Küberjulgeoleku strateegia 2008–2013

Küberjulgeoleku strateegia komisjon

Kaitseministeerium

Tallinn 2008

SISUKORD:

KOKKUVÕTE

Küberruumi haavatavus on tõsine asümmeetriline julgeolekuoht, mis puudutab kõiki riike ning millega peab võitlema globaalsel tasandil. On hädavajalik, et infotehnoloogiliste lahenduste laialdase kasutamisega kaasneks ka infosüsteemide turvalisuse kõrge tase ja küberjulgeoleku üldine tagamine.

Küberruumi turvalisuse tagamise eelduseks on arusaam, et iga arvuti, arvutivõrgu või infosüsteemi omanik tunnetab oma vastutust tema käsutuses olevate info- ja kommunikatsioonitehnoloogiliste vahendite otstarbeka ja heaperemeheliku kasutuse eest.

Küberjulgeolek Eestis tugineb eeskätt riigi kui terviku küberruumi haavatavuse vähendamisele. Ühelt poolt eeldab see vastavate riigisiseste tegevuskavade elluviimist, teisalt aga ka aktiivset rahvusvahelist koostööd, et toetada ka teiste riikide küberruumi turvataseme tõstmist**.**

Küberjulgeoleku tagamise strateegilised eesmärgid on järgmised:

- Eestis on laiaulatuslikult rakendatud astmeline turvameetmete süsteem, mis tagab Eesti riigi küberjulgeoleku;
- Eesti on väga suure infoturbealase kompetentsuse ja teadlikkusega riik;
- infosüsteemide turvalist ja laialdast kasutamist toetab proportsionaalne õiguslik regulatsioon;
- Eesti on küberjulgeoleku tõhustamiseks tehtava rahvusvahelise koostöö üks juhtriike.

Tegevusvaldkonnad küberjulgeoleku tugevdamiseks

1. Turvameetmete süsteemi arendamise ja laiaulatusliku rakendamise aluseks on teadmine, et ühiskonna igapäevane toimimine sõltub infotehnoloogilistest lahendustest. Iga infosüsteemi omanik peab teadvustama ohtusid, mis kaasnevad tema poolt pakutava teenuse katkemise või häirimisega. Sellest tulenevalt peavad olema välja töötatud ja rakendatud ajakohased ja majanduslikult otstarbekad turvameetmed. Olulisemad eesmärgid turvameetmete süsteemi arendamisel ja rakendamisel on:

- suurendada kriitilise infrastruktuuri ja sellele osutatavate teenuste vastupanuvõimet küberruumis olevatele ohtudele. Karmistada kriitilise infrastruktuuri infosüsteemide ja teenuste turvaeesmärke ning määrata kindlaks turvaastmestik;
- tugevdada Interneti füüsilist ja loogilist infrastruktuuri. Interneti turvalisus on küberjulgeoleku tagamisel esmatähtis, sest suurem osa küberruumist põhineb Internetil. Interneti infrastruktuuri tugevdamine, sh Interneti-arvutite nimeserverite (DNS) infrastruktuuri tugevdamine, Interneti-teenuse kasutajate automatiseeritud piiramine olenevalt nende liikluse iseloomust ja autentimisvahendite laialdane kasutamine on esmased prioriteedid;

- suurendada Eesti kriitilise infrastruktuuri juhtimissüsteemide, eelkõige elektri-, gaasi-, vee- jt jaotussüsteemide ning liikluse juhtimissüsteemide turvalisust, määrata kindlaks täiendavad turvameetmed ja rakendada neid;
- täiendada pidevalt küberjulgeolekut tagavaid turvalahendusi ja rakendada vastavaid turvameetmeid tulenevalt tehnoloogiliselt keerukamate ründemeetodite kasutuselevõtust;
- tugevdada ametkondadevahelist koostööd ja koordinatsiooni küberjulgeoleku tagamiseks ning jätkata era- ja avaliku sektori koostööd kriitilise informatsiooni infrastruktuuri kaitsmisel.

2. Küberjulgeoleku alase kompetentsuse tõstmine. Vajaliku kompetentsuse saavutamiseks küberjulgeoleku valdkonnas on püstitatud järgmised eesmärgid väljaõppe ja teadusuuringute osas:

- tagada infoturbealase väljaõppe kvaliteet ja kättesaadavus, et saavutada piisav kompetentsus avalikus ja erasektoris. Kehtestada IT-töötajatele ühtsed infoturbealase kompetentsuse nõuded ning luua vastav täiendusõppe- ja atesteerimissüsteem;
- intensiivistada küberjulgeolekuks vajalikke uuringuid ning arendustööd, et tagada riigi kaitsevõime nimetatud valdkonnas, tõhustada rahvusvahelist teadusalast koostööd ning kindlustada pädevus kõrgtasemel väljaõppe pakkumiseks;
- tagada tegevusvalmidus küberjulgeoleku kriisisituatsioonides nii avalikus kui ka erasektoris;
- arendada Eestis välja rahvusvaheliselt tunnustatud küberjulgeoleku alane kompetentsus, toetudes intensiivsele teadus- ja arendustegevusele.

