4. TEHNOLOOGIAKURITEOD

MARI-LIIS SÖÖT

Tulevik

Tulevikukuriteod jagunevad tehnoloogilisteks kuritegudeks ja traditsioonilisteks kuritegudeks, millel pole tehnoloogiaga pistmist (vargused, joobes juhtimine, vägivald), aga tulevikus on tehnoloogial suurem roll – peegeldab see ju üldist ühiskondlikku arengut. Seejuures ei hõlma tehnoloogiline kuritegevus üksnes küberkuritegusid, kus seadmeid ja operatsioonisüsteeme nakatatakse pahavaraga vms, vaid ka traditsioonilistest valdkondadest pärit uusi pahategusid, kuhu on lisandunud tehnoloogiline mõõde. Küberkuritegusid on toime pandud juba aastaid, kusjuures eristatakse arvutisüsteemide vastaseid kuritegusid ning kuritegusid, kus arvuti ja tehnoloogia on ainult üks paljudest kuriteo meediumidest (näiteks 60% inimkaubanduse juhtumite puhul võetakse ohvriga kontakti just suhtlusmeedias, 28% kõigist seksuaalkuritegudest on toime pandud internetti kasutades). **See, mis praegu iseloomustab peamiselt küberkuritegevust, on peatne reaalsus paljudes kuritegevuse valdkondades:** tehnoloogiast saab horisontaalne mõõde enamikus kuritegudes, kus füüsilise ja tehnoloogilise piirid kipuvad hägustuma.[14] Me ei tea, millised tuleviku tehnikaseadmed annavad halbade kavatsustega inimestele võimaluse kuritegu toime panna. Juba praegu varastatakse raha pangakaartidelt seadmetega, mis võimaldavad teha seda taskus olevalt viipekaardilt. Digitaalne valuuta on oma haavatavuse pärast sihtmärk, aga mõnel hinnangul on see tervikuna määratud väljasuremisele[15] – seda suundumust toetab suure rahapesu ja kuritegelikkuse riski tõttu ka Eesti riigi ettevaatlikkus krüptovaluutaga tegelevate ettevõtete suhtes.[16] Suurandmete kogumine ja kasutamine toob kaasa rohkem andme- ja identiteedivargusi, kus kurjategijad spetsialiseeruvad andmete edasimüügile. Pahatahtlike kätte sattunud salasõnu saab muuta, aga seni ei ole vastust, mida teha biomeetriliste andmetega, kui neid on häkitud. 3D-printimine võimaldab välja printida ka relvi ja muud ebaseaduslikku.[17] DNA manipuleerimine, narkoaine geneetilise koodiga tehtud õlle või leiva müümine, aju- või südamestimulaatori kaugteel seiskamine Parkinsoni või südamehaigel[18] on

14 Europol. 2015. Exploring Tomorrow's Organised Crime. https://www.europol.europa.eu/publications-documents/exploring-tomorrow%E2%80%99s-organised-crime

15 ERR. 08.01.2018. Hansson nimetas krüptoraha täielikuks mõttetuseks, mis peagi välja sureb. https://www.err.ee/892935/hansson-nimetas-kruptoraha-taielikuks-mottetuseks-mis-peagi-valja-sureb

16 Rahandusministeerium on ette valmistanud seaduseelnõu, millega karmistatakse krüptorahaga seotud tegevuslubade andmist. Lisaks on finantsinspektsiooni juht Kilvar Kessler hinnanud krüptorahandust väga sagedaseks kelmuste realiseerimise vahendiks (https://www.err.ee/892406/kessler-kruptorahandus-on-vaga-suur-riskikoht).

17 Europol. 2015. Exploring Tomorrow's Organised Crime. https://www.europol.europa.eu/publications-documents/exploring-tomorrow%E2%80%99s-organised-crime.

18 Goodman, M. 2015. Future Crimes. Bantam Press. Lk 392.

mõned õudusfilmilikud näited tulevikukuritegude kohta. Kuna rahvastik vananeb, kasvab ka ravimite võltsimine ja müük internetis ning lisaks personaalmeditsiinile muutuvad aktuaalseks ka personaalviirused. Organiseeritud kuritegevuse huviobjektiks ja ebaseaduslikuks kaubaks saavad e-jäätmed ehk vanad tehnoseadmed, mis on keskkonnale ja inimesele ohtlikud, aga sisaldavad väärtuslikke metalle nagu kuld, hõbe, nikkel ja pallaadium.[19] Sagenevad ka keskkonnakuriteod, kus ohustatud liike ja nendest tehtud tooteid müüakse pimeveebis.[20] Kuna kogu transport on tehnoloogiaga tihedalt seotud ning inimesed, kaubad ja teenused väga liikuvad, tekib siingi kurjategijaile hulk võimalusi. Lähituleviku kuriteoks võib kujuneda isesõitvate masinate või koduseadmete lunavaraga nakatamine, mis ei lase autot käivitada või peatada või koju süüa tellida ilma lunavara maksmata. **Arvestades seda, kui suur osa kelmustest on kolinud internetti – 10 aastaga on nn tava- ja arvutikelmuste vahekord tasakaalustunud, kusjuures arvutikelmuste arv on pidevalt kasvanud, tavakelmuste arv aga kahanenud –, võib prognoosida sarnast küberpuudutust ka teistes kuritegudes.** Sarnased trendid on ka mujal, näiteks Suurbritannias registreeritud 12 miljonist kuriteost oli 2 miljonit küberpettust, kusjuures 10% elanikest oli enda sõnul langenud mõne küberkuriteo ohvriks.[21] Eesti ohvriuuringust ilmneb seni veel üsna tagasihoidlik kontakt küberkuritegudega: ainult 1–3% tunnistab isikuandmete varastamist netist või pangakontolt raha varastamist vms.

