooriatesse.

Propaganda on üheks kategooriaks, mis tähendab rühmituse ideoloogia levitamist virtuaalsete vahenditega. Terroristid püüavad jõuda kaastunnetele globaalselt nn. õhutamise, värbamise ja radikaliseerumise kaudu. Mõnikord võivad levitajad olla omavahel seotud, nad on kaastundlikud terroristliku organisatsiooni ideoloogiale.

Teiseks kategooriaks on rahastamine, ehk rahaliste vahendite otsing, mis võib hõlmata otseseid lähenemisviise, e-kaubandust, virtuaalse maksesüsteemide kasutamist (krüptoraha) ja juriidiliste finantsorganisatsioonide toetust. Terroristid kasutavad sotsiaalmeediat finantskampaaniate koordineerimiseks kaasates sellega toetajaid oma tegevusele. Sellised sotsiaalmeedia platvormid nagu Facebook, WhatsApp ja Viber aitavad terroristidel kontakteeruda laia kogukonnaga. Tavaliselt toimub terroristliku tegevuse rahastamine heategevusorganisatsioonide kaudu ning annetust on võimalik teha bitcoiniga või muu meetodiga.

Üldiselt kasutavad kurjategijad sotsiaalmeediat kahel viisil. Esimene meetod hõlmab teabe edastamist ohvritele, vandenõustajatele või üldsusele. Esimene meetod on liigitatud I kategooria tegevusse. Seda kategooriat saab jagada veel kahte rühma (A ja B). A-rühm koosneb kuritegelikust käitumisest, mis toimub täielikult internetis,

näiteks kiusamine, ahistamine või jälitamine. B-rühm aga koosneb kuritegelikust tegevusest, mis toimub nii võrgus kui ka võrguühenduseta.

Teine kuritegeliku tegevuse kategooria hõlmab sotsiaalvõrgustiku kasutamist ohvrite kohta teabe kogumiseks. Nagu I kategooria, võib II kategooria samuti jagada kahte rühma. A-rühmas kasutab kuritegija sotsiaalmeediast kogutud teavet, et teha kaasaegseid kuritegusid, mida võib seostada internetipõhise kuriteoga, nt. identiteedivargus (Lohr, 2010). B-rühmas kasutab kurjategija sotsiaalvõrgustikust kogutud teavet traditsiooniliste kuritegude teostamiseks, näiteks murdvarguse tegemiseks (Komando, 2014). Teatavate isikuandmete saamiseks peavad kuritegijad jälgima ohvrite sotsiaalmeediat teatud aja jooksul. Näiteks kui kurjategija soovib teada saada ohvri füüsilist asukohta või igapäevast rutiini. Praegu toimub valdav osa sotsiaalmeediaga seotud kuritegevusest I kategooriast (Tomlinson, 2011).

Tänapäeval on sotsiaalmeedia kuritegusid lihtsam toime panna ja neid on raskem ennetada. Ahistamine võib nüüd toimuda ilma, et kurjategija kunagi suhtleks ohvriga. Tegelikult ei pea kurjategija isegi oma majast kuriteo sooritamiseks lahkuma. Samuti ei ole oluline, kas ohver asub võrgus või mitte, sest digitaalse jälje abil on ta kergesti jälgitav. Samuti võib kurjategija sotsiaalvõrgustiku vahendusel ohvrit ahistada kolmandate isikute kaudu.

Üheks levinumaks kuritegevuseks sotsiaalmeedias on andmepüük. Andmepüük hõlmab ennast paroolide, kontonumbrite ja sellega seotud teave kättesaamist. Seda teavet kasutatakse selleks, et teostada identiteedivargust. Andmepüügil saadavad kurjategijad kahtlase sisuga sõnumeid, mis kannavad pahatahtlikke programme andmete kättesaamiseks. Sageli kahtlase sisuga sõnumid näevad välja nagu õigustatud ja turvalised allikad (Leyden, 2009). Sotsiaalmeedia annab võimalusi viiruste ja tarkvara arendajatele. Kasutajad, kes klõpsavad linkidel, avavad manuseid ja reageerivad sõnumitele võrkudes, võivad saada ohvriks sellest teadmata. Selle tulemuseks on pahatahtlik reklaam, viirused ja pahavara kahjulik mõju.

2.2 Ebaseadusliku tegevuse tõkestamise meetmed sotsiaalvõrgustikudes

Küberkeskkonna kaitsmiseks on vaja aru saada riskidest, ohud ära tunda ning olla valmis keskkonda nende eest kaitsma ja võimalike tagajärgedega toime tulema. Häid

teadmisi küberkeskkonna, tehnoloogia ja selle kasutamise riskidest on tarvis nii ettevõtete ja asutuste juhtidele kui ka koolilastele.

Küberkaitse eesmärgiks on infosüsteemide vastu suunatud küberrünnakute kindlakstegemine, ennetamine ja rünnetele vastamine (Küberkaitseliit, 2009). Kuna on võimatu teadlik olla kõigest, mis küberruumis igal ajahetkel sünnib, siis keskendutakse küberkaitses sellele, mida seal ei tohi olla ja mida seal ei tohi toimuda.

Tunnustatud küberkuritegude ja tehniliste vahendite kasvav arv küberkuritegude automatiseerimiseks (sealhulgas anonüümsed failijagamise süsteemid ja tarkvaratooted arvutiviiruste arendamiseks) tähendab, et küberkuritegevuse vastane võitlus on oluliselt muutunud. Küberkuritegevus toob väljakutseid õiguskaitseasutustele nii arenenud kui ka arengumaades. Kuna info- ja sidetehnoloogia areneb nii kiiresti, eriti arengumaades, on oluline luua küberkuritegevuse vastane tõhus strateegia, mis on osa riigi küberjulgeoleku strateegiast.

Euroopa Liit (EL) on teadlik võimalikust ohust ja võtab kõik võimalikud meetmed, et tagada kõigi EL liikmesriikide ja nende elanike julgeolek. Sellega seoses on Euroopa Liit huvitatud sellest, et kõik riigid oleksid ohutuseeskirjadest teadlikud.

