Sisekaitseakadeemia

Politsei- ja piirivalvekolledž

Raido Aidak

KÜBERTERRORISM

Lõputöö

Juhendaja:

Risto Kasemäe

MPA

Koostaja:

Raido Aidak
PK090

Tallinn 2012

LÕPUTÖÖ ANNOTATSIOON

SISEKAITSEAKADEEMIA

Kolledž: Politsei- ja piirivalvekolledž	Kuu ja aasta: mai 2012
Töö pealkiri eesti keeles: Küberterrorism Töö pealkiri inglise keeles: Cyberterrorism	
Töö autor: Raido Aidak	Olen/ei ole nõus oma lõputöö kättesaadavaks tegemisega elektroonilises keskkonnas. Allkiri:
Lühikokkuvõte: Käesolev lõputöö keskendub küberterrorismi mõiste, küberterrorismiga seotud õigusaktide ning infotehnoloogiliste vahendite käsitlemisele. Lõputöö maht on 45 lehekülge. Käesoleva töö põhieesmärgid olid: 1) anda ülevaade küberterrorismi mõiste käsitlusest 2) analüüsida olemasolevaid õigusakte küberterrorismi kohta Eestis ning mujal maailmas 3) välja tuua erinevad infotehnoloogilised vahendid küberterrorismi teostamiseks ning analüüsida nende poolt tekitatud kahjustuste ulatuslikkust 4) välja pakkuda küberterrorismi mõiste Eesti õigusaktide jaoks Analüüs näitas, et küberterrorismi mõiste ei ole riikide vahel ühtselt kokku lepitud ning puuduvad ühtsed rahvusvahelised redaktsioonid ning strateegiad. Sellest tulenevalt on küberjulgeoleku tagamiseks vajalik lisaks rahvusvahelise õigusruumi arendamisele kutsuda riike üles koostama vastavat mudelseadust. Eestis on küberterrorismi mõiste välja toodud küberjulgeoleku strateegias 2008-2013, kuid välja on toodud vaid mõiste poliitiline aspekt ning seetõttu vajab see täiendamist. Küberrünnakuteks kasutatavad vahendid arenevad pidevalt ning muutuvad üha lihtsamini kättesaadavamaks ning kasutatavaks. Infotehnoloogilise pahavaraga on võimalik häirida elutähtsate teenuste toimimist ning sellest tulenevalt tõsiselt häirida riigi tööd ja ühiskondlikku korraldust. Antud tööd on võimalik kasutada üldise arusaama saamiseks küberterrorismi puudutavatest õigusaktidest ja tehnilistest vahenditest ning autori väljapakutud mõistet võiks kasutada õigusaktides. Edasistel uuringutel küberterrorismi teemal võiks keskenduda küberterrorismi ennetusele ja mudelseaduse väljatöötamisele.	
Võtmesõnad: Terrorism, küberterrorism, küberkaitse, küberrünne, õigusakt	
Võõrkeelsed võtmesõnad: Terrorism, cyberterrorism, cyber security, cyber attack, legislation	
Säilitamise koht:	
Kaitsmisele lubatud Kolledži direktor:	Allkiri:
Vastab lõputöö nõuetele: Juhendaja: Risto Kasemäe	Allkiri:

MÕISTED

Elutähtis teenus – teenus, mis on hädavajalik ühiskonna toimivuse, tervishoiu, turvalisuse ning inimeste majandusliku ja sotsiaalse heaolu korraldamiseks. (Kriitilise...09.04.2012)

Kriitiline informatsiooni infrastruktuur (KII) on info- ja kommunikatsioonisüsteemid, mille toimimine, töökindlus ja turvalisus on olulised riigi toimimise seisukohast. (Kriitilise...09.04.2012)

Küberkaitse on riigi kriitilise infrastruktuuri toimimist toetavate info- ja sidesüsteemide kaitse korraldamine, mis seisneb nii infotehnoloogiliste, organisatoorsete kui ka füüsiliste turvameetmete kasutuselevõtmises ja ajakohastamises. (Küberjulgeoleku...2008:41)

Küberrünne – arvutisüsteemi (arvuti, arvutivõrk) vahendusel toime pandud rünne arvutisüsteemi või selles sisalduvate andmete vastu eesmärgiga häirida arvutisüsteemi tööd või muuta õigusliku aluseta andmetöötlusprotsessi (muutmine, kustutamine, sulustamine jne). (Küberjulgeoleku...2008:41)

Pahavara – üldnimetus programmide kohta, mis on kirjutatud spetsiaalselt selleks, et arvutit kahjustada või kuritarvitada ja häirida või kontrollida arvutisüsteemide tööd. Pahavara jaguneb paljudesse liikidesse, näiteks viirused, ussid, troojalased jpt. (Küberjulgeoleku...2008:42)

Ping - programm sihtkohtade kättesaadavuse kontrolliks Internetis kajataotluse saatmise teel. Lisaks sellele, et ping võimaldab kindlaks teha, kas sihtkohaks olev arvuti on liinil, saab domeeninime sisestamisel teada sellele nimele vastava IP aadressi (e-Teatmik 15.04.2012)

Programmeeritav loogikakontroller - programmjuhtimisseade, mis juhib keerukat tehnoloogilist protsessi või seadet varem koostatud programmi (eeskirja ehk mällu salvestatud tarkvara) järgi. (Lehtla ja Rosin 03.03.2012:2)

Rootkit ehk juurkomplekt - teatud tüüpi *Trooja hobuse* pahavara, mis hoiab iseennast ning oma tegevuseks vajalikku failidest, registrivõtmetest ja võrguühendustest koosnevat komplekti peidetuna, nii et arvutikasutajal on võimatu avastada selle olemasolu ja tegutsemist oma arvutis. Et selline jälgede peitmine oleks võimalik, peab *Trooja hobune* looma endale juurkasutaja õigused. (e-Teatmik 12.03.2012)

SCADA – akronüüm Tehnilise Järelvalve ja Andmete Kogumise Süsteemile. SCADA juhtimissüsteeme kasutatakse tehase või seadmete järelvalveks ja kontrolliks sellistes tööstusharudes nagu telekommunikatsioon, veesüsteemide ja jäätmetekäitluse kontroll, energiatööstus, õli ja gaasi rafineerimine ning transport. (National 2004:4)

Step7 – tööstuslik kontrolltarkvara, mille eesmärk on kontrollida juhtsüsteemide ventiile ja lüliteid (tehased, tööstused). Step7 programmeerib ja monitoorib seadet nimega Programmeeritav Loogikakontroller. (Zetter 2011)

SISUKORD

Sissejuhatus

Riikide majandussüsteemid ja avalik haldus on üha enam sõltuvad IT-lahendustest, mida kasutavad nii valitsus, äriettevõtted kui ka kodanikud.

Viimaste aastate jooksul on meie sõltuvus IT-lahendustest oluliselt suurenenud. Mõne infosüsteemi mittetoimimine võib avaldada olulist mõju äriettevõtte ja/või riigiasutuse tööle ja selle kaudu ka klientide/kodanike teenindamisele. Riigi toimimise seisukohast on eriti oluline elutähtsate teenuste tagamine – vähemalt nende teenuste, mida iga päev vajame.

IT-lahenduste mittetoimimise võivad põhjustada küberrünnakud ning olenevalt juhtumist- küberterrorism. 2007. aasta sündmused Eestis näitasid maailmale, kuivõrd haavatavad on IT-süsteemid. Eesti on teinud tihedat rahvusvahelist tööd küberjulgeoleku ja –kaitse valdkonnas. NATO koostas Eesti eestvedamisel oma esimese küberjulgeoleku poliitika (Rikk 13.03.2012), 2008. aastal sai akrediteeringu NATO küberkaitse kompetentsikeskus Tallinnas.

Samas aga ei ole Eestis küberterrorismi mõistet seadusega sisustatud. Käesoleva töö eesmärk on:

1) anda ülevaade küberterrorismi mõiste käsitlusest
2) analüüsida olemasolevaid õigusakte küberterrorismi kohta Eestis ning mujal maailmas
3) välja tuua erinevad infotehnoloogilised vahendid küberterrorismi teostamiseks ning analüüsida nende poolt tekitatud kahjustuste ulatuslikkust
4) välja pakkuda küberterrorismi mõiste Eesti õigusaktide jaoks

Käesolevas töös on kasutatud peamiselt internetis olevaid materjale. Õigusaktide redaktsioonid on 17.04.2012 seisuga.

1. Küberterrorismi mõiste ja õiguslik regulatsioon

Mõiste „terrorism“ jaoks puudub ühtne ülemaailmne definitsioon. Selle tulemusena on terroriste üle riigipiiride väga raske süüdi mõista. Kuigi rahvusvahelised kokkulepped terrorismi vastu eksisteerivad, on terrorismi mõiste defineerimine jäetud riikide enda teha. Sama kehtib ka küberterrorismi mõiste kohta.

60ndate aastate alguses võttis ÜRO vastu 13 suuremat kokkulepet terrorismi kohta, nagu kaaperdamised, tuumaterrorism, mereterrorism, plastilised lõhkeained, pommitamised ja terroristide finantseerimine. Tänu neile on lihtsam asjaosalisi kohtulikule vastutusele võtta. Need 13 kokkulepet on ratifitseeritud enamikes ÜRO liikmesriikides. Kuna aga ühist mõistet nendes kokkulepetes ei defineerita, siis defineerib iga riik seda individuaalselt nii, nagu endale paremini sobib. (Goldman 2009:3)

Küberkuritegevusega võitlemine on keeruline, kuna arvutikuritegevuse liigid, kahjuulatus, motiivid ning tagajärjed varieeruvad suures ulatuses. Kuritegusid saadetakse korda majandusliku kasu saamise eesmärgil, uudishimust ja huligaansusest. Küberkuritegevusega rünnatakse infosüsteeme ning infosüsteemides paiknevaid andmeid, häiritakse teenuse pakkumist või katkestatakse teenuse töö, mõjutatakse inimesi, levitatakse ebaseaduslikku materjali jne. Küberterrorism eristub tavalistest arvutikuritegevustest selle poolest, et selle eesmärk on häirida riigi ja rahvusvaheliste organisatsioonide tööd, mõjutada ühiskondlikku korraldust või hirmutada elanikkonda.

23. novembril 2001.a koostati Budapestis Euroopa Nõukogu arvutikuritegevuse konventsioon, millega kehtestati küberkuritegevuse erinevaid aspekte hõlmav üldine ja ühtne raamistik. Tegemist on maailma ainukese kübervaldkonda reguleeriva lepinguga, mis on jõustunud enamikes Euroopa Liidu liikmesriikides ning lisaks ka USAs (Convention...09.04.2012). Konventsioon jõustus Eestis 1. juulil 2004. a.

Konventsiooni peamiseks eesmärgiks on otsida üldist kriminaalpoliitikat, mille eesmärk on kaitsta ühiskonda küberkuritegevuse vastu, rakendades asjakohast seadusandlust ja edendada rahvusvahelist koostööd. Konventsioon lähtub eeldusest, et arvutikuriteod on eeskätt varavastased kuriteod ning pannakse toime üksiküritustena. Eesti 2007. aasta kogemus aga näitab, et sisuliselt võidakse arvuteid ja võrke nii rahvaalgatuse korras kui ka organiseeritult kasutada riigi toimimise takistamiseks ning propaganda eesmärgil. Konventsiooniosalised peavad võtma seadusandlikke ja muid meetmeid, et oma seaduses määratleda kuriteona sealhulgas:

1) ebaseaduslik sisenemine arvutisüsteemi või selle osasse
2) arvutiandmete ebaseaduslik pealtkuulamine
3) andmetesse sekkumine
4) süsteemi sekkumine
5) seadmete kuritarvitamine
6) arvutiandmete võltsimine
7) arvutikelmus (Arvutikuritegevusvastane...23.11.2001)

Nimetatud süüteod võidakse korda saata ka küberterrorismi rünnakute käigus, näiteks kasutades ebaseaduslikku ligipääsu arvutisüsteemile, mitteavalike elektrooniliste andmete sulustamist, seadmete, andmete või programmide kahjustamist jne (Cohen 2010:33).

Euroopa Nõukogu Parlamentaarne Assamblee ja ka Euroopa Nõukogu mitmesugused komiteed on asunud seisukohale, et olemasolevad rahvusvahelised õigusaktid juba kriminaliseerivad küberterrorismi ning ründed arvutisüsteemide vastu ja seetõttu puudub vajadus täiendavate rahvusvahelise õiguse instrumentide järele. Rahvusvaheline õigus sätestab üksnes miinimumnõuded ning liikmesriikidel on võimalik nendest lähtudes sätestada täiendavad karistused riigisisestes õigusaktides, mida üksikud riigid on ka teinud. (Küberjulgeoleku...2008:17)

Eesti küberjulgeoleku strateegias 2008-2013 on välja toodud, et küberjulgeoleku tagamiseks on vajalik lisaks rahvusvahelise õigusruumi arendamisele kutsuda riike üles koostama vastavat mudelseadust. Mudelseadus on oma olemuselt parimaid tavasid koondav dokument, mille eeliseks on õiguspoliitiline pingevabadus ning

modifitseerimise lihtsus. Samas tuleb arvestada, et riigisiseselt on küberjulgeoleku tagamine sisuliselt osa riiklikust järelevalvest ja üldisest korrakaitsest, samuti on sellel ühisosa riigikaitselise tegevusega. (Küberjulgeoleku...2008:22)

Käesolevas peatükis tuuakse välja terrorismi ning küberterrorismi mõiste ning antakse ülevaade õigusaktidest ja strateegilistest dokumentidest Euroopa Liidus, Eestis ning USAs.