3. Küberjulgeoleku tagamiseks vajaliku õigusruumi täiendamine. Küberjulgeolekut puudutava siseriikliku ja rahvusvahelise õigusruumi kujundamisel on eesmärgiks:

- täiendada Eesti õigusruumi, lähtudes küberjulgeoleku strateegia eesmärkidest ja rakendusplaanist;
- valmistada ette kriitilise infrastruktuuri küberkaitset tagavad õigusaktid ning nende rakendamine;
- osaleda küberjulgeoleku valdkonnas rahvusvahelise õiguse loomisel ja arendamisel ning algatada Eesti siseriiklikke õiguslahendusi tutvustavaid ja propageerivaid rahvusvahelisi samme.

4. Rahvusvahelise koostöö arendamine. Strateegia seab küberjulgeoleku tagamisega seotud rahvusvahelise koostöö arendamisel järgmised eesmärgid:

- saavutada rahvusvaheline moraalne hukkamõist küberrünnetele, mis häirivad inimeste elu ja ühiskonna toimimist. Samas tuleb jälgida, et võitlus küberohtudega ei saaks inimõiguste ja demokraatlike vabaduste piiramise ettekäändeks;
- taotleda võimalikult laiapinnalist ühinemist küberkuritegevust ja -ründeid käsitlevate rahvusvaheliste konventsioonidega ning nende sisu tutvustamist rahvusvahelisele üldsusele;

- osaleda rahvusvahelise küberjulgeoleku poliitika väljatöötamisel ja jõustamisel, samuti üleilmse küberkultuuri kujundamisel;
- arendada rahvusvahelisi küberjulgeolekuga tegelevaid koostöövõrgustikke ja tõhustada nende toimimist.

5. Teavitustegevuse eesmärgid:

- tutvustada Eesti küberjulgeoleku alaseid seisukohti nii riigisiseselt kui ka rahvusvahelisel tasandil ning toetada koostöövõrgustikke meedia abil;
- tõsta infoturbeteadlikkust ja -taset kõigi arvutikasutajate, eelkõige üksikkasutajate ja väikeettevõtete hulgas. Teavitustöö eesmärgiks on tutvustada küberkeskkonna ohte ning parandada arvutikasutajate teadlikkust turvalisest arvutikasutusest ja infoturbe põhitõdedest;
- korraldada teavitustööd koordineeritult koostöös erasektoriga.

1 Sissejuhatus

Viimastel aastatel sagenenud küberrünnakud arenenud infoühiskondade avaliku ja erasektori infosüsteemide toimimise häirimiseks on tõstnud küberruumi kuritarvitamise arvestatavate uute julgeolekuohtude hulka. Küberohtude teadvustamine jõudis 2007. aastal rahvusvahelise julgeoleku seisukohalt uuele tasandile mitte ainult esimese koordineeritud küberrünnaku toimepanemise tõttu Eesti kui riigi vastu, vaid ka paljude teiste riikide era- ja avaliku sektori oluliste infosüsteemide vastu suunatud ulatuslike küberrünnakute tõttu. Sagenenud küberrünnakud annavad tunnistust uue ajajärgu saabumisest, kus küberruum on saavutamas globaalset julgeolekumõõdet ning kriitilise tähendusega infosüsteemide kaitset käsitletakse sama olulisena kui riikide traditsioonilist kaitsevõimet ja julgeoleku tagamist.

Koordineeritud küberrünnakud Eesti valitsusasutuste, pankade, meedia- ja telekommunikatsioonifirmade vastu tõendasid, et ühiskonna infosüsteemide haavatavus on üks riikliku julgeoleku aspekte, millele on tarvis pöörata senisest rohkem tähelepanu. Kuigi oleme Eestis selgelt ja üheselt teadvustanud infosüsteemide kaitse vajadust arenevas infoühiskonnas, pole selleks võetud meetmed olnud alati piisavad. Terve riigi küberjulgeoleku tagamine nõuab kogu ühiskonna kaasamist ning selget riigisisest tööjaotust küberrünnakute ennetamisel, samuti infoturbealase kompetentsuse suurendamist ja ühiskonna teadlikkuse üldist tõstmist küberruumis varitsevatest ohtudest.