EL Interneti platvormide ebaseadusliku sisu poliitika tähistab väljuvate ohtude kriitilisi aspekte ning näitab, kuidas nendega toime tulla. Euroopa Komisjon oli 1. märtsil 2018.a vastu võtnud soovituse meetmeid, millega tõhusalt võidelda ebaseadusliku infosisuga. Vastu võetud soovitused tuginevad varasemale teatisele „Suurema vastutuse võitlus ebaseadusliku infosisu vastu veebipõhiste platvormidel". Komisjoni motiveerivad mured, et ebaseadusliku infosisu eemaldamine võrgus on ebapiisav. Selle all on mõeldud, et terrorismi, ebaseadusliku vihakõne või laste seksuaalse kuritarvitamise materjali õhutamine ning intellektuaalomandi õiguste rikkumine ja tarbijakaitse Internetis tuleb lahendada kogu EL'is (European Commission, 2018).

Seoses 2017.a andmelekke intsidendi avastamisega on Riigi Infosüsteemi Amet välja toonud mõned reeglid oma kasutajakontode kaitsmiseks. Kasutaja peaks vahetama paroole regulaarselt ning paroole ei tohi ristkasutada. Samuti peab olema parool tugev ja meeldejääv, seda ei tohi üles kirjutada ega teistega jagada. Lisaks tuleb kasutada kahetasemelist autentimist kõikides keskkondades, kus see on võimalik.

Eestit rünnatakse küberruumis igalt poolt ja igal ajal. Kasutatakse teiste riikide infosüsteeme, nii et USAst tehtud rünnaku taga võib olla hoopis mõni Aasia või Euroopa riik. Riigina oleme teadlikkuse ja reageerimise osas heal järjel, aga kübersõja mõistes on veel palju vaja ära teha, et saavutada vähemalt rahuldav tase (Riigi Infosüsteemi Amet, 2018).

Nagu varem oli märgitud, küberturvalisus mängib olulist rolli kuna infotehnoloogia ja internetiteenused arenevad pidevalt. Interneti ja selle hõlmava sotsiaalmeedia turvalisemaks muutmine on saanud nii uute teenuste pakkujate kui ka valitsuste poliitika lahutamatuks osaks. Küberjulgeoleku strateegiad, mis rõhutavad tähelepanu tehniliste kaitsesüsteemide arendamisele ja kasutajate harimisele küberkuritegevuse ohvriks langemise vältimiseks võivad aidata küberkuritegevuse ohu vähendamises.

Kurjategija ei ole alati seadusevastase tegevuse tagajärjetest teadlik. Karistusest mõistmine võib vähendada kuritegude arvu. Näiteks Eesti karistusseadustiku (KarS) § 213 kohaselt karistatakse rahalise karistuse või kuni kolmeaastase vangistusega neid kurjategijaid, kes tekitas teisele isikule varalise kahju arvutiprogrammiga või andmete ebaseadusliku sisestamisega, muutmisega, kustutamisega, rikkumisega, sulustamisega või muul viisil andmetöötlusprotsessi ebaseadusliku sekkumisega varalise kasu saamise eesmärgil (Karistusseadustik, 2001, § 213).

Üheks kuritegude ennetamise viisiks sotsiaalmeedias on seadusandlus. Eestis oli 2018. aastal loodud küberturvalisuse seadus, mis on tihedalt seotud ka sotsiaalmeediaga. Uue seadusega uuendatakse võrgu- ja infosüsteemide nõudeid, mis on sotsiaalmeedia lahutamatu osa. Samuti küberintsidentide ennetamise ja lahendamise põhimõtteid ning ka järelevalve täitmise kohustusi. Eestis vastutab riiklikest organisatsioonidest küberturvalisuse tagamise eest Riigi Infosüsteemi Amet (RIA). RIA arendab küberturbe strateegiat ja poliitikat ning teeb järelevalvet elutähtsa teenuse osutamiseks kasutatavate infosüsteemide ja infovarade turvameetmete rakendamise üle. Võrreldes varasemate õigusaktidega katab uus seadus ka Eesti Interneti sihtasutust ning kõiki digiteenuste pakkujaid, näiteks veebikauplusi, otsingumootori- ja pilveandmeteenuseid.

Küberturvalisuse seaduse eelnõus on välja toodud küberturvalisuse tagamise põhimõtted. Nende jälgides võib tõsta riigi ja ühiskonna turvalisuse taset ja vähendada

ohvriks langemise riskid sotsiaalmeedias. Esimeseks on isiklikkuse põhimõte, ehk süsteemi ja sellega seotud infovara turvalisuse tagamist peab korraldama selle haldaja. See põhimõtte aitab sellega, et riik ei pea kulutama lisavahendeid sotsiaalvõrgustike turvavahendite loomiseks, vaid seda peab luua sotsiaalvõrgustik ise (teenuse osutaja).

Teiseks põhimõtteks on tervikliku kaitse põhimõte, mis sätestab, et süsteemi haldaja peab kindlaks teha võimalikud ohud süsteemile ja sellega seotud infovarale ning rakendama süsteemi kaitseks kohaseid korralduslikke ja tehnilisi abinõusid. Teisisõnu luuakse kohustused sotsiaalmeedia platvormidele, mis aitavad ennetada ohude mõjud kasutajatele.
Järgmiseks põhimõtteks on kahjuliku mõju vähendamise põhimõte, mis sätestab vajalikku hoolsuse rakendamist küberintsidendi korral, et vältida küberintsidendi mõju laienemist ja võimalikku levimist teisele süsteemile.
Eelviimaseks on koostööpõhimõte, mis tähendab, et küberturvalisuse tagamisel ja küberintsidentide lahendamisel teevad osalised koostööd ja võtavad vajadusel arvesse süsteemide ja teenuste omavahelist seotust ning sõltuvust. Ekspertintervjuust Maarja Punakiga selgus, et sotsiaalvõrgustikud ei tee piisaval tasemel koostööd politseiga, seega on see üheks arengukohaks, millele tuleb tähelepanu pöörata.
Eelnimetatud põhimõtted sätestavad nõuded riigi ja ühiskonna toimimise seisukohast oluliste võrgu ja infosüsteemide pidamisele, küberintsidentide ennetamise ja lahendamise alused ning järelevalve seaduses sätestatud kohustuste täitmise üle.