1.1 Küberterrorismi mõiste ning õigusaktid ja strateegilised dokumendid Euroopa Liidus

Euroopa Liidu institutsioonid ja liikmesriigid on arendanud oma koordinatsiooni, mehhanisme ja plaane võitlemaks terrorismiga, mis ohustab Euroopa Liitu ning selle ülemaailmseid huvisid. Eesmärk on kaitsta kodanikke, ühiskonda ja väärtusi.

Euroopa Liidu liikmesriigis Suurbritannias võeti 2000. aastal vastu terrorismi akt (*Terrorism Act of 2000)*. Selles aktis tähendab terrorism tegevuse toimepanemist või sellega ähvardamist, kus

a) 1) kaasneb tõsine vägivald isiku vastu
   2) kaasneb tõsine kahju varale
   3) ohustatakse isiku elu, väljaarvatud teo toimepanija elu
   4) luuakse tõsine risk avalikkuse (või selle osa) tervisele või turvalisusele
   5) tegevuse eesmärk on tõsiselt häirida või katkestada elektroonilisi süsteeme

a) teo toimepanek või sellega ähvardamine on kavandatud valitsuse mõjutamiseks või avalikkuse (või selle osa) hirmutamiseks

b) teo toimepanek või sellega ähvardamine on eesmärgiga esile tõsta poliitilist, religioosset või ideoloogilist alust (Goldman 2009:4)

Küberterrorismi mõistet on võimalik Suurbritannia õigusaktides käsitleda vastavalt eeltoodud punktile 5, kus on toodud välja elektrooniliste süsteemide tõsine häirimine või katkestamine.

Euroopa Liidus on oluline avaliku ja erasektori koostöö, kuna infotehnoloogiliste lahenduste pideval täiustamisel on mitmed erafirmad tihedalt seotud riigile strateegiliste teenuste ja infrastruktuuri pakkumisega. Euroopa Võrgu- ja Infoturbeamet *(European Network and Information Security Agency - ENISA)* toetab liikmesriike, Euroopa Liidu institutsioone ja ettevõtjaid võrgu- ja infoturbeprobleemide ennetamisel, nendega tegelemisel ja neile reageerimisel. Küberjulgeolekuga tegeleb ka Euroopa Liidu kriitilise infrastruktuuri kaitset ja liikmesriikide kriitilise infrastruktuuri kaitse alast koostööd ning uuringuid toetav Euroopa Kriitilise Infrastruktuuri Kaitse Programm *(EPCIP- European Programme for Critical Infrastructure Protection).* (Küberjulgeoleku...2008:24)

Euroopa Liidus võeti 2005. aastal vastu võetud raamotsus 222/2005/JSK infosüsteemide vastu suunatud rünnete kohta. Raamotsuse materiaalõiguse osa kordab põhimõtteliselt Euroopa Nõukogu konventsioonis reguleeritut. Raamotsuse puuduseks on selle kohaldatavus üksnes Euroopa Liidu liikmesriikide suhtes, kuid küberkuritegevuse puhul on tegemist märksa laiema piiriülese probleemiga. Nii konventsiooni kui ka raamotsuse puhul on puuduseks see, et need käsitlevad arvutisüsteemide vastaseid ründeid eeskätt varavastaste kuritegudena ning jätavad tagaplaanile riigi julgeolekumõõtme. Erinevaid arvutisüsteeme käsitletakse ühetaoliselt ning ei eristata suvalist arvutisüsteemi kriitilise infrastruktuuri arvutisüsteemist, samuti ei räägita neis eraldi massiliselt toime pandud rünnetest. (Küberjulgeoleku...2008:18)

Euroopa Majandus- ja Sotsiaalkomitee 2006.a arvamuses teemal "Kodanikuühiskonna osalus võitluses organiseeritud kuritegevuse ja terrorismiga" on välja toodud, et Euroopa seisab silmitsi uue ohuga: küberterrorism, mis võib halvata kogu ühiskonna. Internetioperaatorid peavad täiustama turvasüsteeme ning tegema koostööd politsei- ja õigusteenistustega, et tulla toime uut tüüpi kuritegude vastu võitlemisega.

30.03.2009.a Komisjoni teatises Euroopa Parlamendile, Nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele „Euroopa kaitsmine laiaulatuslike küberrünnakute ja häirete eest: valmisoleku, turvalisuse ja vastupidavuse suurendamine" märgitakse, et elutähtsate sideinfrastruktuuride turvalisuse ja vastupidavuse suurendamine on pikaajaline eesmärk, mille strateegia ja meetmed vajavad korrapärast hindamist. Euroopa tõhus varajase hoiatamise ja intsidentidele reageerimise süsteem

peab põhinema riikide või valitsuste infoturbeintsidentidega tegelevatel rühmadel (*Computer Emergency Response Teams* – CERTid), mis toimivad hästi, st neil on ühiselt kokkulepitud põhisuutlikkus.

Euroopa Komisjon esitas 30.09.2009 ettepaneku, millega asendati 24.veebruari 2005. aasta raamotsus 2005/222/JSK infosüsteemide vastu suunatud rünnete kohta. Ettepanekute hulgas on teabe ebaseadusliku pealtkuulamise kriminaliseerimine.

2011. aastal välja antud Euroopa Liidu terrorismivastasel tegevuskaval (*EU Action Plan on combating terrorism*) on viis tugisammast. Antud tegevuskava kaitsmise tugisamba all on eraldi välja toodud eesmärk valmistuda küberterrorismiga võitlemiseks:

1) ennetus - terrorismivastase strateegia kõige suurema väljakutsega haru, kuid väga tähtis. Eesmärk on ära hoida ühiskonnagruppide äärmuslust ning neisse uute liikmete värbamist.

2) kaitsmine – eesmärk on vähendada kodanike ja infrastruktuuri haavatavust terroristide rünnakule, kasutades erinevaid abinõusid (piiride kontroll, transpordi täiustatud turvalisus, küberkaitse)

3) jälitamine – eesmärk on otsida ja juurelda terroriste Euroopas ja väljaspool. Vajalik on jätkata ja suurendada pingutusi terroristide võrgustike paljastamiseks, takistada terroristide ning nende toetajate vahelist suhtlemist, reisimist ja tegevuste planeerimist. Samuti lõigata ära rahastamise allikad ning saada ligipääs rünnakute materjalidele, mida esitada kohtus.

4) reageerimine – eesmärk on terroristide rünnakutega toime tulla ning minimeerida tagajärgi.

5) rahvusvaheline koostöö (EU...2011).

1.2 Küberterrorismi mõiste ning õigusaktid ja strateegilised dokumendid Eestis

Vabariigi Valitsuse 17.08.2006 istungi protokolli nr 38 otsusega nr 15 kiideti heaks Eesti terrorismivastase võitluse põhialused, milles on sätestatud, et Eesti terrorismivastase võitluse üldeesmärgiks on kaitsta Eesti jurisdiktsioonile alluvate isikute turvalisust ning riigi julgeolekut. Selle saavutamiseks on vajalik süstemaatiline

ja koordineeritud tegevus terroriaktide ennetamisel, terroristide rahastamise tõkestamisel ja terrorismiga seotud hädaolukordade lahendamiseks valmisoleku tagamisel. Võitluses terrorismi vastu peab Eesti oluliseks inimõiguste ja põhivabaduste austamist.

Eesti terrorismivastase võitluse eesmärkide all on eraldi välja toodud kõrge rünnakuriskiga ja elutähtsate objektide kaitsmine. Tulenevalt terroritegevuse eesmärkidest on tõenäolisteks terroristide sihtmärkideks objektid, mille ründamine tekitab laia avalikkuse tähelepanu ning massiüritused. Rünnakute korraldamine elutähtsatele objektidele avaldab laiaulatuslikku mõju ühiskonna toimimisele. Dokumendis toodi välja vajadus riiklikult määrata kõrge rünnakuriskiga ja elutähtsad objektid ning kehtestada põhimõtted nende kaitse korraldamiseks.

2008. aasta karistusseadustiku muutmise eelnõu kohaselt loeti § 237 all terrorikuriteoks ka arvutiandmetesse sekkumine, arvutivõrgu toimimise takistamine, samuti selliste tegude toimepanemisega ähvardamine, kui see on toime pandud eesmärgiga sundida riiki või rahvusvahelist organisatsiooni midagi tegema või tegemata jätma või tõsiselt häirida riigi poliitilist, põhiseaduslikku, majanduslikku või ühiskondlikku korraldust või see hävitada või tõsiselt häirida rahvusvahelise organisatsiooni tegevust või see hävitada või tõsiselt hirmutada elanikkonda. Muudatuste eesmärgiks oli täiendada karistusseadustikku selliselt, et see oleks kooskõlas nõuetega, mis on sätestatud Euroopa Nõukogu arvutikuritegevusvastases konventsioonis (*Convention on Cybercrime*) ja Euroopa Liidu nõukogu 24. veebruari 2005. a raamotsuses infosüsteemide vastu suunatud rünnete kohta 2005/222/JSK. (Karistusseadustiku...13.04.2012:1)

Karistusseadustiku (KarS) §-s 237 kohaselt on terrorikuritegu:

1) rahvusvahelise julgeoleku vastase kuriteo toimepanemine
2) isiku vastase kuriteo toimepanemine
3) elu või tervist ohustava keskkonnavastase kuriteo toimepanemine
4) välisriigi või rahvusvahelise organisatsiooni vastu suunatud kuriteo toimepanemine
5) üldohtliku kuriteo toimepanemine
6) keelatud relva tootmine, levitamine või kasutamine
7) vara ebaseaduslik hõivamine või olulises ulatuses rikkumine või hävitamine

8) arvutiandmetesse sekkumine
9) arvutisüsteemi toimimise takistamine (Karistusseadustik, 06.06.2001).

Kuigi küberterrorismi mõistet ei ole Eesti õigusaktides veel sisustatud, on arvutiandmetesse sekkumine või arvutisüsteemi toimimise takistamine terrorikuriteo definitsioonis eraldi ära mainitud. Seega on alusbaas mõiste olemuse käsitlemiseks olemas.

Küberjulgeoleku strateegia 2008-2013 kiideti heaks Vabariigi Valitsuse 08.05.2008 korraldusega nr 201. Strateegias tuuakse välja küberrünnete jaotus ründe motiivide alusel, mille puhul eristatakse küberkuritegevust, küberterrorismi ning sõjategevust küberruumis. Küberjulgeoleku tagamise strateegilised eesmärgid on järgmised:

1) Eestis on laiaulatuslikult rakendatud astmeline turvameetmete süsteem, mis tagab Eesti riigi küberjulgeoleku
2) Eesti on väga suure infoturbealase kompetentsuse ja teadlikkusega riik
3) infosüsteemide turvalist ja laialdast kasutamist toetab proportsionaalne õiguslik regulatsioon
4) Eesti on küberjulgeoleku tõhustamiseks tehtava rahvusvahelise koostöö üks juhtriike (Küberjulgeoleku...2008:27)

Eesti küberjulgeoleku strateegias 2008-2013 on välja toodud küberründe ja küberterrorismi mõisted:

1) **Küberrünne** – arvutisüsteemi (arvuti, arvutivõrk) vahendusel toime pandud rünne arvutisüsteemi või selles sisalduvate andmete vastu eesmärgiga häirida arvutisüsteemi tööd või muuta õigusliku aluseta andmetöötlusprotsessi (muutmine, kustutamine, sulustamine jne)

2) **Küberterrorism** – arvutite või teiste kommunikatsioonivõrgustike abil toime pandud küberrünne, mille eesmärgiks on tekitada kaost või hävingut ning destabiliseerida ühiskonda teatud poliitiliste eesmärkide saavutamiseks (Küberjulgeoleku...2008:41)

Strateegias esitatud mõiste definitsiooni kohaselt on küberterrorismil vaid politiilised eesmärgid.