Peame teadvustama, et infosüsteemide kasutusega kaasnevate riskide ja infotehnoloogia laialdase kasutamise tasakaalustamine on väljakutse mitte ainult Eestis, vaid kogu maailmas. Küberjulgeoleku probleemide kasv ei tohiks takistada info- ja kommunikatsioonitehnoloogial toimimast ka edaspidi ühiskondade kasvumootorina. Kuna riikide küberruume on raske piiritleda ning küberohud on oma olemuselt globaalsed ja asümmeetrilised, on väga oluline rõhutada iga kodaniku, infosüsteemi omaniku ja riigi vastutust ning taotleda küberrünnakute moraalset hukkamõistu rahvusvahelisel tasandil.

1.1 Küberjulgeoleku tagamise põhimõtted

Riigi küberjulgeolek[1] on laia tähendusväljaga mõiste, mis hõlmab kõiki elektroonilise teabe, teabekandjate ning teenustega seotud toiminguid, mis mõjutavad riigi julgeolekut. Riigi küberruumi julgeoleku tagamine koosneb mitmesugustest tegevustest eri tasanditel. Olulisemad neist on küberruumi haavatavuse vähendamine, küberrünnakute ennetamine ning infosüsteemide toimimise võimalikult kiire taastamine rünnakute korral. Küberjulgeoleku tagamiseks on vaja hinnata riigi kriitilise infrastruktuuri haavatavust, kavandada ennetavate meetmete süsteem küberrünnakute ärahoidmiseks ja määrata kindlaks riigisisene tööjaotus küberjulgeoleku

[1] Strateegias kasutatavad mõisted ja erialased terminid on ära toodud dokumendi lõpus. Vt. Lisa 2.

korralduses. Tähtis on ka täiendada küberjulgeoleku tagamiseks vajalikku õigusruumi, arendada rahvusvahelist ja institutsionaalset koostööd, teavitada avalikkust ning töötada välja küberjulgeoleku alased koolitus- ja teadusprogrammid.

Küberjulgeoleku haavatavuse vähendamiseks tuleb senisest rohkem tähelepanu pöörata infosüsteemide turvalisuse suurendamisele, andmeturbestandardite kehtestamisele ning arvutikasutajate koolitusele. Oluline on koordineeritud tegutsemine riigi tasandil ja eri institutsioonide vaheline konkreetne tööjaotus küberjulgeoleku tagamisel.

Küberjulgeoleku tagamisel arvestatakse järgmiste põhimõtetega:

- küberjulgeoleku tagamiseks vajalikud tegevuskavad lülitatakse olemasolevasse riikliku julgeoleku tagamise protsessi;
- küberjulgeoleku arendamine toimub avaliku, era- ja kolmanda sektori koordineeritud tegevuse kaudu ja kõikide osapoolte koostöös;
- kriitilise informatsiooni infrastruktuuri kaitse tagamiseks on vajalik era- ja avaliku sektori tõhus koostöö;
- küberjulgeoleku tagamise aluseks on hea infoturve, kus iga infosüsteemi omanik on teadlik oma vastutusest infosüsteemi heaperemehelikul kasutamisel ja rakendab teadvustatud riskidele vastavaid turvameetmeid;
- küberjulgeoleku tagamise oluline eeldus on ühiskonna teadlikkus küberruumis levivatest ohtudest ja infoturbealane kompetentsus. Infoühiskonnas vastutab iga osaline tema valduses oleva võrguühendusega tehnilise seadme või süsteemi turvalisuse eest;
- Eesti teeb ulatuslikku koostööd rahvusvaheliste organisatsioonide ja teiste riikidega küberjulgeoleku üleilmseks tugevdamiseks;
- küberjulgeoleku tagamisel peab olema kindlustatud inimeste põhiõiguste kaitse, isikuandmete ja identiteedi kaitse;
- avalike teenuste pakkumiseks kasutatavate infotehnoloogiliste lahenduste arendamisel ja haldamisel tuleb järgida „Riigi IT-arhitektuuri ja koosvõime raamistikku", sh infoturberaamistikku. Arvestama peab ka asutuse infoturbepoliitikat ning soovitusi asutuse infosüsteemi talitluspidevus- ja taasteplaanide kohta.

1.2 Küberjulgeoleku strateegia ja selle seos teiste riiklike arengukavadega

Eesti küberruumi haavatavuse vähendamiseks ja infosüsteemide senisest tõhusamaks kaitseks kogu riigis andis Vabariigi Valitsus Kaitseministeeriumile korralduse koostada valdkondlik arengukava "Küberjulgeoleku strateegia 2008–2013" koostöös Haridus- ja Teadusministeeriumi, Justiitsministeeriumi, Majandus- ja

Kommunikatsiooniministeeriumi, Siseministeeriumi ja Välisministeeriumiga[2]. Ametkondadevaheline komisjon strateegia koostamiseks kaasas ka Eesti ettevõtete infoturbeeksperte.