Illegaalse sisu blokeerimine sotsiaalmeedia platvormidel on samuti oluline meede kuritegude ennetamiseks ja tõkkestamiseks. Peamine probleem internetisisu blokeerimisel seisneb selles, et erinevad juriidilised isikud, kes on teenusepakkujad, asuvad sageli erinevates riikides, mille tõttu ebaseadusliku sisu probleemi võidakse kohelda erinevalt. Ebaseadusliku infosisu blokeerimist raskendavad ka Interneti tehnilised omadused. Sellise sisu blokeerimiseks ei piisa teatud serveri sulgemist, kuna sisu postitanud isik võib asuda ühes riigis, kuid sisuserverid asuvad teises riigis ning domeeni nimi on registreeritud kolmandas. Selle tulemusena on nad väljaspool ühe riigi juriidilisest institutsioonist. See eeldab erinevate juriidiliste institutsioonide koostööd ja vajadust tihedalt kooskõlastada tegevusi riigiga mitte seotud sidusrühmadega. Eeltoodud probleemile tähelepanu pööramine võib suurendada turvalisuse taset.

Nagu eespool märgiti, on tähelepanu pööramine aktuaalsetele probleemidele ja nende järkjärgulisele lahendamisele üheks oluliseks kuritegevuste ennetamise sammuks sotsiaalmeedias.
Majandus- ja Kommunikatsiooniministeeriumi Küberturvalisuse strateegia 2019-2022 dokumendis on välja toodud väljakutsed ja probleemid seoses küberturvalisuse tagamisega.
Sellisteks probleemideks on piiratud spetsialiseerumisvõime, mis on Eesti kui väikese ja väheneva rahvastikuga alusprobleemiks; Puudulik tervikjuhtimine, ehk strateegiline ja ühtne koordinatsioon; Ebapiisav arusaam küberohtude ja intsidentide mõjudest ja taristu sõltuvustest, ehk ühtsete turbepõhimõtete ja standardite eiramine või puudumine; Ebapiisav küberturvalisuse alane teadlikkus ja vähene omanikutunne; Spetsialistide puudus ja ebapiisav juurdekasv, mis mõjutab kõiki strateegiliste eesmärkide täitmist; Ebapiisav teadus- ja arendustegevuse maht, mis tuleneb spetsialistide puudusest; Eesti, kui usaldusväärse ja väärtusliku rahvusvahelise partneri maine hoidmine, kuna tegemist on kiirelt muutuva ja üha tiheneva konkurentsiga valdkonnas.

Ülaltoodust võib järeldada, et problemid on olemas. Eestil on kõrge innovatiivsuse tase, kuid tegemist on kiirelt muutuva ja üha tiheneva konkurentsiga valdkonnas. Tuleb märkida, et spetsialistide puudumine raskendab olukorda Eesti jaoks.

Kokkuvõtvalt võib öelda, et küberturvalisuse tagamiseks ja ennetamiseks peavad panustama nii riik kui ka selle ametivõimud, ning sotsiaalmeedia loojad ja kasutajad. Kuritegevusteks sotsiaalmeedias on illegaalne kaubandus, andmepüük, pahatahtliku tarkvara kasutamine, identiteedivargus ja jälitamine. Ettevaatlikus ja ohutusprotseduuride järgimine on oluline ennetamise osa. Sotsiaalmeedia on kiiresti arenev valdkond, mistõttu on oluline jälgida ja mõõta nende halbu mõjusid.
On vaja tagada seda, et teatamis- ja tegutsemise menetlused oleksid võimalikult avatud ja selged. Sotsiaalmeedia juhid peaksid kehtestama lihtsaid ja läbipaistvaid ebaseadusliku infosisu teavitamise eeskirju.

Tihe koostöö kasutajate ja ametiasutuste vahel mängib olulist rolli. Kui sotsiaalmeedia kasutajal on tõendeid tõsise kuriteo või kahtluse kohta, mis kujutab endast ohtu elule või ühiskonnale, peaksid kasutajad viivitamatult teavitama õiguskaitseasutusi. Kõik liikmesriigid peaksid kehtestama asjakohased õiguslikud kohustused.

Sotsiaalmeedia kasutamises peavad olema tõhusamad vahendid ja ennetavad tehnoloogiad, et sätestada lihtsad ja läbipaistvad eeskirjad ebaseadusliku sisu teatamiseks.

Küberterrorismi vähendamisele võib kaasa aidata küberterrorismi alane terviklik haridus- ja teadlikkuse tõstmise programmid. Riik peaks tegema küberjulgeoleku alaseid koolitus- ja haridusprogramme teadlikkuse tõstmiseks. Reklaamikampaaniad ja programmid, mis hõlmavad seminare ja küberjulgeoleku näitusi võivad samuti ennetamisel kaasa aidata. Sotsiaalmeedia illegaalse sisu ja tegevuste uurimine aitab nii paremini mõista, kuidas sotsiaalmeedia mõjutab kasutajate ja kurjategivate käitumist, kui ka võimaldab kujundada sobivamaid ennetamise ja tõkkestamise meetmeid. Samas on oluliseks ennetamise meetmeks ka sotsiaalmeedia negatiivsete aspektide kindlaksmääramine ja nendele kiire reageerimine.

Narkootiliste ainete pakkumist võib sotsiaalmeedias vähendada, kui sotsiaalmeedia platvormide omanikud pööravad suurema tähelepanu illegaalse sisu blokeerimisele ja turvameetmete rakendamisele.

Andmepüügi ennetamiseks peavad ettevõtted kasutama turvalist meilide jaotamise süsteemi, et kirju ei segataks rämpsposti või andmepüügiga. Kvaliteetset viirusetõrje programmi peaks kasutama nii üksik kasutaja kui ka ettevõtted, et pahatahtlikku tarkvara ja veebilehekülgi blokeerida. Autentimine peaks toimuma veebilehekülgede igal tasandil, et vältida ründajate juurdepääsu kasutaja isiklikele andmetele.

Sotsiaalmeedia kasutajatel on võimalik oma kontot turvalisemaks muuta, kasutades privaatsusseadeid, ning kasutajad saavad määratleda, kes näevad tema profiili sisu, postitusi ja teisi andmeid. Kuna sotsiaalvõrgustiku kasutatakse veebibrauseris, siis kasutaja peaks brausereid ajakohastama ja lubama brauseri jaoks automaatsed uuendused.

Paroolide määratlemine on igal veebileheküljel oluline osa, kus kasutaja loob esmase kaitse oma profiilile. Riigi Infosüsteemi Amet näitas Eesti kasutajate 20 levinuimat parooli, mis olid võetud lekkinud andmebaasist tumeveebis. Seal loetletud paroolid ei ole turvalised, sest seda on lihtne ära arvata. See tõestab, et ohuteadlikkuse tase on Eestis üsna väike.