Hädaolukorra seaduse (HOS) § 34 on esitatud elutähtsad teenused ning antud paragrahvi lõikes 2 punktis 14 on elutähtsa teenusena nimetatud ka andmesidevõrgu toimimine. § 40 kohaselt on elutähtsa teenuse osutaja kohustatud tagama elutähtsa teenuse osutamiseks kasutatavate infosüsteemide ning nendega seotud infovarade turvameetmete alalise rakendamise. (Hädaolukorra seadus, 15.06.2009)

Siseministeeriumi poolt välja antud 2011. aasta riskianalüüside kokkuvõtte kohaselt on küberrünnak küberruumi vahenditega ja küberruumi vastu toimuv rünne eesmärgiga peatada teenuste osutamine või vähendada nende käideldavust või rikkuda andmete terviklikkust või konfidentsiaalsust. Kokkuvõttes on välja toodud mõiste ulatuslik küberrünnak, mis on küberrünnak, millega osaliselt või täielikult katkeb elutähtsa teenuse toimepidevus või tekib reaalne oht elutähtsa teenuse toimepidevuse katkemisele või mille tõttu juhtub või võib potentsiaalselt juhtuda vähemalt üks järgmistest:

1) ohtu satub paljude inimeste elu või tervis
2) tekib suur keskkonna- või varaline kahju sealhulgas füüsilisi purustusi kriitilisele infrastruktuurile;
3) tekib oluline mainekahju riigile
4) ühiskonna majandusaktiivsuse oluline langus ja ühiskonnakorralduse destabiliseerumine

Vastavalt Vabariigi Valitsuse määruse Hädaolukorrast või hädaolukorra tekkimise vahetust ohust Siseministeeriumi teavitamise kord (Vabariigi Valitsuse 06.05.2010 määrus nr 57) teavitab Riigi Infosüsteemi Amet (RIA) kindlaks tehtud küberrünnakutest elutähtsa teenuse osutaja või elutähtsa teenuse korraldaja või muu ministeeriumi või selle allasutuse infosüsteemide vastu, mille toimimine on vajalik elutähtsa teenuse osutamiseks.

Strateegilisel tasemel tegeleb infosüsteemide kaitsega Riigi Infosüsteemi Ameti kriitilise informatsiooni infrastruktuuri kaitse (KIIK) osakond, kus kogutakse ja hoitakse kriitilise informatsiooni infrastruktuuri (KII) alast teavet. Lisaks koostatakse KII alaseid riskianalüüse, töötatakse välja vastavad turvameetmed ja käivitatakse järelevalve nende järgimise üle. Kriitiline informatsiooni infrastruktuur on info- ja kommunikatsioonisüsteemid, mille toimimine, töökindlus ja turvalisus on olulised riigi toimimise seisukohast. (Kriitilise...09.04.2012)

Potentsiaalselt kõige suurema kahjuulatusega on riigi kriitilise infrastruktuuri ja selle infosüsteemide vastu suunatud küberrünnakud. Kuna ühiskonna toimimine sõltub suurel määral infotehnoloogiast, on selle haavatavus muutunud väga tõsiseks julgeolekuohuks. Kriitiliste infosüsteemide häired või toimimise katkemine võivad väga ulatuslikult mõjutada ühiskonna normaalset elutegevust ja omada ettearvamatuid tagajärgi. Kõige tõsisem oht, mis võib tuua kaasa märkimisväärseid kahjustusi on riigi kriitilise infrastruktuuri vastu suunatud küberrünne. Kriitilise infrastruktuuri küberkaitsel tuleb arvestada nii selle infotehnoloogilise ja füüsilise haavatavusega kui ka sellega, et infosüsteemide vastastikune sõltuvus suurendab haavatavust veelgi. Rike mõnes riigi jaoks elutähtsas infosüsteemis võib avaldada tugevat mõju mõne teise kriitilise infrastruktuuri ettevõtte poolt pakutavale olulisele teenusele või riigi e-teenusele. (Küberjulgeoleku...2008:10)

Vabariigi Valitsuse korralduse Ulatuslikust küberrünnakust põhjustatud hädaolukorra lahendamise plaan (Vabariigi Valitsuse 25.08.2011 korraldus nr 372) kohaselt teeb Riigi Infosüsteemi Ameti peadirektor otsuse ulatusliku küberrünnaku hädaolukorra plaani rakendamise kohta, tuginedes infoturbeintsidentide käsitlemise osakonna (CERT Eesti) poolt tehtud vormikohasele kirjalikule ettepanekule, kus muu hulgas on vajadusel arvestatud ekspertide arvamust. RIA ülesanneteks küberrünnaku korral on määrata hädaolukorra lahendamise juhtimisstruktuur, koguda ja analüüsida teavet, sh koondada teadaolevaid andmeid prognoositava mõju kohta elutähtsate teenuste toimepidavusele.

Hetkel on menetluses hädaolukorra seaduse muutmise eelnõu, mille eesmärk on tagada, et elutähtsa teenuse osutamine toimiks nii tavaolukorras kui ka olukorras, kus ei toimi välisriikides asuvad teenust tagavad infosüsteemid või elektroonilise side teenus (elektroonilise side seaduse tähenduses) välisriikidega on katkenud. Välisriikides asuvate infosüsteemide rikked ja töökatkestused ning elektroonilise side teenuse katkemine välisriikidega on olulisteks julgeolekuohtudeks, seetõttu on vajalik elutähtsate teenuste toimepidevuse tagamisel antud ohtudega arvestada. (Hädaolukorra...10.03.2012)

Tulenevalt eeltoodust võib väita, et Eesti õigusaktidega on võimalik küberterrorismi hallata läbi elutähtsate andmesidevõrkude toimimise.

1.3 Küberterrorismi mõiste ning õigusaktid ja strateegilised dokumendid USAs

Küberterrorism on globaalne nähtus ning sellest tulenevalt on oluline välja tuua ka rahvusvaheline dimensioon. USA on heaks näiteks, kuna selle riigi valitsus on teostanud arvu abinõusid küberruumi kaitseks. 2001. aasta 11. septembri terroristirünnakud muutsid täielikult rahvusvahelise turvalisuse põhimõtteid. Olemasolevad rahvusvahelise turvalisuse strateegiad on ümberhinnatud ja loodud uued strateegiad küberruumi tarbeks.

USA Kaitseministeeriumi poolt defineeritud mõiste kohaselt on terrorism kalkuleeritud seadusevastane vägivald või vägivallaga ähvardamine, selleks et sisendada hirmu. Eesmärgiks on sundida või hirmutada valitsusi või ühiskonda järgima eesmärke, mis on üldiselt poliitilised, religioossed või ideoloogilised (Goldman 2009:3). Selles definitsioonis lisandub terrorismi mõistele ka võimalus, et vägivalla tagaplaanil võib terrorismil olla ka poliitilisi, religioossed või ideoloogilisi aluseid.

USA seaduste kogu kohaselt tähendab terrorism ettekavatsetud poliitiliselt motiveeritud vägivalda, mis on toime pandud mittesõjaliste sihtmärkide vastu etniliste gruppide või salaagentide poolt. (Goldman 2009:3)

Föderaalne Juurdlusbüroo defineeris 1999. aastal küberterrorismi kui terrorismi, mis algatab või ähvardab algatada informatsiooni süsteemi ära kasutamist või rünnakut informatsiooni süsteemile. (Lewis 1999:6)

2001. aastal oli FBI definitsioon järgmine. Küberterrorism on kübervahendite kasutamine selleks, et sulgeda kriitilised riiklikud infrastruktuurid (energia, transport või riiklikud operatsioonid) eesmärgiga sundida või hirmutada valitsust või tsiviilelanikkonda (Dick 2001). Küberterrorism on ettekavatsetud poliitiliselt motiveeritud rünnak informatsiooni, arvutisüsteemide või programmide ja andmete vastu, mille tulemusena tekib vägivald tsiviilelanikkonna vastu mitteriiklike gruppide või salajase vastupanuliikumise poolt (Cyberterrorism 08.04.2012).

Küberterrorismi 2004. aasta FBI poolne definitsioon on kriminaalne tegu, mis on pandud toime arvuti või telekommunikatsiooni võimekuse abil, mille tulemus on

vägivald, häving või teenuste katkestus, eesmärgiga põhjustada hirmu, korraldades selleks segadust ja ebakindlust rahvastiku seas või eesmärgiga mõjutada valitsust või rahvastikku kohanduma kindla poliitilise, sotsiaalse või ideoloogilise plaaniga. (Lourdeau 2004)

Riikliku Infrastruktuuri Kaitsekesus, mis on Sisejulgeolekuministeeriumi allüksus USA-s defineerib küberterrorismi kui arvutitega juhitud kriminaalne tegu, mille tulemus on vägivald, häving või sihtmärkide surm eesmärgiga toota terrorit, et sundida valitsust muutma oma poliitikat. (Cyberterrorism...11.03.2012)

Obama valitsus andis 2009. aastal välja ulatusliku küberruumi poliitika ülevaate (*Cyberspace Policy Review*) aruande, mis näitab küberkaitse staatust USAs riikliku julgeoleku vaatevinklist. Aruandes teadvustati, et USA vajab endiselt küberkaitse strateegiat, mis kujundaks rahvusvahelist keskkonda ja tooks ühiste huvidega riigid kokku mitmetel teemadel nagu tehnilised standardid ja sobilikud õigusnormid, mis puudutavad territoriaalset õigusmõistmist, suveräänset vastutust ja sunni kasutamist.

Olulise aktina võiks välja tuua arvutikelmuse ja kuritarvitamise akti (*Computer Fraud and Abuse Act of 1984*), mille kohaselt peetakse kuriteoks:

1) autoriseerimata ligipääs arvutile riigikaitse alase info saamiseks eesmärgiga kahjustada Ameerika Ühendriike või saada kasu teisele riigile
2) autoriseerimata ligipääs arvutile eesmärgiga saada salastatud rahanduslikku või krediidi informatsiooni
3) autoriseerimata ligipääs arvutile, mida kasutab valitsus
4) autoriseerimata ligipääs kaitstud arvutile pettuse eesmärgiga
5) kaitstud arvuti tahtlikult kahjustamine
6) pettuslik arvutiparoolide ja muu info andmevoo liikumise jälgimine, mille eesmärk on saada ligipääs kaitstud arvutile
7) kaitstud arvuti ähvardamine eesmärgiga välja pressida raha või muud väärtuslikku. (Computer...1984)

Pärast 9/11 aset leidnud sündmusi võttis Kongress 2001. aastal vastu tuntud USA patrioodi akti (*USA PATRIOT Act*), mille eesmärk on tõrjuda terrorismi ja karistada terroriste. 2002.a kodumaa kaitse akt (*Homeland Security Act of 2002)* osana võeti vastu

küberkaitse edendamise akt (*Cyber Security Enhancement Act of 2002).* Antud aktiga suurendati karistusi, mis on seotud arvutikelmuse ja kuritarvitamise aktiga (*Computer Fraud and Abuse Act of 1984*) ning tehti järgnevad muudatused:

1) Ettevõtted saavad jagada föderaalsetele ja regionaalsetele riigiteenistujatele nende klientide elektroonilist informatsiooni (nagu elektronkirjad, suhtluskeskkondade vestlused, telefonikõnede salvestised, ostude nimekiri) ilma, et peaks kasutama ametlikke dokumente või kohtumäärust.
2) Ettevõtted võivad informatsiooni jagada ka omal initsiatiivil
3) Ettevõtted saavad ise anda hinnangu, kas tegemist on otsese ohuga riikliku turvalisuse huvide suhtes. Seadus ei täpsusta antud sõnastuse tähendust.
4) Kui ettevõte jagab informatsiooni hea usu põhimõtte järgi, siis kliendil puudub õigus ettevõtet kohtusse kaevata
5) Ettevõtted, mis annavad teada ettevõtte-sisestest turvalisuse probleemidest, on kaitstud klientide poolsete õigusvaidluste poolt ja avaldused vabad infovabaduse akti (*Freedom of Information Act)* nõuetest. (Holtzman 2003)

Praeguse seisuga ei ole rohkem laiahaardelisi küberturvalisust puudutavaid seadusakte vastu võetud (Fischer 2011). *Cybersecurity Enhancement Act of 2010* sai parlamendi heakskiidu, kuid senatit ei läbinud. Hetkel on 112. Kongressile lugemiseks esitatud *Cybersecurity Enhancement Act of 2011* eelnõu.

2. Küberterrorismi vahendid ja juhtumid

Küberterrorism muutub iga aastaga järjest aktuaalsemaks teemaks, kuna IT valdkond areneb väga kiiresti ja iga aasta tuleb esile uusi vahendeid küberrünnakuteks. Küberrünnakuteks kasutatavad vahendid muutuvad järjest lihtsamini kasutatavaks ja raskemini tõkestatavaks.

Käesolevas peatükis tuuakse välja põhilisemad küberrünnaku vahendid, mis võivad esineda küberterrorismi juhtumite puhul ning analüüsitakse juhtumeid küberterrorismi vaatenurgast.

2.1 Stuxnet

Stuxnet on ussviirus, mis avastati 2010. aasta juulis (Stuxnet...22.03.2012). Esimene teadaolev Stuxneti viiruse versioon ise loodi 2009. aasta juunis (Zetter 2011).

Ussviirus nakatab Microsoft Windowsi operatsioonisüsteeme kasutavaid arvuteid, kuid selle sihtmärgiks on Siemensi tööstustarkvara ja varustus. See on esimene avastatud pahavara, mis spioneerib ja hävitab tööstuslikke süsteeme ning sisaldab programmeeritavate loogikakontrollerite *rootkit*'i (Stuxnet...22.03.2012).