Küberjulgeoleku strateegia koostamisel on infoturbe ja infoühiskonna arendamise ning riigi sisejulgeoleku ja kaitsevõime tagamise osas arvestatud ka teiste riiklike arengukavadega. Käesoleva strateegia põhimõtted on kooskõlas Majandus- ja Kommunikatsiooniministeeriumi poolt 31. jaanuaril 2007 vastu võetud „Infoturbe koosvõime raamistikuga", kus on kindlaks määratud Eesti infoturbe toimimise põhimõtted, infoturbe koordineerimise kord ja regulatsioonid, infoturbealase koolituse põhimõtted, samuti informatsiooni infrastruktuuri kaitsega seotud tegevused. Eelmainitud dokument oli esimene samm riigiasutuste ja erasektori ühtsete standardite kehtestamiseks riigisisese infoturbe tagamisel ning kriitilise infrastruktuuri infosüsteemide kaitsmisel.

Küberjulgeoleku strateegiaga on seotud ka Majandus- ja Kommunikatsiooniministeeriumi poolt 2007. aastal koostatud „Infoühiskonna arengukava 2013", mis rõhutab inimeste kaasamist infoühiskonda ning Eesti infotehnoloogilise konkurentsivõime arendamist. Samuti on koostatava strateegiaga seotud Haridus- ja Teadusministeeriumi poolt 2007. aastal välja töötatud dokument „Teadmistepõhine Eesti. Eesti teadus- ja arendustegevuse ning innovatsiooni strateegia 2007–2013", mille teadus- ja arendustegevuse põhisuundades on tähtsal kohal riigi infotehnoloogiline kompetentsus ning erinevate valdkondade e-lahendused. Kuna võitlust küberkuritegevusega käsitleb Justiitsministeeriumi poolt ette valmistatud dokument „Kriminaalpoliitika põhisuunad" ja Siseministeeriumi poolt ette valmistatud eelnõu „Eesti turvalisuspoliitika põhisuunad aastani 2015", ei käsitleta käesolevas strateegias eraldi küberkuritegevuse vastaseid riiklikke meetmeid. Riigi kaitseotstarbeliste infosüsteemide turvameetmeid käsitletakse detailsemalt Kaitseministeeriumi poolt koostatavas dokumendis "Sõjalise riigikaitse arengukava 2009–2018", mis valmib 2008. aasta III kvartalis.

[2] Vabariigi Valitsuse korraldus nr. 497 "Küberjulgeoleku strateegia 2008-2013 koostamine" jõustus 19.11.2007.a. Koostamise aluseks on Vabariigi Valitsuse määrus 13. detsembrist 2005.a. nr. 302 "Strateegiliste arengukavade liigid ning nende koostamise, täiendamise, elluviimise, hindamise ja aruandluse kord".

2 Ohud küberruumis

Küberruumi haavatavus on muutunud üheks olulisemaks asümmeetriliseks julgeolekuohuks, millega peavad arvestama kõik aktiivselt infosüsteeme kasutavad ühiskonnad. Küberrünnakute ohtlikkus ühiskonna jaoks seisneb ründaja võimaluses tekitada suure vahemaa tagant ning väheste vahenditega märkimisväärset kahju, alates normaalse elutegevuse lühiajalistest katkestustest kuni suure majandusliku kahju ja inimohvritega lõppevate katastroofideni. Kuigi seni pole küberrünnakud veel inimohvreid nõudnud, ei saa välistada, et see juhtub tulevikus korraldatavate rünnakute puhul riigi kriitilisele informatsiooni infrastruktuurile. Küberruumi kuritarvitamine terroristlike rühmituste ja organiseeritud kuritegevuse poolt on juba praegu tõsiseks julgeolekuohuks maailmas.

Ohud küberruumis on raskesti defineeritavad ründeallika määramise keerukuse, selgete motiivide teadmatuse ja küberruumis toimuvate rünnakute ettearvamatu käigu tõttu. Küberohtude tuvastamise teeb keeruliseks ka asjaolu, et küberruumis on raske eristada riikliku, riigivälise, era- ja avaliku sektori piire ning tegutsejaid. Ohud küberruumis on oma olemuselt globaalsed ja nendega võitlemine muutub järjest keerukamaks ülesandeks, nõudes kõrgetasemelist väljaõpet, arenenud õigusruumi, efektiivset organisatsioonilist koostööd ja ka arvestatavaid ressursse.