Ettevaatlikus klõpsates saadud linkidel on vajalik ohutusprotseduur, isegi kui lingi saatis lähedane sõber. Sellisel juhul peab saaja küsima selle sisust enne linki klõpsamist.

Enda kohta teave postitamine peab olema turvaline. Levinud viis, kuidas häkkerid saavad kontodesse sisse, on klõpsates „Unustasid parooli?“ nuppu sisselogimise lehel. Kontosse murdmiseks otsivad nad vastuseid kasutaja turvaküsimustele, näiteks sünnipäev, kodulinn, keskkooli nimetus või ema neiupõlve nimi. Turvaküsimused on vaja koostada selliselt, et vastused küsimustele oleksid ainult kasutaja mälus.

Sotsiaalmeedia kasutaja peab veenduma, et ta mõistab selle veebilehe privaatsuspoliitikat ning uurida välja, kas veebilehekülg jälgib inimeste postitatavat sisu. Samuti peab olema kasutaja ettevaatlik selle üle, keda ta sotsiaalmeedias sõbraks võtab. Sageli kasutatakse võltsprofiile identiteedivarguseks. Kuna sellised platvormid nagu Facebook ja Twitter puutuvad kokku mitmekülgse suhtlemisega geomajanduslike ja sotsiaalsete elementidega, on oluline pidevalt jälgida, kuidas nad arenevad, analüüsida, kuidas nad töötavad ja mõõta nende potentsiaali. Selles protsessis on eesmärgiks, et riigid saaksid jälgida, teavitada ja neutraliseerida sotsiaalmeedia potentsiaalselt solvavat iseloomu.

Autori järeldusel on Facebooki kasutustingimused põhjalikult ja arusaadavalt välja toodud. Nad hõlmavad kõiki ebaseadusliku tegevuse olulisi aspekte. Korraldatud küsitlusest selgus, et 40% vastajatel puuduvad piisavad teadmised keelatud kaupade osas. Teadmiste tõstmine ja kasutustingimustest põhjalik teavitamine võib olulisel määral vähendada illegaalset kauplemist Facebookis. Intsidentide vastu pole 100% kaitset, kuid valmisolek määrab turvalisuse. Küberkuritegude vastu võitlemine nõuab palju tähelepanu, teadmisi, toetust, koordineerimist ja eksperte.

KOKKUVÕTE

Sotsiaalmeedia võimaldab jagada teavet ja ideid mitmel viisil. Erinevad funktsioonid võimaldavad kasutajatel oma ideid avaldada kas kirjalikult, piltidega või videote ja helisalvestiste kaudu. Sotsiaalmeedia on ka isiklik õppevahend. On võimalik uurida, mis toimub teie kogukonnas ja kogu maailmas. Sotsiaalmeedia kõige võimsam element on selle interaktiivne olemus. Üha enam kasutatakse sotsiaalmeedia funktsionaalsust kuritegelikel eesmärkidel. Selleks, et tõkkestada küberkuritegevust, on vaja uurida kurjategijate ja tavakasutajate käitumist sotsiaalmeedias. Teadmised küberjulgeoleku valdkonnas ja nende rakendamine mängib selles olulist rolli.

Lõputöö uurimisobjektiks oli sotsiaalmeedia platvorm Facebook, mis omab kõige suurema populaarsuse ja kasutajate arvu.

Töö teema oli aktuaalne, kuna sotsiaalmeedia kasutamine on kasvavas trendis. Peaagu kõigil Euroopas elavatel on mingigi kokkupuude sotsiaalvõrgustikega, kes kasutab seda sõprade ja sugulastega ühenduses olemiseks, kes aga ärilisteks eesmärkideks, näiteks - müües kaupa või teenuseid. See viimane osa sisaldab ka endas ärilist tegevust, mis on vastuolus seadustega, olgu see siis rahavargus, ebaseadusliku sisu levitamine või isiku andmete kasutamine kuritegelikel eesmärkidel.

Probleemiks oli see, et sotsiaalmeedias toimuvad ebaseaduslikud tegevused on peaaegu nähtamatud ning ühiskonnal on ebapiisav arusaam küberohtude ja intsidentide mõjudest.

Esimeseks uurimisülesandeks oli ebaseadusliku tegevuse ülevaade sotsiaalmeedias, millest selgus, et on olemas erinevaid kuritegevuse liike, mis põhjustavad erinevat kahju. Küberkuritegevust sotsiaalmeedias kasutatakse rahapesuks, identiteedivarguseks, internetipettuseks ja küberterrorismiks.

Teiseks uurimisülesandeks anti ülevaade sotsiaalvõrgustikkude funktsionaalsusest. Sealt selgus, et uus veebi tehnoloogia Web 2.0 võimaldas luua laiemaid funktsioone sotsiaalmeedias.

Kolmandaks uurimisülesandeks oli välja selgitada sotsiaalmeedia mõju küberturvalisusele. Sellest selgus, et Euroopa Liit mõistab küberkuritegevuse

võimalikke ohte sotsiaalmeedias ja aktiivselt võitleb. EL Interneti platvormide ebaseadusliku sisu poliitika tähistab väljuvate ohtude kriitilisi aspekte ning näitab, kuidas nendega toime tulla. 2018. aasta maikuuks olid kõik Euroopa Liidu riigid kohustatud uuendama oma küberturvalisuse seadusi. Kuna Eestis varem ei olnud küberturvalisuse seadust, siis 2018. aastal oli loodud küberturvalisuse seadus. Uue seadusega uuendati võrgu- ja infosüsteemide nõudeid, küberintsidentide ennetamise ja lahendamise põhimõtteid ning ka järelevalve täitmise kohustusi. Samuti uuendatakse Eestis pidevalt küberjulgeoleku strateegiat ning praegu on Eestis kehtiv Küberturvalisuse strateegia 2019–2022. Ülaltoodust võib järeldada, et infotehnoloogia arendamisega on vaja suurendada küberjulgeoleku taset.

Neljandast uurimisülesannest selgus, et identiteedivargus on levinum kuriteo liik sotsiaalmeedias. Üks osa identiteedivargusest on andmepüük, mis hõlmab ennast paroolide, kontonumbrite ja sellega seotud teave kättesaamist. Samuti võib identiteedivargus põhjustada sellise eraelu teabe ebaseadusliku kasutamist, nagu isiku sünniaeg, sünnikoht, kodune aadress, perekonnaseis ja perekonnaliikmete nimed.