Ussviirus levib valimatult, kuid selles sisalduva pahavaralise andmekogumi sihtmärgiks on Siemensi tööstustarkvara (Siemens Supervisory Control And Data Acquisition ehk SCADA) süsteemid, mis on seadistatud juhtima ja jälgima spetsiifilisi tööstuslikke protsesse. SCADA süsteeme kasutatakse näiteks elektrijaamades (ka tuuma- ja hüdroelektrijaamades), veemajanduse, liiklusfooride, keskkonna kontroll- ja tootmissüsteemides ning transpordi juhtimiskeskustes.

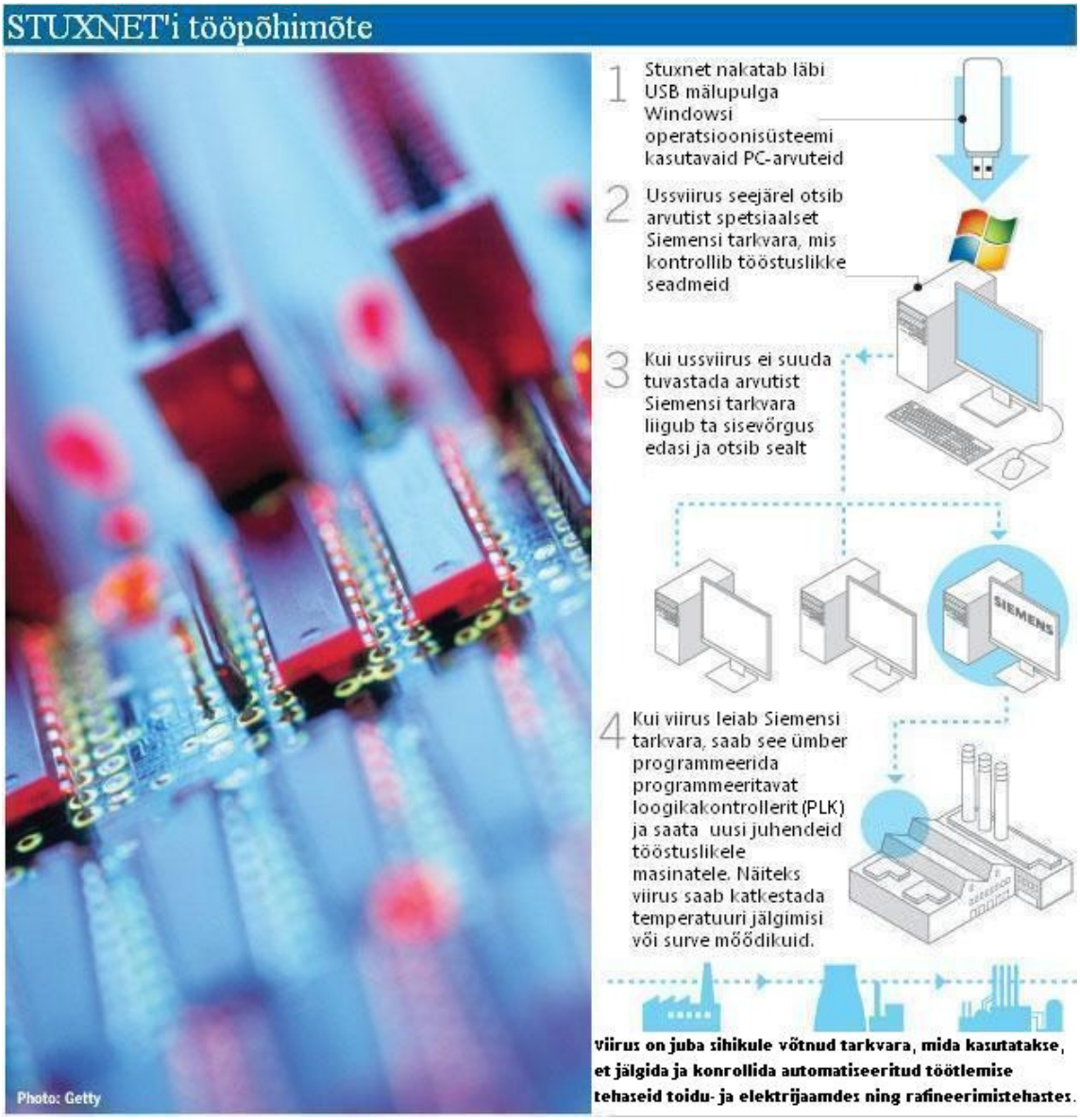
Stuxnet on relv, mis on täielikult valmistatud koodist (Stuxnet...22.03.2012). See on kõige ehtsam näide kõrgetasemelisest küberterrorismi relvastusest, mis suudab kontrollida elutähtsate teenuste arvutisüsteeme ja vastavalt vajadusele neid süsteeme välja lülitada või saboteerida. Eestis on Stuxneti-laadse ussviirusega võimalik tekitada kahju inimestele näiteks energiatööstuse või reoveepumplate saboteerimisega.

Stuxneti tööpõhimõte

Stuxnet nakatab läbi USB mälupulga Windowsi operatsioonisüsteemi kasutavaid PC-arvuteid. Stuxnet kasutas kahte kehtivat allkirjastatud sertifikaati selleks, et nakatatav arvutisüsteem ei tunneks viirust ära. Sertifikaadid olid varastatud RealTek Semiconductor ja JMicron Technology firmast.

Stuxnet kasutas korraga nelja nn null-päeva rünnet (seni avalikkusele ja tootjale teadmata turvaauku kasutavat rünnet) Windowsi operatsioonisüsteemidele:
1) Windows Exploreri LNK faili turvaauk – kui nakatunud USB mälupulk sisestati arvutisse, siis Windows Explorer automaatselt skäneeris pulgal olevat sisu. Skäneerimise hetkel aga turvaaugu kood aktiveerus ja salaja asetas suure osaliselt krüpteeritud faili arvutisse.
2) Stuxnet kasutas ära printimise trükijärjekorra turvaauku Windowsi arvutites, et levida masinate vahel, mis kasutasid jagatud printereid.
3) Stuxnet kasutas Windowsi klaviatuuri faili turvaauku, et laiendada ründajate privileege masinas ja anda neile täielik kontroll masina üle.
4) Stuxnet kasutas ülesannete planeerija (*Task Scheduler*) faili turvauku, et laiendada ründajate privileege masinas ja anda neile täielik kontroll masina üle. (Zetter 2011)

Lisaks kasutas Stuxnet staatilise salasõna turvaauku, mis oli otseselt sisse kirjutatud Step7 tarkvarasse. Stuxnet kasutas seda salasõna, et saada ligipääs ja nakatada server, mis jagas andmebaasi, mida kasutab Step7. Selle kaudu Stuxnet nakatas teisi masinaid, mis olid ühenduses serveriga. (Zetter 2011)



Joonis 1. Stuxnet'i skemaatiline illustratsioon (how...03.04.2012)

Kui Stuxnet oli arvutisüsteemi üle võtnud, võttis see ühendust kahe domeeniga – www.mypremierfutbol.com ja www.todaysfutbol.com, mis asusid Malaisia ja Taani serverites, et anda edasi informatsiooni nakatanud masinatest. Sinna hulka kuulus masina sisemine ja väline IP aadress, arvuti nimi, selle operatsioonisüsteem ja versioon ning kas Step7 tarkvara oli installeeritud masinasse (Zetter 2011). Juhul, kui nakatatud masinas ei olnud Step7 tarkvara, liikus ussviirus järgmisesse arvutisse (vt joonis 1 punkte 2 ja 3).

Kui Stuxnet tegi kindlaks, et nakatatud süsteem omas Step7 installitud tarkvara, dekrüpteeris ja laadis see pahavara DLL faili masinasse. Fail esines seadusliku DLL-na

(s7otbxdx.dll), mis toimis ühtse varamuna Step7 tarkvara funktsioonide jaoks. (Zetter 2011)

Stuxneti DLL fail püüab kinni käsklusi, mis lähevad Step7 tarkvarast programmeeritavasse loogikakontrollerisse (PLK) ja asendab need oma enda pahatahtlike käsklustega. Samal ajal Stuxnet blokeerib pahavara poolt aktiveeritud automaatalarmi. Vastavalt joonis 1 punktile 4 püüab Stuxnet kinni seadmete staatuse raportid, mis saadetakse PLK-st Step7 masinasse ja võtab maha igasugused märgid pahatahtlikest käsklustest. Seega töölised, kes monitoorivad PLK ja Step7 masinaid näevad aruannetes ainult seaduspäraseid käsklusi.

Stuxneti seadistuse failist selgus, et ussviirusel oli lõppkuupäev 24.juuni 2012, millal eeldatavalt oleks pidanud kõik eesmärgid täidetud olema (Zetter 2011).

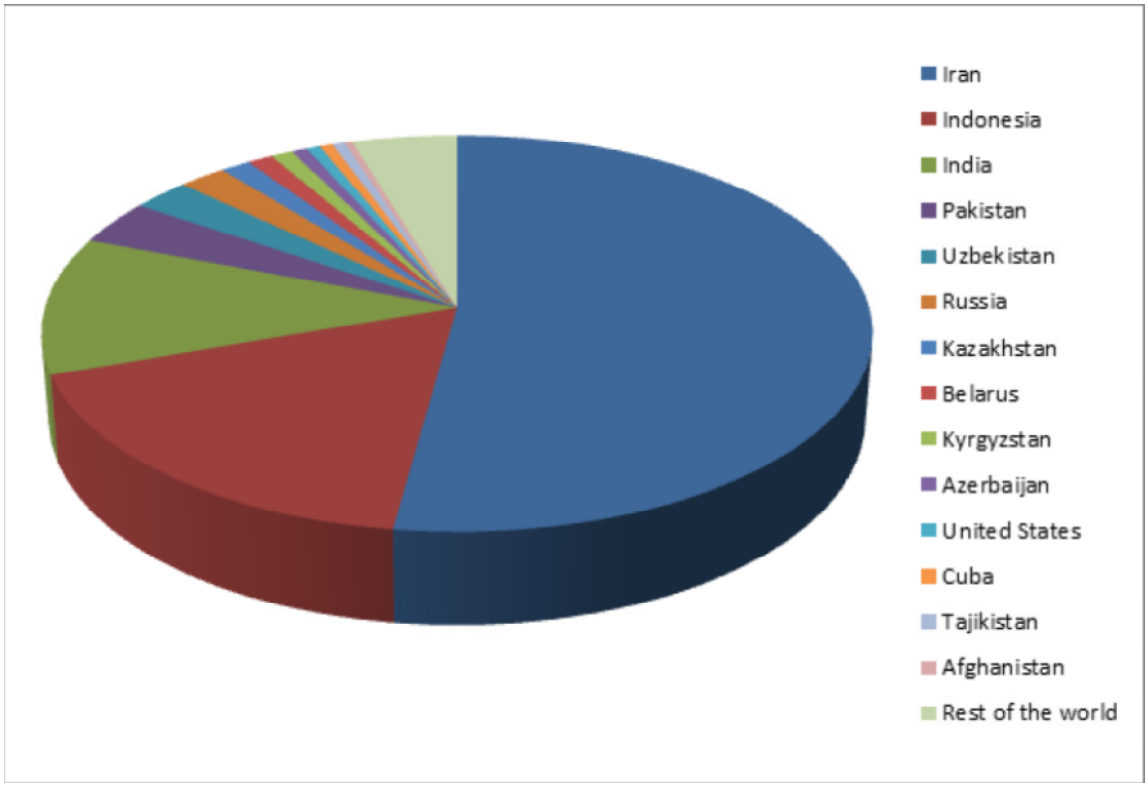
Kuna Stuxnet sisestab käsklusi PLK-sse ja varjab neid, siis võib eeltoodust järeldada, et antud ussiviirus ei ole disainitud mitte spioneerimiseks, vaid füüsiliseks saboteerimiseks.

Stuxneti juhtum

Eelmises alapeatükis nimetatud domeenide www.mypremierfutbol.com ja www.todaysfutbol.com registri haldur katkestas andmete liikumise ründajatele. Symantec'i ettepanekul pandi Stuxneti infovoog liikuma peibutusarvutisse. Nädala jooksul saadud andmed kaardistati ja imelik seaduspärasus tõusis esile. Nimelt 38 000-st nakatunud arvutist 22 000 olid Iraanis (vt joonis 2). Järgnesid Indoneesia 6 700 ning India 3 700 nakatunud arvutiga. Samas Ameerika Ühendriikidel oli vähem kui 400 nakatumist. Ainult vähestes seadmetes oli paigaldatud Step7 tarkvara - 217 masinat Iraanist ja 16 USA-st (Zetter 2011).

Iraani president Mahmoud Ahmadinejad esines teatega, et riigi vaenlased on saboteerinud Iraani Natanzi tuumajaama tsentrifuuge pahatahtliku programmiga. Ta ütles, et limiteeritud aja jooksul tekitati osadele tsentrifuugidele probleeme tarkvaraga, mis oli installeeritud elektroonilistesse osadesse. Kuid ta ei maininud midagi Stuxnetist (Zetter 2011).