Ohte küberruumis liigitatakse mitmel viisil. Väga levinud on küberrünnete jaotus ründe motiivide alusel, mille puhul eristatakse ohtusid kolmes kategoorias: küberkuritegevus, küberterrorism ning sõjategevus küberruumis. Tehnoloogia ja ründeviiside arenedes on üha keerulisem ründemotiive selgelt määratleda ning mõnikord järjestatakse ohtusid ka ründe tüübi ja tekitatud kahju mõjuulatuse alusel. Arvutivõrkude suure sidususe ja informatsiooni infrastruktuurist sõltuvate teenuste vastastikuse sõltuvuse tõttu võib rünnakute tekitatud kahju ulatus olla ettearvamatu. Näiteks võib rünnak ühe teenusepakkuja serverile põhjustada teiste, selle teenustest sõltuvate kriitilise infrastruktuuri ettevõtete infosüsteemide toimimise katkemise. Tuleb rõhutada, et ühiskonnale on ohtlik mis tahes motiividel toime pandud küberruumi kuritarvitamine, alustades rumalusest või huligaansusest korda saadetud häkkimisest ja lõpetades organiseeritud rünnakutega riigi kriitilise infrastruktuuri infosüsteemide vastu.

Kriitilise infrastruktuuri vastu suunatud küberrünnakud. 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.

Näiteks võib edukas küberrünnak avalikule telekommunikatsioonivõrgule jätta kliendid ilma telefoniteenusest. Küberrünnak keemia- või loodusliku gaasi rajatise juhtimissüsteemidele võib viia inimkaotuste ning märkimisväärsete füüsiliste kahjustusteni. Samuti võib tekkida tõsiste tagajärgedega infrastruktuuririke siis, kui infrastruktuuri ühe osa rike toob kaasa teiste osade rikked, põhjustades lumepalliefekti, mille tagajärjel toimunud sündmused võivad olla väga kahjustavad ja tuua kaasa rajatiste või tähtsate teenuste ulatusliku seiskumise. Eriti ulatuslikud infosüsteemide rikked võivad tekitada suurt rahalist kahju või kaasa tuua isegi inimohvreid. Üheks eriti tõsiseks ohuks on küberrünnaku kasutamine koos füüsilise rünnakuga või küberrünnakute sooritamine suurte loodusõnnetuste ajal.

Küberkuritegevus. Kõige suurema osa rünnetest nii infosüsteemide kui ka infosüsteemis paiknevate andmete vastu moodustavad varalise kasu saamise eesmärgil toime pandud kuriteod. Need kuriteod võivad avalduda teenuse pakkumise häirimises või teenuse töö katkestamises, andmete konfidentsiaalsuse, tervikluse ja käideldavuse rikkumises. Küberruumis võib aset leida ka inimeste mõjutamine ja ahistamine, kelmus, ebaseadusliku materjali levitamine ja intellektuaalse omandi rikkumine. Võrreldes teiste kuriteoliikidega on küberkuritegevust soodustavaks asjaoluks selle toimepanemise ning varalise kasu saamise lihtsus. Küberkuritegevust soodustavad ka võimalus jääda anonüümseks, rahvusvaheliselt vähe reguleeritud küberruumi kasutus ning nii infosüsteemide valdajate kui ka lõppkasutajate vähene hoolsus turvalisuse tagamisel.

Küberkuritegevusega võitlemise teeb keeruliseks arvutikuritegevuse liikide, kahjuulatuse, motiivide ning tagajärgede suur erinevus. Kuritegusid saadetakse korda majandusliku kasu saamise eesmärgil, uudishimust ja huligaansusest. Viimaste aastate jooksul on küberkuritegevus jõudnud etappi, mida iseloomustavad suured ressursid, organiseeritus ja kuritegelike võrgustike selge omavaheline tööjaotus. Interneti abil toime pandud rünnakud on muutunud süstemaatilisemaks ja võivad sageli olla kavandatud konkreetsete sihtmärkide ründamiseks. Spetsiaalselt küberkuritegevuseks mõeldud pahavara väljatöötamise ning rünnakute korraldamisega tegelevate organiseeritud kuritegevuslike gruppide tegevus on muutumas üha laialdasemaks.

3 Küberjulgeolekut toetavate valdkondade kirjeldus ja analüüs

3.1 Eesti infoühiskond ja informatsiooni infrastruktuur

Tänapäeva maailmas on majanduslikku edu ning kõrget elukvaliteeti suutnud tagada vaid need riigid, kus tähtsustatakse teadmiste ja informatsiooni efektiivset käsitlemist ning rakendatakse seda ühiskonna hüvanguks.[3] Infoühiskonna all mõistetakse ühiskonna elukorraldust, kus enamik inimkonna loodud väärtusi on kätketud teabesse, mida talletatakse, hoitakse, teisendatakse ja edastatakse universaalsel digitaalsel kujul. Kasutades üleüldist andmeedastusvõrku, on kõigile ühiskonna liikmetele tagatud juurdepääs teabele.[4]

Eesti infoühiskonna areng on koos meie üleminekuperioodi reformidega olnud majandusarengu oluliseks kasvumootoriks ning loonud eluviisi, mida me tahame jätkata, hoida ja vajadusel ka kaitsta. Oleme igal elualal harjunud kasutama e-teenuseid ning elanikkonna usaldus infosüsteemide kasutuse vastu on Eestis erakordselt suur. 2007. aastal tehti 98% kõigist pangatoimingutest elektrooniliste kanalite vahendusel ja 82% maksudeklaratsioonidest edastati Internetis, peaaegu igas Eesti koolis on võimalik õppida e-õpikeskkonnas, ID-kaardi ning elektrooniliste allkirjade kasutus on rutiinsed toimingud nii avaliku kui ka erasektori asjaajamises ning Eesti on maailmas tuntuks saanud e-valitsemise ja e-valimiste edendajana.