Illegaalse kaubanduse osas on tubakatooted levinum kaup. Seda näitas nii küsitluse tulemus, kui ka eksperdi vastus intervjuus Andreas Sõlega.

Küberterrorism on veel üks kuriteo liik, millele tuleb tähelepanu pöörata. Sotsiaalmeedia on küberterrorismi jaoks sobiv ala. Tänu sotsiaalsete platvormide laialdase kättesaadavusele, kasutavad terrorirühmitused sotsiaalmeediat oma eesmärkide saavutamiseks riigi piires ja väljaspool.

Tänapäeval toimub 90% küberrünnakutest internetis sotsiaalmeedia kaudu. Küberterrorismi rühmitused kasutavad sotsiaalmeediat oma tegevuse laiendamiseks ja organiseerimiseks, kuna sotsiaalmeedia platvormid pakuvad terroristidele oma sõnumit kiiremini ja tõhusamalt levitada.

Sotsiaalmeedia platvormid arenevad pidevalt ning küberkuritegevusega seotud ohud suurenevad. Sotsiaalmeedia veebilehtede kaudu loodud andmete ja ohtude hulk on suurenenud koos sotsiaalmeedia veebilehtede laialdase kasutamisega.

SUMMARY

The thesis is written in Estonian and consists of 51 pages. The thesis has been based on 68 cited sources. The topic is revelant as the use of social media is on the rise. Almost everybody living in Europe has some kind of exposure to social networks, using it to keep in touch with friends and relatives, but also for commercial purposes, for example, by selling goods or services. This last part also includes commercial activities that go against the law, be it money laundering, illegal content distribution or the use of personal data for criminal purposes. The question of how to reduce the impact of illegal activities in social media on society is a problem of thesis. The aim of the thesis is to provide possible measures to prevent crime in social media. In order to achieve the goal of the thesis, the following research tasks were set up:

1. Provide an overview of illegal activities in social media.
2. Provide an overview of social networking functionality.
3. Analyze the impact of social media on cyber security.
4. Analyze the most common forms of crime in social media.

In thesis was used documentary analysis (media texts, program descriptions and activities, written interviews, media publications, web pages). Citations and references of used sources are provided. The data is analyzed by regularities. The way to investigate information needs is an expert interview and a survey. The cyber security law and the European Commission acts are also analyzed. The work uses a qualitative research method.

VIIDATUD ALLIKATE LOETELU

Kwak, D., Kim, W., 2017. Understanding the process of social network evolution: Online-offline integrated analysis of social tie formation. *SOCIAL network theory*, 12 (5), pp. 1-16. Leitav: Ebscohost [Kasutatud 21.02.2019].

Priit, 2010. *Mis on Veeb ehk World Wide Web.* [Võrgumaterjal] Leitav: https://arvutiturve.wordpress.com/2010/05/02/mis-on-veeb-ehk-world-wide-web/ [Kasutatud 21.02.2019].

Webcache, 2013. *Mis on Internet?* [Võrgumaterjal] Leitav: http://webcache.googleusercontent.com/search?q=cache:o0nzLpwjopkJ:kingpool.hak.edu.ee/materjalid/Eksam/Mis%2520on%2520Internet.doc+&cd=1&hl=ru&ct=clnk&gl=ee [Kasutatud 21.02.2019].

Ellison, N.B., Vitak, J., Gray, R., Lampe, C., 2014. Cultivating social resources on social network sites: Facebook relationship maintenance behaviors and their role in social capital processes. *Journal of Computer-Mediated Communication*, 19 (4), pp. 855. Leitav: Ebscohost [Kasutatud 22.02.2019].

Grieve, R., Indian, M., Witteveen, K., Tolan, G.A., Marrington, J., 2013. Face-to-face or Facebook: Can social connectedness be derived online? *Computers in Human Behavior*, 29 (3), pp. 604-609. Leitav: Ebscohost [Kasutatud 22.02.2019].

Sosik, V.S., Bazarova, N.N., 2014. Relational maintenance on social network sites: How Facebook communication predicts relational escalation. *Computers in Human Behavior*, 35, pp. 124-131. Leitav: Ebscohost [Kasutatud 22.02.2019].

Hartshorn, S., 2010. 5 Differences Between Social Media and Social Networking. [Võrgumaterjal] Leitav: http://www.socialmediatoday.com/SMC/194754 [Kasutatud 23.02.2019].

Cohen, L. S., 2009. Is There A Difference Between Social Media And Social Networking? [Võrgumaterjal] Leitav: http://lonscohen.com/blog/2009/04/difference-between-social-media-and-social-networking/ [Kasutatud 23.02.2019].

Simeon E., Sitalaskshmi K. P., Doriane K., Jonelle W., Tom S., 2011. The history of social media and its impact on business. *The Journal of Applied Management & Entrepreneurship*, 16 (3) pp. 79-91. Leitav: ResearchGate [Kasutatud 23.02.2019].

Ritholz, B., 2010 History of social media. [Võrgumaterjal] Leitav: http://www.ritholtz.com/blog/2010/12/history-of-social-media/ [Kasutatud 23.02.2019].

Anon, 2016, AVAST Software. *Cybercrime.* [Võrgumaterjal] Leitav: https://www.avast.com/c-cybercrime [Kasutatud 23.02.2019].

Manning, J., 2014. Social media, definition and classes of. In K. Harvey (Ed.). *Encyclopedia of social media and politics,* p. 1158. [Võrgumaterjal] Leitav: https://www.researchgate.net/publication/290514612_Definition_and_Classes_of_Social_Media [Kasutatud 23.02.2019].

Junco, R., Heibergert, G., Loken, E., 2011. The effect of Twitter on college student engagement an grades. *Journal of Computer Assisted Learning*, 27, pp. 119-132 [Kasutatud 23.02.2019].

Andrew B., Kimi Y., 2011. The Game's 'Telephone Flash Mob' Delayed Responses to Robberies, [Võrgumaterjal] Leitav: http://latimesblogs.latimes.com/lanow/2011/08/game-rapper-twittertelephone-flash-mob-sheriff.html [Kasutatud 23.02.2019].