Tavaliselt vahetas Iraan aastas välja 10% tuumaprogrammis kasutatavatest tsentrifuugidest materjalidefektide ja teiste põhjuste tõttu, mis teeb Natanzi 8 700 tsentrifuugi puhul umbes 870 aastas. Aastal 2010 vahetati tsentrifuuge mõne kuu jooksul 1000-2000 vahel (Zetter 2011).



Joonis 2. Globaalne nakatumine Stuxneti poolt (Matrosov, Rodionov, Harley, Malcho 15.03.2012:15)

Viiruse avastas S. Ulasen, kellele kuulus Minski arvutiturbe firma nimega VirusBlokAda**.** Nende kliendile kuuluv arvuti tabati restardi tsüklist olenemata operaatorite pingutustest see kontrolli alla saada. Selgus, et arvuti oli nakatunud viirusega ja selleks oli Stuxnet, mille oletatav eesmärk oli saboteerida Iraani tuumaprogrammi. (Zetter 2011)

2012. aastal ütlesid Reutersile Euroopa ja USA ametnikud, et Iraani insenerid on saavutanud edu Stuxneti viiruse neutraliseerimises ja puhastamises riigi tuumamasinavärgist (Hosenball 2012).

Paljud eksperdid usuvad, et Iisreal on USA abiga vastutav Stuxneti loomises ja paigaldamises kuid mingeid usaldusväärseid seletusi sellest, kes leiutas Stuxneti ja kuidas see Iraani tuumajaamade tsentrifuugide kontrollimise varustusse sattus. (Hosenball 2012)

Kuna Stuxneti eesmärk oli varjata oma süsteemi kahjustavate tegude jälgi, on see ilmselge näide sellest, et Stuxneti peamine ülesanne oli saboteerida tehases asuvaid seadmeid ning läbi selle takistada elutähtsate teenuste toimimist.

2.2 Veebi muundamine

Veebisaidi muundamine on rünnak veebilehele, mis muudab visuaalset väljanägemist saidist. Seda saadavad korda tavaliselt süsteemi kräkkerid, kes murravad sisse veebiserverisse ja vahetavad veebisaidi välja nende enda omaga. Kõige tavalisem viis veebisaidi muundamiseks on kasutada SQL sisestamist (injektsiooni), et logida sisse administraatori kasutajasse. Veebisaidi muundamised hõlmavad tavaliselt tervet saiti. Leheküljele sisestatakse tavaliselt muundaja pseudonüüm või häkkimise koodnimi. (Kanti, T.; Richariya, Vineet; Richariya, Vivek 01.04.2012)

Veebimuundajast häkkerid, kes murravad veebilehtedele sisse, võivad varastada ka personaalset infot nagu krediitkaardi numbrid, salasõnad vms. Enamasti tegeletakse veebimuundamisega kui interneti graffitiga, kuid siiski tuleb arvestada ka info varastamisega. (Kanti jt 01.04.2012)

Veebi muundamisega võivad küberterroristid ära kasutada inimeste usaldust igapäevaselt kasutataval veebilehel asuva info kohta. Näiteks võtavad veebimuundajad üle www.delfi.ee või www.valitsus.ee veebilehe ja sisestavad uudiseid kohe algavast või käimasolevast tuumarünnakust Eesti vastu või seda, et mõnes suuremas linnas on info kohaselt kohe lõhkemas mitu terroristide pommi ning soovitatakse võimalikult kiiresti linnast evakueeruda. Selle info tõttu tekib inimestes paanika ja paanikahoos tegutsedes võivad tekkida inimohvrid. Veel võib selline asi mõjuda rängalt riigi majandusele.

Veebi muundamise tehnika tööpõhimõte

SQL sisestamine on rakenduse andmebaasikihi turvanõrkus, mida põhjustab SQL lausesse lisatud muutuv väärtus, mis muudab teksti esitamise andmetüübi ebakorrektseks jadaks (osaks või nn lauseks). Tegemist on kõige tavalisema turvanõrkuse rünnakuga, kus üks programmi- või skriptikeel on manustatud teise sisse.

Kui näiteks veebilehele sisselogimise vormi sisestada õige kasutajanimi ja parooli lahtrisse kirjutada `"'OR 1=1"`, siis genereeritakse SQL-lause

```
SELECT UserList.Username
FROM UserList
WHERE
UserList.Username = 'Username'
AND UserList.Password = 'Password' OR 1=1'
```

mis annab alati tulemuseks `TRUE` ja avab juurdepääsu andmebaasile.

SQL sisestamise takistamine ei ole raske, antud näites tuleks lihtsalt vormi sisestatud jadadest ülakomad välja filtreerida (e-Teatmik 12.03.2012)

Veebi muundamise juhtumid

Veebi muundamise juhtumiteks võib lugeda United Loan Gunmen'i juhtumit ning Eesti valitsuse veebilehtede rünnak välismaa serveritest.

Grupp küberkurjategijaid ründas 1999. aastal veebimuundamisega Nasdaq/AMEX veebilehte. Grupp „United Loan Gunmen" postitas veebilehe pealkirja alla artikli nimega „United Loan Gunmen võtab Nasdaq'i aktsiaturu üle kontrolli". (Lemos 1999)

Selline tegevus võib aga tekitada avaliku hirmu aktsiaturu kokkuvarisemises, mille tulemusena hakatakse aktsiad massiliselt müüma ning võib tekkida suur finantsiline kahju mida võiks liigitada küberterrorismiks.

28. aprilli 2007. aasta öösel rünnati Reformierakonna koduleheküIge ja paigaldati sinna justkui peaminister Andrus Ansipilt pärinev vene keeles kirjutatud vabandustekst. Viimases väideti, et peaminister ja Eesti valitsus palub vene elanikkonnalt vabandust.

Samuti lubas peaminister ja valitsus, et nad toovad pronkssõduri vanale kohale tagasi. Lehekülg taastati endisel kujul mõne tunni jooksul. (Kirna 2007)

2.3 Teenusetõkestamise rünnak (Denial of Service ehk DoS)

Teenusetõkestamise rünnaku põhimõte on segada või takistada võrgu ühe osa või kogu võrguühenduse kasutamist. Teenusetõkestamise rünnak võib kasutaja sihikule võtta selleks, et takistada tal võrguga ühendust saamast. See võib samuti võtta sihikule terve organisatsiooni, et tõkestada mingi kindla võrguteenuse väljaminevat või sissetulevat võrguliiklust, nagu näiteks organisatsiooni koduleht (Denial...04.04.2012).

Teenusetõkestamise rünnakut on kerge sooritada, kui võtta üle sihikul oleva arvutisüsteemi administratiivne ligipääs. Sellepärast ongi teenuse tõkestamise rünnakud saanud internetis päris tavaliseks nähtuseks (Denial...04.04.2012).

Teenusetõkestamise rünnakud küberterrorismi vaatevinklist vaadatuna võivad mõjutada mitmeid elutähtsate teenuste valdkondi. Nimelt saab antud rünnakuga viia rivist välja side- ja infotehnoloogia servereid, kahjustatada internetipangandust ning põhjustada sellega suurt majanduslikku kahju.

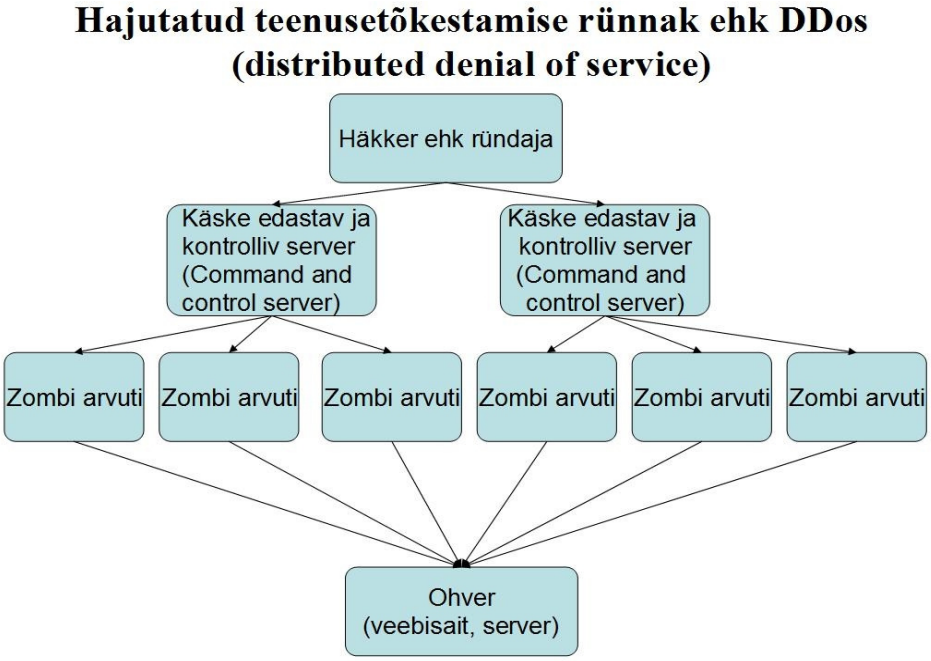
Teenusetõkestamise rünnaku tüübid

On olemas mõned klassikalised teenuse tõkestamise rünnakud. Enamus neist toetub TCP/IP protokolli nõrkustele. Müüjapoolsed lisad ja korralik võrgu konfiguratsioon on muutnud enamike teenuse tõkestamise rünnakute teostamise väga raskeks või isegi võimatuks (Denial...04.04.2012).

1) **Uputuse rünnak (*flood attack*) -** Esimene rünnakuviis teenuse tõkestamiseks oli uputuse rünnak. Ründaja lihtsalt saatis serverisse rohkem võrguliiklust, kui ohver suutis käsitseda. Uputuse rünnak nõudis ründajalt kiiremat võrguühendust, kui seda oli ohvril. See on kõige lihtsam teenuse tõkestamise ründeviis ja samas ka kõige raskemini välditav. (Denial...04.04.2012)

2) **Surmaping (*Ping of Death*) -** Ping on võrgustiku pakettsondi programm, mis kontrollib sihtkohtade kättesaadavust Internetis kajataotluse saatmise teel. (e-Teatmik 15.04.2012). Surmapingi rünnak tugines Berkeley TCP/IP veal, mis samuti eksisteeris paljudel Berkley võrgukoodi kopeerivatel süsteemidel. Surmaping lihtsalt saatis ohvrile pingpaketid suuremana kui 65,535 bitti. See teenuse tõkestamise rünnak on lihtne: Ping -1 86600 ohver.org (Denial...04.04.2012).

3) **Hajutatud teenusetõkestamise rünnak (*Distributed Denial of Service* ehk *DDos*) -** Hajutatud teenusetõkestamise rünne (DDos) on teenusetõkestamise rünne, mis pärineb paljudest erinevatest asukohadest võrgus.



Joonis 3. Hajutatud teenusetõkestamise rünnak (koostatud autori poolt)

DDos rünnakud pärinevad tavaliselt suurest arvust nakatanud süsteemidest. Need süsteemid on tavaliselt nakatunud *Trooja hobuse*, ussviiruse või mõne muu manuaalse häkkimise viisiga. (Denial...04.04.2012)

Hajutatud teenusetõkestamise ja teenusetõkestamise rünnaku Eesti juhtum (DDos ja Dos)

27.04.2007 pronkssõduri teisaldamise varjus sattus Eesti küberrünnaku alla. Rünnak hõlmas endas mitut erinevat rünnaku faasi:

1 faas – emotsionaalne vastus (27.-29. aprill) – kasutati lihtsaid teenusetõkestamise rünnakuid nagu näiteks automaatse pingi päringuid (*automated ping requests*), väärdunud veebipäringuid (*malformed web queries*). (Tikk, E., Kaska, K., Vihula, L. 2010:18)

2 faas – põhirünnak (30. aprill kuni 18. mai) – kasutati veel keerulisemaid ja paremini koordineeritud rünnakuid. Need rünnakud ilmusid nelja erineva lainena. Rünnaku märksõnadeks on suured robotvõrgustikud (*botnets*). Foorumites toimusid arutelud kuidas rahastada serverfarmide ja robotvõrgustike rentimist, et viia läbi hajutatud teenusetõkestamise rünnakut. Rünnati Elioni DNS servereid. (Tikk jt 2010:19)

Esimene laine 04.05.2007

Hajutatud teenusetõkestamise ründed jätkusid veebisaitide ja DNS serverite vastu näidates üles täpset koondumist, mis viitab robotvõrgustike kasutamisele. (Tikk jt 2010:19)

Teine laine 09-11.05.2007

Hajutatud teenusetõkestamise rünnakud kasvasid kuni 150%. Rünnakud enamasti keskendusid valitsuse veebisaitidele. Hansapank ei suutnud tänu hajutatud teenusetõkestamise rünnakule pakkuda klientidele teenuseid 1,5 tunni vältel 9. mail ja 2 tunni vältel 10. mail. (Tikk 2010:19)