2007. aastal oli 51% Eesti leibkondadest varustatud kiiret Interneti-ühendust võimaldava lairiba püsiühendusega. Kuna igas leibkonnas on mitu arvutikasutajat, on reaalne kodukasutajate suhtarv ligikaudu 70% kogu elanikkonnast.[5] Sellele on suuresti kaasa aidanud Eestis 1990. aastatel alustatud „Tiigrihüppe" ja „Külatee" algatused, mille tulemusena arendati välja laiaulatuslik avalike Interneti-teenuste võrk, mis võimaldas kaasata kõiki ühiskonna liikmeid sõltumata nende geograafilisest asukohast. See on võimaldanud kõigil kodanikel kaasuda ühiskonna arengusse, kasutada riigi poolt pakutavaid teenuseid ja arendada igas paikkonnas oma huvi- või tegevusalasid.

Teenuste mahu suurenemine Interneti-keskkonnas on märgatavalt tõstnud meie igapäevaste toimingute ja eluviisi sõltuvust infotehnoloogiliste lahenduste turvalisusest. Internet on tähtis osa Eesti kriitilisest informatsiooni infrastruktuurist, mida kasutab enamik Eesti ettevõtteid ja riigiasutusi, samuti kuulub praegu enam kui pool Eesti elanikkonnast Interneti-kasutajate hulka. Interneti-teenuse pakkujad (ISPd), riigi ja ISP nimeserverid, Eesti juurdomeeni nimeserverid, asutuste võrgusõlmed, teenuseserverid ja tulemüürid on Eesti kriitilise informatsiooni

[3] "Infoühiskonna arengukava 2013"

[4] Valdo Praust „Infoühiskond ja selle teetähised. Infotehnoloogia haldusjuhtimises" MKM Aastaraamat 1998.

[5] Uuring „Avalike e-teenuste kasutamine", TNS Emor, oktoober 2007.

infrastruktuuri olulised komponendid, moodustades Eesti IT-infrastruktuuri, mida nii ettevõtted kui ka asutused kasutavad e-teenuste osutamiseks. Selle infrastruktuuri töökindlus on esmatähtis Eesti majanduse igapäevase toimimise seisukohalt.

Eesti riigi infosüsteemi arhitektuuri põhikomponent on avalikul Internetil põhinev turvaline andmevahetuskiht X-tee. X-tee kasutab küll Internetti, kuid tagatud on kõik kolm infosüsteemi turvaeesmärki – käideldavus, konfidentsiaalsus ja terviklus. X-tee kesksete komponentide hulk on minimeeritud ja kahe X-teed kasutava infosüsteemi vahelise andmevahetuse toimimine on tagatud ka kesksete komponentide töökatkestuste puhul. X-tee infrastruktuur sisaldab vastuvahendeid nii ajutistele katkestustele kui ka teenusetõkestamisrünnetele. Samas on oluline jätkata X-tee turvameetmete arendamist tulenevalt uutest ründeviisidest ja ohtudest küberruumis.

Ühiskonna toimimise seisukohalt on esmatähtis sellise informatsiooni infrastruktuuri töökindlus, mis toetab igapäevase elu toimimiseks vajalikku kriitilist infrastruktuuri. Kõik kriitilise tähtsusega sektorid – vee- ja toidumajandus, tervishoid, transport, energiasüsteemid, telekommunikatsioon ning finantsteenused[6] – sõltuvad informatsiooni infrastruktuuri toimimisest. Paljude kriitiliste majandussektorite infosüsteemid ja teenused ei toetu siiski ainult Internetile ning nende haavatavuse tõenäosus võrgust tulenevate ohtude tõttu on väiksem. Näiteks on Eesti telekommunikatsiooni infrastruktuuri puhul suuremate telefoni- ja mobiilisidet pakkuvate firmade kõnesidevõrgud Internetist lahutatud. Ka on enamik kriitilise infrastruktuuri automatiseeritud SCADA-juhtimissüsteeme Internetist sõltumatud. Kuigi SCADA-süsteemid ning telekommunikatsioonisektori kõnesidevõrgud pole seotud avaliku Internetiga, võivad hooletuse või tahtliku tegevuse korral küberohud ka neid võrke ähvardada. Näiteks elektri tootmise ja müügiga tegelevates ettevõtetes on elektrijaamade juhtimisega seotud infosüsteemid ja sidevõrgud Internetist küll täielikult eraldatud ning jaamad ja jaotusvõrk vajadusel käsitsi juhitavad, kuid hooletus ja turvaaugud võivad ka need infosüsteemid haavatavaks muuta.