Steve L., 2010. How Privacy Vanishes Online, *N.Y. TIMES.* [Võrgumaterjal] Leitav: http://www.nytimes.com/2010/03/17/technology/17privacy.html?_r=0 [Kasutatud 23.02.2019].

Kim K., 2014. Burglars Use Social Media to Target Homes, *USA TODAY*. [Võrgumaterjal] Leitav: http://www.usatoday.com/story/tech/columnist/komando/2014/01/03/socialmedia-identity-theft-home-videos/4248601/ [Kasutatud 24.02.2019].

Simon T., 2011. How's Your Social Security? Burglars Monitor Facebook and Twitter to See When You're Away from Home, *DAILY MAIL.* [Võrgumaterjal] Leitav: http://www.dailymail.co.uk/sciencetech/article-2056079/Hows-socialsecurity-Burglars-monitor-Facebook-Twitter-youre-away-home.html [Kasutatud 24.02.2019].

Thaddeus H., 2012. Investigating Jurors in the Digital Age: One Click at a Time. [Võrgumaterjal] Leitav: https://kuscholarworks.ku.edu/bitstream/handle/1808/20186/03_Hoffmeister_Final.pdf;sequence=1 [Kasutatud 24.02.2019].

Shah, S., 2016. *The history of social networking.* [Võrgumaterjal] Leitav: https://www.digitaltrends.com/features/the-history-of-social-networking/ [Kasutatud 25.02.2019].

Cohn, M., 2011. *Social Media vs Social Networking.* [Võrgumaterjal] Leitav: https://www.compukol.com/social-media-vs-social-networking/ [Kasutatud 25.02.2019].

Murugesan, S., 2007, Understanding Web 2.0. *IT Professional*. 9 (4), pp. 34-41. Leitud: ResearchGate [Kasutatud 25.02.2019].

Mergel, I., 2012. The social media innovation challenge in the public sector. *Information Polity: The International Journal of Government & Democracy in the Information Age.* 17 (3/4), pp. 281-292. Leitav: Ebscohost [Kasutatud 25.02.2019].

Shirky, C., 2011. The political power of social media. Technology, the Public Sphere, and Political Change. *Foreign Affairs*, 90 (1), pp. 28-41. [Võrgumaterjal] Leitav: https://www.foreignaffairs.com/articles/2010-12-20/political-power-social-media/ [Kasutatud 25.02.2019].

Neumann, M., Elsenbroich, C., 2017. Introduction: the societal dimensions of organized crime. *Trends in Organized Crime,* 20 (1/2), pp. 1-15. Leitav: Ebscohost [Kasutatud 25.02.2019].

Sofaer, A., Goodman, S., 2001. The Transnational Dimension. *Cyber Crime and Security.* [Võrgumaterjal] Leitav: http://media.hoover.org/documents/0817999825_1.pdf [Kasutatud 26.02.2019].

Williams, S., 1991. The Double Criminality Rule and Extradition: A Comparative Analysis. *Nova Law Review.* 15 (2), pp. 581-624. [Võrgumaterjal] Leitav: https://digitalcommons.osgoode.yorku.ca/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1454&context=scholarly_works [Kasutatud 26.02.2019].

Jenkins, H., 2008. Convergence culture: Where old and new media collide. *New York University Press,* p. 282 [Võrgumaterjal] Leitav: https://www.hse.ru/data/2016/03/15/1127638366/Henry%20Jenkins%20Convergence%20culture%20where%20old%20and%20new%20media%20collide%20%202006.pdf [Kasutatud 26.02.2019].

Jurgenson, N. & Ritzer, G., 2010. Production, consumption, prosumption: The nature of capitalism in the age of the digital 'prosumer'. *Journal of Consumer Culture*, 10 (1), pp. 13–36. [Võrgumaterjal] Leitav: http://www.facoltaspes.unimi.it/files/_ITA_/COM/Production_Consumption_Prosumption_-_COM.pdf [Kasutatud 26.02.2019].

Miller, V., 2011. Understanding digital culture. *London: Sage,* pp. 171–173. [Võrgumaterjal] Leitav: https://www.academia.edu/261338/_Understanding_Digital_Culture_-_Introduction [Kasutatud 26.02.2019].

Mann, B.L., 2008. Social networking websites – A concatenation of impersonation, denigration, sexual aggressive solicitation, cyber-bullying or happy slapping videos. *International Journal of Law and Information Technology,* p. 255. [Võrgumaterjal] Leitav: http://www.ucs.mun.ca/~bmann/0_ARTICLES/Mann_Social_Netg_PrivInfoSoc_15.pdf [Kasutatud 26.02.2019].

Bazelon, E., 2011. Why facebook is after your kids. The New York Times. [Võrgumaterjal] Leitav: http://www.nytimes.com/2011/10/16/magazine/why-facebook-is-after-your-kids.html?_r¼1 &ref¼technology [Kasutatud 27.02.2019].

Hargittai, E., Boyd, D., Palfrey, J. & Schultz, J., 2011. Why parents help their children lie to Facebook about age: Unintended consequences of the 'Children's Online Privacy Protection'. [Võrgumaterjal] Leitav: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3850/3075 [Kasutatud 27.02.2019].

O'Connell, R., 2003. A typology of cybbersexploitation and on-line grooming practices. *Cyberspace Research Unit.* [Võrgumaterjal] Leitav: http://image.guardian.co.uk/sys-files/Society/documents/2003/07/17/Groomingreport.pdf [Kasutatud 27.02.2019].

Mitchell, K.J. & Ybarra, M.L., 2008. How risky are social networking sites? A comparison of places online where youth sexual solicitation and harassment occurs. *Pediatrics*, 121 (2), pp. 350–357. [Võrgumaterjal] Leitav: https://www.academia.edu/14878526/How_Risky_Are_Social_Networking_Sites_A_Comparison_of_Places_Online_Where_Youth_Sexual_Solicitation_and_Harassment_Occurs [Kasutatud 27.02.2019].

Jones, S., 2009. MySpace removes 90,000 sex offenders. [Võrgumaterjal] Leitav: http://www.guardian.co.uk/technology/2009/feb/04/myspace-social-networking-sexoffenders [Kasutatud 27.02.2019].

BBC News, 2008. Sex offenders face website bans. *BBC News.* [Võrgumaterjal] Leitav: http:// news.bbc.co.uk/1/hi/uk/7328170.stm [Kasutatud 27.02.2019].