Kolmas laine 15.05.2007

Tugev hajutatud teenusetõkestamise rünnak umbes 85000-st zombiarvutist koosneva robotvõrgustiku poolt. Rünnati valituse veebilehti ja SEB Eesti Ühispanka, mis oli võrgust väljas 1,5 tundi. (Tikk 2010:20)

Neljas laine 18.05.2007

Järgmine tugev hajutatud teenusetõkestamise rünnak valitsuse veebisaitide vastu. Pangad kogesid väiksemaid katkestusi. (Tikk 2010:20)

Kokkuvõtvalt toimusid mitmed teenusetõkestamise ja hajutatud teenusetõkestamise rünnakud. Esialgsetel päevadel olid rünnakud algelisemad ja kergemad, hilisemalt aga konsentreeritumad ja raskemad. Tehti kindlaks 128 unikaalset hajutatud teenusetõkestamise rünnakut, mis toimusid erinevate Eesti veebisaitide vastu.
(Tikk 2010:20)

Õigusalased probleemid

Seoses antud küberrünnakutes vastutavate isikute välja selgitamisega ja vastutusele võtmisega tekkisid mitmed probleemid menetlusõiguses. Nimelt Eesti Jälitustegevuse seaduses on sätestatud, et igasugune isikute kohta info kogumine läbi kommunikatsioonivõrkude, on rangelt määratud teostamiseks ainult jälitusasutustele. Volituseta jälitustegevus on seaduse poolt karistatav. See välistas internetiteenuste pakkujatel ja CERT'il jälgida ning analüüsida andmelogisid eesmärgiga teha kindlaks konkreetsed rünnakut sooritanud isikud. (Tikk jt 2010:26)

Kriminaalmenetluse seaduse (KrMS) § 110 lg 1 sätestab, et tõendeid võib koguda ainult järgmistel juhtudel: kui tõendite kogumine muude menetlustoimingutega on välistatud või oluliselt raskendatud ning kriminaalmenetluse esemeks on esimese astme kuritegu või tahtlikult toimepandud teise astme kuritegu, mille eest on ette nähtud karistusena vähemalt kuni kolm aastat vangistust (Kriminaalmenetluse seadus, 12.02.2003).

Kuid enamus küberrünnaku tegusid, mis pandi toime, ei andnud karistusena kolme aasta vangistust välja. Karistusseadustiku järgi kvalifitseerus enamus kuritegusid karistusega maksimum üks aasta vangistust. Seega nende kuritegude puhul ei ole jälitustegevus lubatud.

Kriminaalmenetluse seadustiku § 110 lg (1^1) küll lubab teatud juhtudel lubada tõendeid koguda üksikpäringuna jälitustoimingu raames, kuid kui arvestada Eestit rünnanud masse ei oleks see otstarbekas.

Tekkisid ka probleemid rahvusvahelisel koostöötasandil. Nimelt Venemaa ja Eesti vastastikuse abistamise lepingu kohaselt osutavad riigid üksteisele õigusabi, mis hõlmab menetluslike tegevusi seaduses ette nähtud korras ja viiakse läbi riigi poolt, kes saab selle palve. Kuid esitades Venemaa riigile õigusabi taotluse kriminaalmenetluse asjaolude välja selgitamiseks keeldus Venemaa taotluse rahuldamisest.

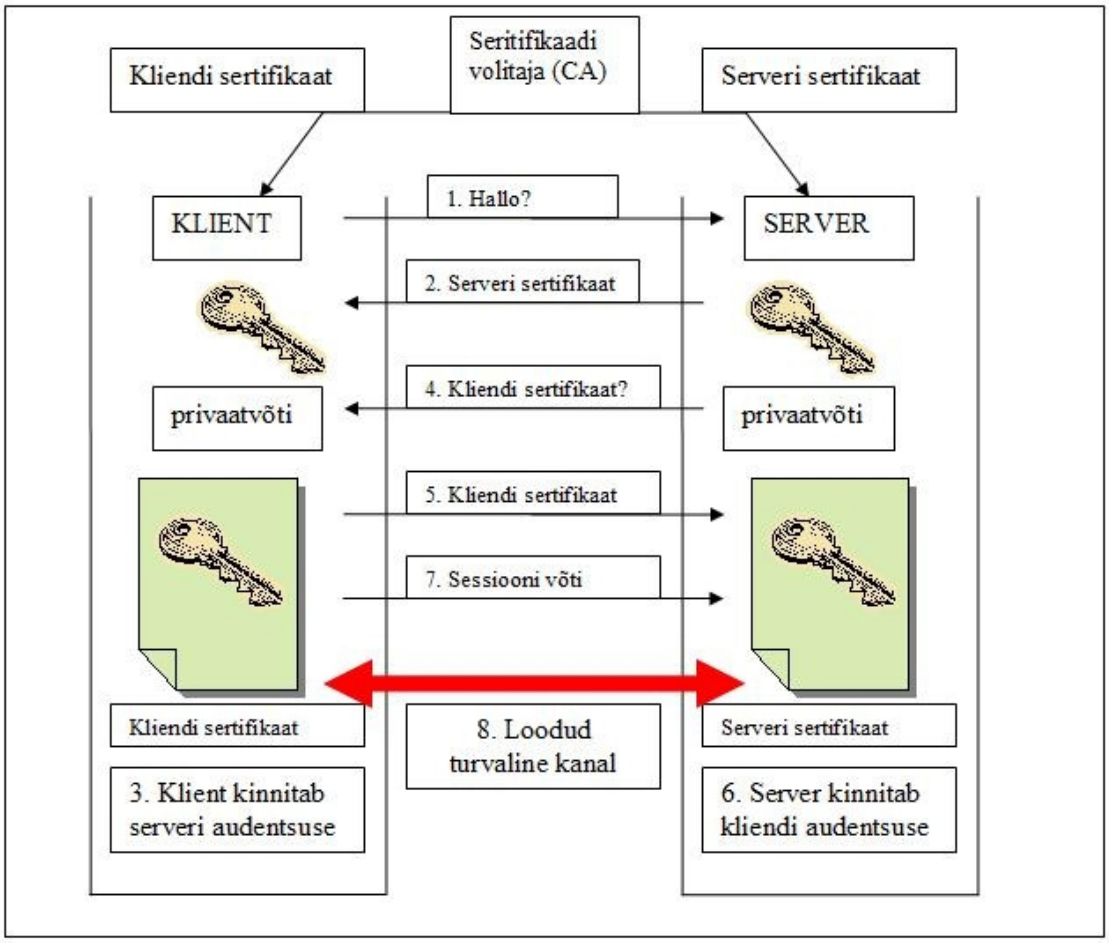
2.4 Digitaalne sertifikaat

Digitaalne sertifikaat (*digital certificate*) on tõend, mis kinnitab usalduspritsiipi SSL-krüpteeritud tehingute puhul (sisaldab avalikku võtit). Sertifikaadis on informatsioon selle väljastaja (sertifitseerimisasutuse), sertifikaadiomaniku (organisatsioon, kellele sertifikaat on väljastatud), avaliku võtme ja sertifikaadi kehtivusaja kohta (harilikult üks aasta) ning selle peremeesarvuti nimi, millel sertifikaati kasutatakse. Sertifikaadil on sertifitseerimisasutuse digitaalallkiri, nii et sertifikaadi mistahes detaili omavoliline muutmine tühistab sertifikaadi automaatselt. (Digitaalne...04.04.2012)

Kui vaadelda digiserifikaatide kasutamist küberterrorismi vahendina, võib välja tuua seda, et digitaalsed sertifikaadid annavad kinnitust allalaetavate programmide ja veebilehtede ehtsusest või digitaalse sertifikaadi olemasolu annab ligipääsu piiratud infole. Seega kui küberterroristid omavad varastatud sertifikaate, saavad nad paigaldada elutähtsate teenuste arvutisüsteemidesse pahavara ja tekitada kahju. Varastatud digitaalsete sertifikaatide kasutamine paneb kahtluse alla kõik tehingud ja andmete avaldamised, mida eelnevalt sooritati eeldades täielikku turvalisust. See omakorda kahjustab interneti usaldatavust ning võib riigile nagu Eesti, mis kasutab mitmeid riiklikke e-teenuseid, põhjustada olulist majanduslikku kahju.

Digitaalse sertifikaadi tööpõhimõte

Kui sertifikaat on installeeritud veebiserverisse lubab see kasutajal kontrollida serveri autentsust. See kindlustab, et serveril, milles organisatsioon tegutseb, on õigus kasutada serveri digitaalse sertifikaadiga seostuvat nime. See kaitseb kasutajaid usaldamast volitamata saite (How...05.04.2012).



Joonis 4. Digitaalse sertifikaadi tööpõhimõte (How...05.04.2012)

1. Kasutaja külastab turvalist veebilehekülge.
2. Server tõendab oma lehekülje identiteeti saates oma serveri sertifikaadi kliendi veebilehitsejasse.
3. Kasutaja kontrollib üle serveri autentsuse, et kindlustada selle lehekülje õigsus, mida ta külastab.
4. Server teeb päringu kliendile tema sertifikaadi kohta.
5. Kasutaja valib esitamiseks volitatud sertifikaadi.
6. Server kinnitab kliendi autentsuse, et kindlustada seda, et klient on volitatud kasutaja.

7. Kui autentimine on lõpetatud, saadab klient serveri avalikku võtit kasutades serverile krüpteeritult sessioonivõtme.
8. Turvaline kanal on loodud kliendi ja serveri vahel koos kolme fundamentaalse turvalisuse teenusega. (How...05.04.2012)

Turvaline veebiserver saab kontrollida ligipääsu ja kliendi identiteeti viidates kliendi sertifikaadile. See välistab salasõna kahekõne, mis keelab ligipääsu teatud kasutajatele (How...05.04.2012).

Nähtus, mis lubab mõlemal (serveri ja kliendi) identiteedil autentsust kinnitada läbi digitaalse sertifikaadi vahetuse ja ehtsuse kontrolli, nimetatakse vastastikuseks serveri-kliendi autentimiseks. Tehnoloogiat, mis kindlustab vastastikuse serveri-kliendi autentimist, nimetatakse SSL krüpteerimise skeemiks (How...05.04.2012).

Digitaalse sertifikaadi juhtum Diginotar

Häkkeril, kes varjub varjunime ComodoHacker taha, õnnestus sisse saada Hollandi ettevõtte DigiNotar süsteemi. DigiNotar pole lihtsalt järjekordne IT-ettevõte, vaid kuulub kitsasse usaldusväärsete firmade ringi, mis omavad juursertifikaate. (Lõugas 2011)

Sertifikaadid on kasutusel selleks, et kinnitada interneti lehekülgede ja tarkvara autentsust. Neid väljastavad vähesed ettevõtted üle maailma. Näiteks Swedbanki Eesti internetipanga õigsust kinnitab VeriSign, eesti.ee riigiportaali Thawte (Lõugas 2011). Nende hulka kuulub ka DigiNotar.

9. juulil 2011. aastal murti DigiNotari süsteemi sisse ja väljastati sadu sertifikaate, mida saaks kurjalt ära kasutada. Ettevõte küll tuvastas sissemurdmise ja proovis ka kahju vähendada. Sertifikaate on võimalik tühistada ja mõnede puhul seda ka tehti, kuid mitte kõigi puhul. (Lõugas 2011)

Kõige nimekam neist veebisaitidest, mille sertifikaat õnnestus sissemurdjatel saada, on Google.com. Kuid nimekirjas on veel palju tuntud ettevõtete ja asutuste lehekülgi nagu

Facebook, Microsoft, Yahoo!, Skype, Mossad, CIA, MI6, Twitter, WordPress jne. Kokku on nimekirjas ligi 500 veebisaiti. (Lõugas 2011)

Hollandi valitsus võttis DigiNotari häkkimist esialgu stoiliselt kinnitades, et kõik saab korda. Olukorra tõsidust taibates andis Hollandi siseminister 3. septembri öösel kell veerand kaks pressikonverentsi, milles teatati, et DigiNotari sertifikaatide usaldamine lõpetatakse, ühtlasi uuritakse Iraani valitsuse seotust häkkimisega. New York Timesi andmetel on esialgne uurimine juba näidanud, et häkkerite jäljed viivad Iraani. Hollandi valitsusele on tegelikult kogu intsident kõige valusam. Peale mainekahju on probleem ka valitsuse internetiteenustega. Kasutati kõikjal vaid omamaist sertifikaatide väljastajat. (Lõugas 2011)

DigiNotari intsident pole aga veel läbi. Mikko Hyppönen, Soome arvutiturbe guru, kirjutas, et DigiNotari varastatud sertifikaatidel oli ka võime kinnitada lisaks veebisaitidele ka arvutitarkvara ehtsust. See tähendab, et ohver võib enda arvutisse tõmmata turvauuenduse, mis tegelikult on pahalaste tehtud. (Lõugas 2011)

Kahju, mis tekkis antud Diginotar-i juhtumist Hollandi valitsuse IT infrastruktuurile on päris märkmisväärne. Palju teenuseid ei ole enam saadaval ning kommunikatsioon on häiritud. Sellepärast võib seda rünnakut pidada isegi kübersõja teoks. See juhtum paneb kindlasti küberturvalisuse ja kübersõja poliitilistesse eesmärkidesse. (Schouwenberg 2011)