Eesti majanduse toimimise seisukohalt on üks tähtsamaid e-teenustest sõltuvaid sektoreid finantssektor. Kuna praktiliselt kõik pangatehingud Eestis sooritatakse elektrooniliste kanalite kaudu ja 62% Eesti elanikest kasutab Interneti-panku, on küberrünnetel vaieldamatult tõsised tagajärjed, kui pankade e-teenused tarbijale kas täielikult või peaaegu kättesaamatuks muutuvad. Kui finantsteenused katkevad pikemaks ajaks, võib see tekitada suurt kahju Eesti majandusele, vähendada ühiskonna turvalisust ja märkimisväärselt häirida igapäevast elutegevust.

[6] Eesti kriitilise infrastruktuuri valdkonnad on eraldi välja toodud dokumendi lõpus. Vt. Lisa 1.

3.2 Infosüsteemide turvalisus

2007. aastast kehtiv Eesti „Infoturbe koosvõime raamistik"[7] kirjeldab infoturbe tähtsamaid aspekte, mida tuleb arvestada koosvõimelise infosüsteemi loomisel nii kogu riigi kui ka asutuse tasandil. Koosvõimeraamistik on soovituslik nii avalikule kui ka erasektorile. Alates 2008. aastast kehtivad Eesti riigiasutustele kohustuslikud infoturbestandardid, mis kehtestavad riigi ja kohaliku omavalitsuse andmekogudes sisalduvate andmete töötlemiseks kasutatavate infosüsteemide ja nendega seotud infovarade turvameetmed.

Eesti suuremate ettevõtete, kriitiliste Interneti-teenuse pakkujate, telekommunikatsioonifirmade ja pankade infoturbealane kompetentsus on praegu kõrge. Suurtes finantssektori ja telekommunikatsiooniettevõtetes on eeskujulik infoturbekorraldus ning lisaks tulemüüridele ja viirusevastasele tarkvarale on kasutusel ka muud lahendused küberrünnete tuvastamiseks ning tõrjumiseks.

Lähtudes 2007. aasta küberrünnakute iseloomust rünnete viisi, mastaabi ja dünaamika järgi, võib järeldada, et Eestis rünnatud olulised info- ja kommunikatsioonisüsteemid osutusid oma tehnilise ja infoturbetaseme teatavale ebaühtlusele vaatamata kaitstavateks. Selle eelduseks oli eelkõige infoturbespetsialistide tõhus ja hea koostöö horisontaaltasandil sõltumata sellest, kas tegemist oli avaliku või erasektori teenistuses olevate spetsialistidega. Samas oli siiski arvestataval hulgal süsteeme, mille töö oli rünnakute ajal häiritud. Seetõttu peaksid meie info- ja kommunikatsioonisüsteemid olema ka mastaapsemate rünnete korral piisavalt kaitstud ning selleks tuleb parandada nii infotehnoloogilist kui ka organisatoorset valmisolekut küberohtudega võitlemisel.

Esmalt tuleb karmistada Eesti kriitilise infrastruktuuri ettevõtete, kuid ka teiste infosüsteemide turvalisusnõudeid ning kehtestada selged standardid. 2008. aasta jaanuarist kehtima hakanud infosüsteemide kolmeastmeline etalonturbesüsteem (ISKE) on kohustuslik ainult riigiasutustele. Lisaks tuleks tugevdada ka erasektori üldist infoturbealast ettevalmistust, et tagada infosüsteemide turvalisuse üldine kõrge tase.

Teiseks tuleb tugevdada IT-infrastruktuuri käideldavust, sealhulgas suurendada nii avaliku kui erasektori asutuste teenuseserverite koormustaluvust ning testida teenuste käideldavuse taset. Küberrünnete avastamise ning haldamise osas tuleks tugevdada võrguliikluse monitooringu ning intsidentide strateegilise ja taktikalise analüüsi suutlikkust.