Küberkuritegevus on maailmas enim hoogu koguv kuriteotüüp, mida on keeruline uurida ja tõkestada, sest seda pannakse toime väga kiiresti, see on rahvusvaheline ja seetõttu õiguslikult lünklik.[22] **Ilmselt ei ole meie kriminaaljustiitssüsteem valmis tehnoloogiakuritegusid ennetama ja tõkestama.** Valmisolek eeldab õiguskaitseasutustelt ja kohtutelt peale traditsiooniliste uurimis- ja õigusteadmiste ka tehnoloogiateadmist. Kui paljud eluvaldkonnad on tehnoloogiast läbi imbunud, peab seda peegeldama ka kriminaaljustiitssüsteemi töö. Selleks et jõuda keerukaid teid mööda pahavara kirjutajateni, kelle side lõpliku kuriteoga on üsna nõrk, on vaja analüüsioskusi. **Analüüs peaks olema märksa automatiseeritum kui praegune suuresti käsitööl põhinev tegevus. Suurte andmemahtude analüüsimiseks on vaja ka häid programme ja suuri arvutusvõimsusi.** Küberkuritegusid iseloomustab rahvusvaheline mõõde ning rahvusvahelisest koostööst ja teisest riigist saadud andmetest oleneb nende kuritegude avastamisel väga palju – näiteks Samoast laekunud petukirjade ja -kõnede algallikani jõudmiseks on vaja toimivat riikidevahelist õigusabi, ent Eestil pole hulga riikidega juriidilist koostööraamistikku. **Tulevikus peab suurem vastutus olema tehnoloogiaettevõtetel ja nn koodikirjutajatel, kelle vastutus seadme toimimatuse korral ei väljendu praegu õigusaktides ega ka**

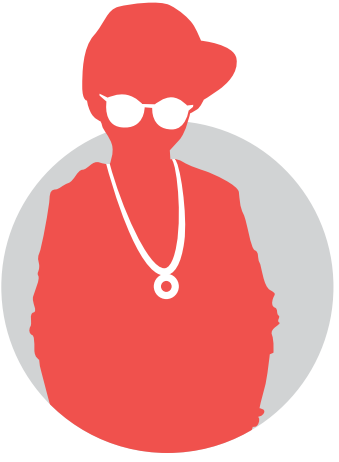
19 Europol. 2015. Exploring Tomorrow's Organised Crime. https://www.europol.europa.eu/publications-documents/exploring-tomorrow%E2%80%99s-organised-crime.

20 Pimeveeb ehk dark net tähistab seda osa internetist, mis on sageli krüpteeritud kujul peidetud ega ole avalikkusele nähtav.

21 The Telegraph. 2017. Fraud and cyber crime are now the country's most common offences. https://www.telegraph.co.uk/news/2017/01/19/fraud-cyber-crime-now-countrys-common-offences/

22 Interpol. https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

praktikas. Eeskuju saab võtta autotööstusest, mille ohutust muutsid tublisti 1960ndatel USAs loodud liiklusohutuse reeglid ja tootja vastutus – samamoodi on võimalik muuta ka tehnoloogiat turvalisemaks ja ettevõtteid vastutavamaks.[23] Samuti tuleks analüüsida, kas nn meili- ja suhtlusmeedia kontode hõivamise lahendamiseks peaks sekkuma just õiguskaitse või on selleks ehk mõni mõistlikum ja vähem kulukas viis (kaaluda õiguskaitsevälist vaheetappi).



KÜBER-KURJATEGIJA
on politsei sõnul enamasti nooremapoolne (ja iseõppinud) mees.

OLEVIK EHK KÜBERKURITEOD

205 arvutisüsteemide vastast kuritegu[24]

\+

651 arvutikelmust

56%
Arvutisüsteemide vastaste kuritegude arv kasvab

Lisaks on **28%** seksuaalkuritegudest interneti teel toime pandud.
SEKSUAAL-KURITEGUDEST

3%
Moodustavad
LUNAVARA VIIRUSEGA
nakatamised või ründed veebilehtede ja arvutisüsteemide vastu.

! Rasked küber-kuriteod on latentsed - neist ei anta üldjuhul teada.

23 Goodman, M. 2015. Future Crimes. Bantam Press, 355.

24 KarS-i §-d 206–207; 216[1]–217[1].

Lunavara viirusega nakatamise ohvriteks on sageli

need ettevõtted, kel on väärtuslikke kliendiandmeid, nagu arstipraksised, turismiettevõtted, ehitusettevõtted.