Mullen, P. & Purcell, R., Pathe, M., 2001. Stalking: New constructions of human behaviour. *Australian and New Zealand Journal of Psychiatry*, 35 (1), pp. 9–16. [Võrgumaterjal] Leitav: https://journals.sagepub.com/doi/abs/10.1046/j.1440-1614.2001.00849.x?journalCode=anpa [Kasutatud 28.02.2019].

McGuire, B. & Wraith, A., 2000. Legal and psychological aspects of stalking: A review. *The Journal of Forensic Psychiatry*, 11 (2), pp. 316–327. [Võrgumaterjal]

Leitav:
https://www.researchgate.net/publication/233572920_Legal_and_psychological_aspects_of_stalking_A_review [Kasutatud 28.02.2019].

D'Ovidio, R. & Doyle, J., 2003. A study on cyberstalking. *FBI Law Enforcement Bulletin*, pp. 10–17. [Võrgumaterjal] Leitav:
http://victimsofcrime.org/docs/Information%20Clearinghouse/a-study-on-cyberstalking-understanding-investigative-hurdles-2003.pdf?sfvrsn=2 [Kasutatud 28.02.2019].

Alexy, E.M., Burgess, A.W., Baker, T., & Smoyak, S.A., 2005. Perceptions of cyberstalking among college students. *Brief Treatment and Crisis Intervention*, 5 (3), pp. 279–289. [Võrgumaterjal] Leitav:
http://triggered.edina.clockss.org/ServeContent?rft_id=info:doi/10.1093/brief-treatment/mhi020 [Kasutatud 28.02.2019].

Kabay, M. (1998). Anonymity and pseudonymity in cyberspace: Deindivduation, incivility and lawlessness versus freedom and privacy. *Paper presented at the Annual Conference of the European Institute for Computer Anti-virus Research.* [Võrgumaterjal] Leitav: http://www.mekabay.com/overviews/anonpseudo.pdf [Kasutatud 28.02.2019].

Morris, S., 2011. Internet troll jailed after mocking deaths of teenagers. *The Guardian.* [Võrgumaterjal] Leitav: http://www.guardian.co.uk/uk/2011/sep/13/internet-troll-jailedmocking-teenagers [Kasutatud 28.02.2019].

Smith, R., 2010. Identity theft and fraud. *Handbook of Internet crime,* pp. 273–301 [Kasutatud 28.02.2019].

Anon, 2010. The truth about social media identity theft: Perception versus reality. *BusinessWire*. [Võrgumaterjal] Leitav:
http://www.businesswire.com/news/home/20100621005370/ en/Truth-Social-Media-Identity-Theft-Perception-Reality [Kasutatud 28.02.2019].

Anon, 2011. Risk for identity theft high for social network users. [Võrgumaterjal] Leitav: http://www.myid.com/blog/risk-for-identity-theft-high-for-social-network-users/ [Kasutatud 28.02.2019].

Riigi Infosüsteemi Amet, 2018. *Küberturvalisus.* [Võrgumaterjal] Leitav: https://www.ria.ee/public/Kuberturvalisus/RIA-kuberturvalisus-2018.pdf [Kasutatud 01.03.2019].

Majandus- ja Kommunikatsiooniministeerium, 2019. *Küberjulgeoleku 2019–2022 strateegia.* Leitav: https://www.mkm.ee/sites/default/files/kuberturvalisuse_strateegia_2019-2022.pdf [Kasutatud 01.03.2019].

Riigi Infosüsteemi Amet, 2017. *Strateegia 2017– 2018.* Leitav: https://www.ria.ee/public/RIA/Dokumendid/RIA_strateegia_2017-2018.pdf [Kasutatud 01.03.2019].

Riigi Infosüsteemi Amet, 2012. *Kokkuvõte küberturvalisuse tagamisest.* Leitav: https://www.ria.ee/public/KIIK/RIA_kyberturbe_ylevaade_2012.pdf [Kasutatud 01.03.2019].

MTÜ Eesti Küberkaitseliit, 2009. *Küberkaitse - kellele ja miks?* [Võrgumaterjal] Leitav: http://kyberkaitseliit.ee/ [Kasutatud 01.03.2019].

Kikkas, K., 2016. *Kuidas saada häkkeriks (Hacker-HOWTO)*. [Võrgumaterjal] Leitav: http://www.kakupesa.net/hacker/ [Kasutatud 01.03.2019].

Karistusseadustik (2001) RT I, 13.03.2019, 77 [Kasutatud 01.03.2019].

Majandus- ja Kommunikatsiooniministeerium, 2018. [Võrgumaterjal] Leitav: https://www.mkm.ee/et/tegevused-eesmargid/infouhiskond/kuberjulgeolek#kberkuritegevus1 [Kasutatud 1.03.2019].

Riigi Infosüsteemi Amet, 2017. *Tumeveebis avaldati 1,4 miljardi kasutaja paroolide seas ka Eesti inimeste paroolid*. [Võrgumaterjal] Leitav:

https://www.ria.ee/et/uudised/tumeveebis-avaldati-14-miljardi-kasutaja-paroolide-seas-ka-eesti-inimeste-paroolid.html [Kasutatud 01.03.2019].

Kirichenko, L., Radivilova, T. & Carlsson A., 2018. *Detecting cyber threats through social network analysis: short survey*. [Võrgumaterjal] Leitav: https://www.researchgate.net/publication/316766488_Detecting_cyber_threats_through_social_network_analysis_short_survey [Kasutatud 01.03.2019].

Janczewski, L., & Colarik, A., 2008. Cyber warfare and cyber terrorism. *Information science reference,* pp. 13–14. [Võrgumaterjal] Leitav: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.670.9033&rep=rep1&type=pdf [Kasutatud 01.03.2019].

Aly, A., Macdonald, S., Jarvis, L. & Chen, T. M., 2016. Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization. *Studies in Conflict & Terrorism*, 40 (1), pp. 1-9. [Võrgumaterjal] Leitav: https://www.researchgate.net/publication/300003339_Introduction_to_the_Special_Issue_Terrorist_Online_Propaganda_and_Radicalization [Kasutatud 01.03.2019].

Galinec, D., Možnik, D. & Guberina B., 2017. Cybersecurity and cyber defence: national level strategic approach. *Automatika*, 58 (3), pp. 273-286. [Võrgumaterjal] Leitav: https://www.researchgate.net/publication/324777689_Cybersecurity_and_cyber_defence_national_level_strategic_approach [Kasutatud 01.03.2019].