Nutitelefonide domeen www.android.com oli samuti üks sihtmärgis olevatest lehekülgedest. Lauaarvutite ja sülearvutite internetilehitsejad saavad uuendusi mustas nimekirjas olevatest sertifikaatidest, kuid mobiiltelefonidele seda infot ei jagata. (Schouwenberg 2011)

2.5 Robotvõrgustikud (botnets)

Botnetiks ehk robotvõrguks (*robot network*) nimetatakse küberkurjategijate poolt kontrollitavat arvutikogumit, mis samal ajal, kui pahaaimamatud omanikud mängivad, surfavad või muid igapäevaseid toimetusi teevad, pommitab mõnd veebiserverit tühiste

päringutega, kuni see enam koormuse all vastu ei pea, serveerib porno- või piraattarkvarakollektsiooni, nakatab uusi arvuteid ja saadab laiali spämmi. (Botnet... 03.03.2012)

Kontrolli alla saamiseks rünnatakse arvutit kas mõne turvaaugu kaudu (eriti kui arvutis on vananenud ja uuendamata tarkvara), sagedamini aga pahavara abil, mis satub arvutisse kas kiirsuhtlusprogrammi või elektronposti kaudu või siis kuritahtlikke veebilehti külastades. Kui operatsioonisüsteemil on sisse lülitatud mingisugusedki turvaseaded, vajab pahavara arvutisse installeerumiseks tavaliselt kasutaja otsest kaasabi "Yes" või "Ok" nupu vajutamisega. (Botnet...03.03.2012)

Botnetti võib kuuluda miljoneid arvuteid, viimasel ajal aga näivad kurjategijad arvavat, et kõige optimaalsem ja ohutum on pidada väikesi, paarikümnest tuhandest arvutist koosnevaid botnette, millest aga täpse rünnaku jaoks täiesti piisab. Sellest hoolimata võib mõnda botnetti kuuluda iga neljas 600 miljonist internetti ühendatud arvutist. (Botnet...03.03.2012)

Vaadeldes robotvõrgustikku küberterrorismi vaatevinklist tuleb tõdeda, et antud vahend on kasutatav teenusetõkestamise rünnakute teostamiseks, mis eeltoodu põhjal võib kahjustada elutähtsate teenuste pakkumist ja põhjustada olulist majanduslikku kahju.

Joonis 5. Botneti tööpõhimõte (How...02.04.2012)

1. Robotvõrgustiku operaator saadab välja viirused nakatades tavaliste kasutajate arvuteid. Viirused koosnevad tavaliselt *trooja* rakendusest nimega robot (bot)
2. Robot nakatunud PC-s logib ennast kindlale IRC serverisse sisse või mõningatel juhtudel veebiserverisse. See server on tuntud kui juhtimise ja kontrollimise server (Command and Control, C&C)
3. Rämpspostija ostab operaatorilt ligipääsu robotvõrgustikku.
4. Rämpspostija saadab juhised läbi IRC serveri või juhtimise ja kontrollimise serveri nakatunud personaalarvutitesse, mis omakorda siis hakkavad rämpsposti levitama. (Is…04.03.2012)

Robotvõrgustiku juhtum Zeus

Zeusi kutsutakse robotvõrgustike jumalaks. Zeus on üks ohtlikumatest troojalastest, mille uute variantide vastu on võimetud paljud viirusetõrjevahendid. Kaks aastat järjest on see kohutanud finantsmaailma ja pangandust, varastades kümneid miljoneid dollareid arvutikasutajate raha. (Aasmäe 2010)

Trusteer.com turvaspetsialist Amit Klein on teatanud, et Zeus viimane täiustatud variant kasutab iseenda peitmis- ja teisendamistüüpe, samuti kernel tasandi rootkit-tehnoloogiat, mis teeb ta veelgi raskemini avastatavaks misiganes tõrjevahenditele. Tema sõnul on ohustatud kõik Windowsipõhised opisüsteemid ja peamiselt just need arvutikasutajad, kes teevad oma *online* rahaülekandeid veebilehitsejate *Mozilla Firefox* ja *Internet Explorer* vahendusel. (Aasmäe 2010)

Troojalane Zeus on olnud aktiivne juba aastast 2007. Esimene tõrjespetsialistide poolt tuvastatud rünnak toimus juulis 2007, mil püüti varastada andmeid mitmetest tuntud Ameerika Ühendriikide suurfirmadest (näiteks Hewlett-Packard Co), kusjuures ohvriks langes isegi USA Transpordiministeerium. (Aasmäe 2010)

Trusteer 2009. aasta septembri aruande järgi oli ainuüksi USA-s nakatanud 3,6 miljonit arvutit, kuid uurimustöö põhjal arvatakse, et tegelikku nakatumiste arvu võib pidada paljudes kordades suuremaks. Irooniline on veel see, et analüüsi järgi olid tervelt 55%

protsenti botnetti kuuluvatest arvutitest viirusetõrjetega kaitstud, kusjuures need olid uuendatud ka viimaste tõrjesignatuuridega. (Aasmäe 2010)

Zeus nakatab umbes 20 000 uut arvutit päevas. Tõrjespetsialistidele on selgeks saanud ka Zeus trooja loojate kavalus – selleks ajaks, kui turvaanalüütikud jõuavad selle identifitseerida ja luua vastumeetmeid kurivara kahjustamiseks, on kräkkerite poolt valmistatud juba uusim versioon pahavarast, mis jätkab edasist takistamatut tegevust. (Aasmäe 2010)

Zeus on pangandus-trooja, mis eeldatavasti pärineb Venemaalt või vähemalt vene keelt kõnelevatest Ida-Euroopa riikidest. Viimaste andmete põhjal arvatakse Zeusi loojaks olevat üksikisik. Zeus pahavarapakett on tänaseks saanud küberkurjategijate seas ülimalt populaarseks ning seda kasutatakse enim finantskuritegude kordasaatmisel. (Aasmäe 2010)

Zeus on loodud varastama kasutajate kõikvõimalikke privaatseid andmeid finantspettuste kordasaatmiseks. Sellisteks andmeteks ei pruugi alati esmajärjekorras olla ainult pankade ja e-poodide kasutajatunnused ja paroolid, vaid ka kõikvõimalike sotsiaalsete võrgustike *(Facebook, MySpace jne)* kontoandmed ja FTP ning e-mailide logimisandmed, mille abil saadakse hiljem, kui kasutaja arvuti on liidetud botnet-võrku, niikuinii ligipääs pangakontodele. (Aasmäe 2010)

Häkker, kes kasutab Zeusi, saab vajadusel lisakäskude abil kas ühte botneti liiget või tervet botnetti juhtida kontrollserverist oma tahtmise järgi. Näiteks huvitavamateks käskudeks on arvuti sulgemine või taaskäivitusele saatmine, muuta veebilehitseja kodulehte, laadida arvutisse faile, kaustu ja pahavaralisi programme, varastada digisertifikaate, muuta ja modifitseerida arvutis olevaid faile ja registrivõtmeid (%systemroot%\system32\drivers\etc\hosts) või siis enesehävitamise käsk KOS (kill operating system), mis võimaldab kräkkeril kaugjuhtimise teel kustutada olulisi süsteemifaile, mille tulemusel ei laadi opisüsteem enam üles ja sageli peale seda tuleb kasutajal uus süsteem asemele installeerida. (Aasmäe 2010)

3. Järeldused ja ettepanekud

Küberrünnakute infotehnoloogilised vahendid arenevad pidevalt ning seoses sellega suureneb ka küberterrorismi esinemise tõenäosus. Stuxnet'i ussviirus on võimeline kontrollima tööstustarkvara ning sellest tulenevalt võib takistada elutähtsate teenuste toimimist. Taolise rünnaku ohtlikkust näitab Iraani tuumajaama nakatumine.

Maailmas puudub ühtne seadusandlus küberterrorismiga tegelemiseks. Riikidevahelised ja organisatsioonide-sisesed küberterrorismi definitsioonid ei ühti. Sellest tulenevalt on küberjulgeoleku tagamiseks on küberjulgeoleku tagamiseks vajalik lisaks rahvusvahelise õigusruumi arendamisele kutsuda riike üles koostama vastavat mudelseadust.

Eesti õigusaktides puudub küberterrorismi mõiste definitsioon. KarS § 237 määratleb terrorikuriteo mõiste ning küberründe ja küberterrorismi mõisted on eraldi välja toodud Eesti küberjulgeoleku strateegias 2008-2013. Antud strateegias on küberterrorismil välja toodud vaid poliitiline aspekt, kuid eesmärgiks võib olla ka elanikkonna hirmutamine või majandusliku ja ühiskondliku korralduse häirimine.

Lähtudes karistusseadustikus, küberjulgeoleku strateegias, hädaolukorra seaduses ning esimeses peatükis välja toodud terrorismi ja küberterrorismi mõistetest mujal maailmas, pakun välja omapoolse nägemuse küberterrorismi definitsioonist, mida võiks kasutada Eesti õigusaktides.

Küberterrorism on interneti või teiste kommunikatsioonivõrgustike vahendusel arvutite või muude kommunikatsiooniseadmetega toime pandud küberrünne, mille eesmärk on:

1) osaliselt või täielikult katkestada elutähtsa teenuse toimepidevus

2) või tekitada reaalne oht elutähtsa teenuse toimepidevuse katkemisele

3) või sundida riiki või rahvusvahelist organisatsiooni midagi tegema või tegemata jätma

4) või tõsiselt häirida riigi poliitilist, põhiseaduslikku, majanduslikku või ühiskondlikku korraldust või see hävitada

5) või tõsiselt hirmutada elanikkonda

Ja/või mille tulemusena juhtub ja/või võib potentsiaalselt juhtuda vähemalt üks järgmistest:

a) ohtu satub paljude inimeste elu või tervis,

b) tekib suur keskkonna- või varaline kahju, sealhulgas kahju elutähtsale ehk kriitilisele infrastruktuurile,

c) tekib oluline mainekahju riigile,

d) tekib ühiskonna majandusaktiivsuse oluline langus ja ühiskonnakorralduse destabiliseerumine

Eelnevate mõistete lahti mõtestamine:

1) **interneti või teiste kommunikatsioonivõrgustike vahendusel -** kommunikatsioonivõrgustike all mõeldakse kohtvõrku (*local area network*)
2) **arvutite või muude kommunikatsiooniseadmetega –** muude kommunikatsiooniseadmete all mõeldakse mobiiltelefone, pihuarvuteid, tahvelarvuteid jm seadmeid
3) **osaliselt või täielikult katkestada elutähtsa teenuse toimepidevus –** elutähsate teenustena on välja loetletud hädaolukorra seaduses energia, pangandus, kommunikatsioonvõrgud, transport jne
4) **tekib oluline kahju elutähtsale ehk kriitilisele infrastruktuurile –** kriitilise infrastruktuuri all mõeldakse vara, süsteemi või nende osa, mis on hädavajalik eluliselt tähtsate ühiskondlike toimingute toimimiseks. Näiteks tervishoiu, turvalisuse, julgeoleku, inimeste majandusliku ja sotsiaalse heaolu toimimiseks. See on infrastruktuur, mille kahjustada saamine või hävimine mõjutaks oluliselt riiki.

Töö autori ettepanekud on järgmised:

1) luua ühtsed rahvusvahelised õigusaktid küberterrorismiga võitlemiseks
2) kuna küberrünnakud ei tunne riigipiire, on vaja arendada riikide vahelist koostööd
3) defineerida Eesti õigusaktides küberterrorismi mõiste

Kokkuvõte

Küberterrorism on üha suureneva ohuga terrorikuritegu maailmas, millele ei ole veel välja töötatud ühtseid õigusakte. Olukorra muudab veel raskemaks asjaolu, et küberründed ei tunne riigipiire. Ühiskond sõltub üha enam IT-lahendustest ning elutähtsad teenused on lihtne sihtmärk küberrünnetele.

Selleks, et riigid saaksid ühtselt küberterrorismi ennetada ning rünnakute korraldajaid vastutusele võtta, peavad riigid tegema tihedat koostööd. USA ning Euroopa Liidu liikmesriigid on selles osas teinud edusamme, kuid õigusaktid on veel nõrgad ja puudulikud ning ei jõua üha kiiremalt areneva IT maailmaga sammu pidada. Koos infotehnoloogiaga areneb üha enam ka pahavara võimekus ning lisaks ka kättesaadavus.

Eesti riik on 2007. aasta sündmuste tõttu maailma parim näide küberterrorismi rünnaku alla sattunud heaoluriigist, kes peab oma õigusakte täiendama selleks, et edaspidi oleks riik rünnakuks paremini valmistunud. Eestis on küberterrorismi mõiste küll välja toodud küberjulgeoleku strateegias, kuid õigusaktides ei ole seda mõistet veel defineeritud. Esmajoones võiks Eesti ametlikult kehtestada küberterrorismi mõiste.