Näiteks registreeriti 2018. aastal juhtum, kus krüpteeriti ühe hooldekodu arvutid ja nõuti arvutite dekrüpteerimise eest lunaraha kuni 3 bitcoini.

Veebilehtede blokeeringute ning lunavara skeemide ohvriks on reeglina juriidilised isikud, kus blokeeringust vabastamise eest tuleb vaevatasu maksta bitcoinides – ühe bitcoini väärtus ulatus 2018. aastal 3900 eurost - 17 000 euroni[25].

Samas inimesed on oma arvutite ja andmebaaside kaitsmisest teadlikumad, mistap ei avata enam suvalisi viirusest nakatunud ekirja lisasid, ent lunavara on muutunud tõhusamaks ning kaugjuurdepääsu abil nakatakse kogu arvutisüsteem koos serveriga, mistap ei pääse omanik enam ligi ka varukoopiatele.

84 000 €

Kaotati keskmiselt pangarekvisiite muutnud kelmide tõttu.

Näide: ettevõte andis rahvusvahelisele ostjale üle 100 000 euro väärtuses kaupa kahekuulise järelmaksuga. Kuna raha ei laekunud, hakkas firma asja uurima ning selgus, et keegi sekkus nende e-kirjavahetusse ja saatis ostjale uue pangaarve, kuhu välismaine firma kandis üle poole summast, millest kaupmees jäigi ilma.

Trendikas nähtus arvutikelmide maailmas on pangarekvisiitide muutmine: sekkutakse kellegi e-posti liiklusesse ning muudetakse tehingupartneri pangarekvisiite, nii et raha kantakse tuvastamata isiku arvelduskontole tundmatus pangas – selliseid juhtumeid oli 1,5%. Mõnikord muugitakse selleks ettevõtte e-kirjavahetusse, mis sisaldab äripartnerite andmeid, ja luuakse olemasolevatele väga sarnased meiliaadressid, mille kaudu antakse teada „uuest“ kontost ning juhised edasisteks pangaülekanneteks.

25 Jürisoo, L. 2018. Bitcoini hind pole tänavu veel nii madal olnudki. Delfi. http://forte.delfi.ee/news/tarkvara/bitcoini-hind-pole-tanavu-veel-nii-madal-olnudki?id=84529911

76%

JUHTUDEL ON OHVRIKS FÜÜSILINE ISIK

Nendest enamiku moodustab ohvrite internetikonto kaaperdamine, aga ka näiteks e-kooli konto häkkimine.

Politseinikud nimetavad seda

digitaalseks perevägivallaks,

kus riidu läinud pooled maksavad teineteisele kätte, ning arvutiadministraatorid kasutavad terminit **picnic**, mis tuleneb ingliskeelsest väljendist **problem in chair, not in computer**[26] – teisisõnu on probleem sageli kehvas paroolidega või rakendustega ümberkäimises.

Näiteks kasutajad laadivad paha-aimamatult seadmesse rakendusi, küsimata, miks peaks rakendus saama ligipääsu telefonis olevatele kontaktidele, asukohale, fotodele, mikrofonile (näiteks milleks on taskulambirakendusel vaja ligipääsu telefoni kontaktidele?[27]). Tarkvara-uuendused tegemata jätnud inimene seab end lihtsaks saagiks – mõni aasta tagasi oli uuendatud tarkvara ainult 4%-l Androidi operatsiooni-süsteemi kasutajatest.[28, 29]

Registreeritud on üksikud virtuaalrahaga toime pandud pettused. Mõnel juhul lubati turule tuua uus krüptovaluuta, koguti investeeringutena raha, andes vastu uut krüptovaluutat ja siis lõpetati tegevus ning valuuta ei saanud väärtust, sest seda ei hakatud laiemalt kasutama. Aga on ka tavaliste kaardipettustega sarnanevaid skeeme, kus teise isiku virtuaalraha kontolt tehakse ülekanne tuvastamata omanikuga kontole.

Eesti Panga analüüsi kohaselt on kaardipettused pangakaartide arvu arvestades suhteliselt vähe levinud. 2016. aastal oli Eesti pangakaartidega 1000 inimese kohta 8 pettusjuhtumit, Euroopa riikides 33.[30] Suurem osa pettusi on seotud e-ostudega ning need jagunevad järgmiselt: tehingud andmepüügiga näpatud kaardiandmetega; libakaupmeestelt toodete ostmine, kus ostja ei saa kaupa; veebipoodnikelt tehingud näpatud krediitkaardiandmetega, aga ka kaardi-omaniku tehtud tehingu eest pangalt raha tagasi nõudmine.

26 Ibid, 363.

27 Ibid, 110.

28 Ibid, 108.

29 Savov. 2018. Android's trust problem isn't getting better. https://www.theverge.com/2018/4/13/17233122/android-software-patch-trust-problem

30 Uiboaid, A. 2018. Kaardipettused on kolinud internetti. Eesti Panga blogi. https://www.eestipank.ee/blogi/kaardipettused-kolinud-internetti.