Matthews, T., 2014. *Tennessee man arrested for Facebook 'like'.* [Võrgumaterjal] Leitav: _http://rt.com/usa/man-arrested-facebook-like-790/ [Kasutatud 01.03.2019].

Lohr, S., 2010. How Privacy Vanishes Online. *N.Y. TIMES*. [Võrgumaterjal] Leitav: http://www.nytimes.com/2010/03/17/technology/17privacy.html?_r=0 [Kasutatud 02.03.2019].

Komando, K., 2014. Burglars Use Social Media to Target Homes. *USA TODAY.* [Võrgumaterjal] Leitav:

http://www.usatoday.com/story/tech/columnist/komando/2014/01/03/socialmedia-identity-theft-home-videos/4248601/ [Kasutatud 02.03.2019].

Tomlinson, S., 2011. How's Your Social Security? Burglars Monitor Facebook and Twitter to See When You're Away from Home. *DAILY MAIL.* [Võrgumaterjal] Leitav: http://www.dailymail.co.uk/sciencetech/article-2056079/Hows-socialsecurity-Burglars-monitor-Facebook-Twitter-youre-away-home.html [Kasutatud 02.03.2019].

Leyden, J., 2009. *One in 200 success rate keeps phishing economy ticking over.* [Võrgumaterjal] Leitav: http://www.theregister.co.uk/2009/12/07/phishing_hit_rate [Kasutatud 02.03.2019].

European Commission, 2018. *Illegal content on online platforms*. [Võrgumaterjal] Leitav: https://ec.europa.eu/digital-single-market/en/illegal-content-online-platforms [Kasutatud 02.03.2019].

Küberturvalisuse seadus (2018) RT I, 22.05.2018, 1.

Kalda, K., 2009. *Mis on Web 2.0*. [Võrgumaterjal] Leitav: https://okia.ee/mis-on-web-20/ [Kasutatud 02.03.2019].

McFadden, C., 2018. *A Chronological History of Social Media*. [Võrgumaterjal] Leitav: https://interestingengineering.com/a-chronological-history-of-social-media [Kasutatud 01.04.2019].

European Monitoring Centre for Drugs and Drug Addiction, 2016. *The internet and drug markets*. [Võrgumaterjal] Leitav: http://www.emcdda.europa.eu/system/files/publications/2155/TDXD16001ENN_FINAL.pdf [Kasutatud 01.04.2019].

Lisa 1. Ekspertintervjuu küsimused

Eksperdid:

Maarja Punak
Politsei- ja Piirivalveamet
Kommunikatsiooni büroo, sotsiaalmeedia ja veebiturvalisuse valdkonna spetsialist

Andreas Sõlg
Maksu- ja Tolliamet
Uurimisosakond, sotsiaalmeedia jälgimise ja monitooringu kanalite spetsialist

Küsimused ekspertidele:

1. Millised on aktuaalsed küberkuritegevuse liigid sotsiaalmeedias?
2. Milliseid tõkkestamise meetmeid on võimalik kasutada?
3. Tänapäevased väljakutsed küberkuritegevuse ennetamisega sotsiaalmeedias?

Lisa 2. Küsitlus Facebooki kasutajatele

Ankeetküsitluse küsimused ja vastuse variandid:

Esimene osa

1. **Teie sugu**

a. Mees

b. Naine

2. **Teie vanus**

a. 14-17

b. 18-30

c. 31-40

d. 41-50

e. 51-60

f. 61-

3. Kui ammu te kasutate sotsiaalvõrgustikku Facebook?

a. Vähem kui 1 aasta

b. 1-5 aastat

c. 6-10 aastat

d. Rohkem kui 10 aastat

4. Kui tihti te ostate-müüte kaupu Facebookis?

a. Mitte kordagi

b. Harva

c. Sageli

d. See on minu peamine tegevus Facebookis

5. Kas te olete teadlik, millised kaubad on ebaseaduslikud müümiseks Facebookis eraisiku poolt?

a. Jah

b. Jah, kuid mitte piisavalt

c. Ei

d. Ei, aga ma tahaksin rohkem teada saada

6. **Kas te olete ise kunagi olnud tunnistajaks ebaseaduslike kaupade müümisel Facebookis?**

a. Jah
b. Ei
c. Ei ole kindel

7. **Kui jah, siis nimelt millised kaubad? (võib valida mitu vastuste variante)**

a. Mul ei olnud juhust
b. Alkohol
c. Tubakas ja tubakatooted
d. Narkootikumid
e. Ravimid
f. Muu (isiklik vastus)

8. **Kas te loete Facebookki turvaliseks kohaks kaupade ostuks ja müügiks?**

a. Jah
b. Ei
c. Ma ei tunne end täiesti turvaliselt

Teine osa

9. **Kui tihti te vahetate parooli Facebookki sisse logimiseks?**

a. Iga kord, kui ma kusagil puhkan ja mul on hea aeg
b. Sageli
c. Peaaegu ei kasuta seda funktsiooni
d. Mitte kunagi

10. **Kas te paljastate selliseid isiklikke andmeid nagu oma sünnipäeva, elukutse, elukoha, telefoni numbri?**

a. Jah
b. Osaliselt
c. Ei paljasta

11. **Kas te olete teadlik sellistest kuritegudest sotsiaalvõrgustikudes nagu isiklike andmete vargus, jälitamine, ahistamine, pahavara levitamine?**

a. Jah
b. Ei
c. Ei, aga ma tahaksin sellest rohkem teada saada
d. Ma tean pealiskaudselt
e. Ma tean pealiskaudselt ja tahaksin rohkem teada saada

12. Kas te olete kunagi langenud pettuse ohvriks Facebookis? Kui jah, siis millise pettuse? (võib valida mitu vastuste variante)

a. Mul ei ole olnud juhust
b. Isiklike andmete vargus
c. Jälitamine
d. Ahistamine
e. Pahavara (nt. viirused)
f. Materiaalne kahju, varaline kahju
g. Muu (isiklik vastus)

13. Kas teate, kuidas ennast Facebookis teha turvaliseks pettusest (privaatsusseaded, turvaline parool, funktsioonide hoolikas kasutamine)?

a. Jah, olen kursis
b. Ei
c. Ei, aga ma tahaksin rohkem teada
d. Vähesel määral
e. Ma tean midagi, kuid tahaksin rohkem teada