Kuigi ühtegi küberterrorismi juhtumit ei ole ametlikult kinnitatud, on siiski oluline, et riigid paneksid paika ühtsed õigusaktid ning toimiva ennetusstrateegia, et küberterrorism ei muutuks reaalsuseks.

Antud tööd on võimalik kasutada üldise arusaama saamiseks küberterrorismi puudutavatest õigusaktidest ja tehnilistest vahenditest ning väljapakutud mõistet võiks kasutada õigusaktides. Edasistel uuringutel küberterrorismi teemal võiks keskenduda küberterrorismi ennetusele ja mudelseaduse väljatöötamisele.

Summary

Present final thesis is focussed on the discussion of the conception of cyberterrorism, legal acts related to cyberterrorism and tools of information technology. The capacity of the final thesis is 45 pages.

The main purposes of present thesis were:

1) to give an overview of the conception of cyberterrorism
2) to analyse present legal acts concerning cyberterrorism in Estonia and worldwide
3) to bring out different IT applications and programs that perform cyberterrorism and to analyse the extent of the caused damage
4) to offer a concept of cyberterrorism for Estonian legal acts

Analysis showed that the concept of cyberterrorism is not uniformly agreed between countries and there is a lack of integrated international redactions and strategies. Due to that it is necessary to appeal countries to develop a model law. In Estonia the conception of cyberterrorism is brought out in the cybersecurity strategy of 2008-2013 but it contains only the political aspect of the concept and therefore it needs supplement.

The tools used for cyber attacks are constantly advancing and changing more easier to use and to get access to. It's possible to disturb the functioning of critical services with IT malware and therefore seriously disturb government's work and polity.

Present thesis can be used to get a grip of legal acts and technical tools concerning cyberterrorism. The author's offered concept of cyberterrorism could be used in legal acts. For futher studies on cyberterrorism should be concentrated on the prevention of cyberterrorism and compilation of a model law.

Kasutatud kirjandus

4.1.4 Digitaalne sertifikaat. E-õppe portaali kodulehelt www.e-uni.ee/e-kursused/itturvalisus/414_digitaalne_sertifikaat.html välja otsitud 04.04.2012.

Aasmäe, P. 01.05.2010. Küberkuritegevuse tippklass – botnet Zeus. Arvutikaitse kodulehelt www.arvutikaitse.ee/kuberkuritegevuse-tippsklass-zeus-botnet välja otsitud 07.03.2012.

Arvutikuritegevusvastane konventsioon 23.11.2001, jõustunud 01.07.2004. Riigi Teataja kodulehelt www.riigiteataja.ee/akt/550359 välja otsitud 10.02.2012.

Botnet. Arvutikaitse kodulehelt www.arvutikaitse.ee/arvutikaitse-algtoed/botnet/ välja otsitud 03.03.2012.

Cohen, A. Cyberterrorism: are we legally ready? Journal of International Business & Law. Volume 9 Number 1, Spring 2010. Hofstra Law kodulehelt lawarchive.hofstra.edu/pdf/academics/journals/jibl/jibl_vol9no1_cohen_cyberterrorism.pdf välja otsitud 12.03.2012.

Computer Fraud and Abuse Act 18 USC 1030. 1984. U.S. Department of Energy kodulehelt energy.gov/sites/prod/files/cioprod/documents/ComputerFraud-AbuseAct.pdf välja otsitud 20.02.2012.

EU Action Plan on combating terrorism 15893/1/10 REV 1. 17.01.2011. Lk 2, 9-10. Euroopa Nõukogu avalike dokumentide kodulehelt register.consilium.europa.eu/pdf/en/10/st15/st15893-re01.en10.pdf välja otsitud 18.03.2012.

Convention on Cybercrime CETS No.:185. Council of Crime kodulehelt conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=EN välja otsitud 09.04.2012.

Cyberterrorism. TechTarget kodulehelt searchsecurity.techtarget.com/definition/cyberterrorism välja otsitud 08.04.2012.

Cyberterrorism: technical definition. Yourdictionary kodulehelt computer.yourdictionary.com/cyberterrorism välja otsitud 11.03.2012.

Denial of Service (DoS) Attacks. Tech-FAQ kodulehelt www.tech-faq.com/denial-of-service-dos-attacks.html välja otsitud 04.04.2012.

Dick, R. L. 05.04.2001. Issue of Intrusions into Government Computer Networks. FBI kodulehelt www.fbi.gov/news/testimony/issue-of-intrusions-into-government-computer-networks välja otsitud 12.02.2012.

e-Teatmik: IT ja sidetehnika seletav sõnaraamat www.vallaste.ee

Eesti terrorismivastase võitluse põhialused. Vabariigi Valitsus, 17.08.2006, lk 6. Vabariigi Valitsuse kodulehelt valitsus.ee/UserFiles/valitsus/et/valitsus/arengukavad/siseministeerium/Terrorismivastase_voitluse_pohialused.pdf välja otsitud 13.04.2012.

Euroopa Majandus- ja Sotsiaalkomitee arvamus teemal "Kodanikuühiskonna osalus võitluses organiseeritud kuritegevuse ja terrorismiga" (2006/C 318/26). Euroopa Liidu Teataja kodulehelt eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2006:318:0147:0147:ET:PDF välja otsitud 08.02.2012.

Fischer, E. A. 22.12.2011. Federal Laws Relating to Cybersecurity: Discussion of Proposed Revisions. Lk 7. Federation of American Scientists kodulehelt www.fas.org/sgp/crs/natsec/R42114.pdf välja otsitud 15.03.2012.

Goldman, B. 2009. The Democratic Dilemmas of Cyber-terrorism and the Internet. PiCa kodulehelt www.thepicaproject.org/?page_id=279 välja otsitud 23.03.2012.

Holtzman, D. H. 01.02.2003. Cyber Security Enhancement Act of 2002 (CSEA) Changes Rules the Game Forever. CIO kodulehelt www.cio.com/article/217427/Cyber_Security_Enhancement_Act_of_2002_CSEA_Changes_Rules_of_the_Game_Forever välja otsitud 22.02.2012.

Hosenball, M. 14.02.2012. Experts say Iran has "neutralized" Stuxnet virus. Reuters kodulehelt www.reuters.com/article/2012/02/14/us-iran-usa-stuxnet-idUSTRE81D24Q20120214 välja otsitud 23.03.2012.

How do digital certificates work in a web site? Link Intime kodulehelt www.linkintime.co.in/tcs/faqs/gfaqs.htm välja otsitud 05.04.2012.

How a botnet works? Wikipedia kodulehelt en.wikipedia.org/wiki/File:Botnet.svg välja otsitud 02.04.2012.

How the Stuxnet worm works. Internetilehelt 4.bp.blogspot.com/-DNVe-muuHO4/ThwOic4OKvI/AAAAAAAAFLg/W8sw_tB0R2w/s1600/how-the-Stuxnet-worm-works.jpg välja otsitud 03.04.2012.

Hädaolukorra seadus 15.06.2009, jõustunud 01.01.2010 - RT I 2009, 62, 405 ... RT I, 29.12.2011, 1

Hädaolukorra seaduse muutmise seadus 204 SE I. Riigikogu kodulehelt www.riigikogu.ee/index.php?page=en_vaade&op=ems&enr=204SE&koosseis=12 välja otsitud 10.03.2012.

Vabariigi Valitsuse määruse Hädaolukorrast või hädaolukorra tekkimise vahetust ohust Siseministeeriumi teavitamise kord, 06.05.2010 nr 57, jõustunud 20.05.2010.

Is Your Computer a Zombie Bot Being Controlled by Hackers? Raymond.CC kodulehelt www.raymond.cc/blog/is-your-computer-a-zombie-bot-being-controlled-by-hackers/ välja otsitud 04.03.2012.

Kanti, T., Richariya, Vineet, Richariya, Vivek. Implementing a Web Browser with Web Defacement Detection Techniques. Scribd kodulehelt www.scribd.com/doc/70532118/Implementing-a-Web-Browser-With-Web-Defacement-Detection-Techniques välja otsitud 01.04.2012.

Karistusseadustik 06.06.2001, jõustunud 01.09.2002 - RT I 2001, 61, 364 ... RT I, 04.04.2012, 1

Karistusseadustiku muutmise seaduse eelnõu, 166 SE II-1. Riigikogu kodulehelt www.riigikogu.ee/?page=pub_file&op=emsplain&content_type=application%2Fmsword&u=20120411155901&file_id=198499&file_name=KarS+seletuskiri+%28167%29.doc&file_size=66048&mnsensk=166+SE&etapp=03.12.2007&fd=13.04.2011 välja otsitud 13.04.2012.

Komisjoni teatis Euroopa Parlamendile, Nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele „Euroopa kaitsmine laiaulatuslike küberrünnakute ja häirete eest: valmisoleku, turvalisuse ja vastupidavuse suurendamine”. Brüssel, 30.3.2009. Euroopa Liidu Teataja kodulehelt eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:ET:PDF välja otsitud 19.03.2012.

Kriitilise informatsiooni infrastruktuuri kaitse. RIA kodulehelt www.ria.ee/kiik/ välja otsitud 09.04.2012.

Kriminaalmenetluse seadus 12.02.2003, jõustunud 01.07.2004 - RT I 2003, 83, 558 ... RT I, 17.04.2012, 4

Küberjulgeoleku strateegia 2008-2013. Kaitseministeerium, 2008. Vabariigi Valitsuse kodulehelt

valitsus.ee/UserFiles/valitsus/et/valitsus/arengukavad/kaitseministeerium/kuberjulgeolek.pdf välja otsitud 12.03.2012.

Lehtla, T. ja Rosin, A. Loogikakontrollerid ja nende programmeerimise alused. Tallinna Tehnikaülikooli kodulehelt www.ene.ttu.ee/leonardo/loogika/LOOGS7.pdf välja otsitud 03.03.2012.

Lemos, R. 15.09.1999. 'United Loan Gunmen' attack again. ZDNet kodulehelt www.zdnet.com/news/united-loan-gunmen-attack-again/103255 välja otsitud 01.04.2012.

Lewis, J. F. Fighting Terrorism in the 21st Century. FBI Law Enforcement Bulletin. Volume 68, Number 3, March 1999, lk 6. FBI kodulehelt www.fbi.gov/stats-services/publications/law-enforcement-bulletin/1999-pdfs/mar99leb.pdf 11.02.2011 välja otsitud 05.03.2012.

Lourdeau, K. 24.02.2004. Virtual Threat, Real Terror: Cyberterrorism in the 21st Century. United States Senate Committee on the Judiciary. Information Warfare Site kodulehelt www.iwar.org.uk/cyberterror/resources/ct-hearing/lourdeau.htm kodulehelt välja otsitud 18.02.2012.

Lõugas, H. 12.09.2011. TÄISMAHUS: Häkkerid kehastuvad Google'iks, et jälgida Iraani internetti, Eesti Päevaleht. Eesti Päevalehe kodulehelt www.epl.ee/news/eesti/taismahus-hakkerid-kehastuvad-googleiks-et-jalgida-iraani-internetti.d?id=57584208 välja otsitud 20.03.2012.

Matrosov, A., Rodionov, E., Harley, D., Malcho, J. Stuxnet Under the Microscope. ESET kodulehelt go.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf välja otsitud 15.03.2012.

National Communications System, Supervisory Control and Data Acquisition (SCADA) Systems. Technical Information Bulletin 04-1, October 2004. National Communication System kodulehelt www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf välja otsitud 18.03.2012.

Rikk, R. Lissaboni mõju küberjulgeolekule. Diplomaatia kodulehelt www.diplomaatia.ee/index.php?id=242&tx_ttnews[tt_news]=1194&tx_ttnews[backPid]=570&cHash=93f55dff15 välja otsitud 13.03.2012.

Schouwenberg, R. 15.09.2011. Why Diginotar may turn out more important than Stuxnet. Securelist kodulehelt www.securelist.com/en/blog/208193111/Why_Diginotar_may_turn_out_more_important_than_Stuxnet välja otsitud 24.03.2012.

Siseministeerium. 2011. aasta hädaolukordade riskianalüüside kokkuvõte. Lk 115. Siseministeeriumi kodulehelt www.siseministeerium.ee/public/HO_RA_2011nov.pdf välja otsitud 13.03.2012.

Stuxnet - a weapon made entirely out of code. Limitless Thoughts kodulehelt limitless-thoughts.blogspot.com/2012/01/stuxnet-weapon-made-entirely-out-of.html#!/2012/01/stuxnet-weapon-made-entirely-out-of.html välja otsitud 22.03.2012.

Tikk, E., Kaska, K., Vihula, L. 2010. International Cyber Incidents: Legal Considerations. Lk 18-21.

Zetter, K. 11.07.2011. How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History. Wired kodulehelt www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1 välja otsitud 12.03.2012.

Ulatuslikust küberrünnakust põhjustatud hädaolukorra lahendamise plaan. 27.07.2011. Majandus- ja kommunikatsiooniministeeriumi kodulehelt www.mkm.ee/hadaolukorra-lahendamise-plaan/ välja otsitud 15.03.2012.