Kolmas oluline aspekt on ametkondadevahelise tööjaotuse ning vastutusalade täpsustamine, et korraldada kriitilise infrastruktuuri küberkaitset ja parandada riigisisest koordinatsiooni küberohtude vastu võitlemisel. Välja tuleb töötada ettepanekud õigusruumi täiendamiseks ja regulatsiooni suurendamiseks riigi küberjulgeoleku tagamisel. Samuti on vaja teadvustada küberohte märksa ulatuslikumalt kui seni, kehtestada efektiivne

[7] "Infoturbe koosvõime raamistik" , Majandus- ja Kommunikatsiooniministeerium, 31.01.2007
http://www.riso.ee/et/files/InfoturbeRaamistik.pdf

infovahetusüsteem ning riigisisene tööjaotus küberrünnakute ennetamisel ja tõrjumisel. Kuna suur osa kriitilisest infrastruktuurist kuulub erasektorile, on era- ja avaliku sektori koostöö kriitilise infrastruktuuri haavatavuse vähendamisel keskse tähtsusega.

Oluline aspekt infoturbe arengus on turvameetmete süsteemi pidev täiustamine. Küberjulgeoleku tagamisel ei ole enam piisavad infoturbe seni üldlevinud turvaeesmärgid – info konfidentsiaalsus, käideldavus ja terviklus. Kriitilise infrastruktuuri küberjulgeoleku tagamisel tuleks tähtsate iseseisvate turvaeesmärkidena täiendavalt käsitleda ka näiteks kriitilise infrastruktuuri mittetoimimise tagajärgede kaalukust, salgamise vääramist ja infoallika autentsust. Küberjulgeoleku tagamisel on vajalik vaadelda ka infoturbes seni vähe käsitletud valdkondi, näiteks info- ja sidesüsteemide elektrooniliste rünnete vastaseid füüsilisi kaitsemeetmeid.

Kuigi Eestis on tipptaseme infoturbealane kompetentsus suur, pole ei küberohud ega infoturve pälvinud ühiskonnas tervikuna kaugeltki sellist tähelepanu, mis vastaks Interneti tähtsusele Eesti ettevõtete, riigiasutuste ja elanike jaoks. Lisaks kriitiliste majandussektorite informatsiooni infrastruktuuri olukorrale on väga oluline osa küberjulgeoleku tagamisest ühiskonnas seotud keskmise suurusega ja väikeettevõtete, väiksemate riigi- ja omavalitsusasutuste, õppeasutuste, kodukasutajate ja kõigi teiste võrguarvutite omanike teadlikkusega infoturbest. Interneti-kasutajate turvateadlikkus on kogu maailmas ja sealhulgas ka Eestis erakordselt madal. Rahvusvahelised uuringud on näidanud, et 97% Interneti-kasutajatest ei suuda eristada turvalisi veebilehekülgi ebaturvalistest, mis tähendab, et nende arvutid võivad iga hetk pahavaraga nakatuda. 80%-l uuritud arvutitest leiti infoturbe seisukohalt ohtlikke programme.[8] Eesti arvutikasutajate madalat turvateadlikkust kinnitab SA Vaata Maailma korraldatud uuring, mille tulemusel selgus, et viirusevastane tarkvara töötab küll 82%-l arvutitest, kuid 59% kasutajatest ei tea, kas ja kui sageli seda uuendatakse. 50% Interneti kasutajatest on installeerinud oma arvutisse infoturbe seisukohalt ohtliku programmi ja hinnanguliselt igas kolmandas arvutis võib olla mõni pahatahtlik programm. Seejuures hindab 70,1% vastanutest end asjatundlikuks arvutikasutajaks ning väga suur osa vastanutest leiab, et nende arvuti ei ole küberkurjategijate jaoks ihaldusväärne sihtmärk.[9] Kahjuks võivad uuringus selgunud numbrid tähendada vastupidist olukorda ning paljud koduarvutid võivad olla nakatatud pahavara või nuhkvaraga.

Tehniliste vastumeetmete kõrval tuleb suurimat tähelepanu pöörata arvutikasutajate teadlikkuse parandamisele. Nagu mujal maailmas, on ka Eestis küberjulgeoleku tagamise tähtis eeldus avalikkuse teadlikkuse tõstmine küberruumis valitsevatest ohtudest ning sellest, kuidas nende ohtudega toime tulla. Paralleelselt teadmistega on vaja ka oskusi nende riskide ennetamiseks ja infoturbeintsidentidega toimetulekuks. Selle tööga on Eestis juba

[8] „Adware and Spyware: Unraveling the Financial Web". McAfee White Paper, August 2006.

[9] „Eesti arvutikasutajate turbealased hoiakud", Sihtasutus Vaata Maailma uuring. 2005.

alustatud: 2007. aastal algatati era- ja avaliku sektori koostöös projekt „Arvutikaitse 2009", mis taotleb Eesti kujunemist väga turvalise infoühiskonnaga riigiks.[10]

3.3 Infoturbealane väljaõpe ja täienduskoolitus

Eestis on olemas arvestatav infosüsteemide turvamise kompetentsus, mis võimaldab seista vastu tõsistele küberrünnetele. Siiski on ilmne, et nii era- kui ka avalikus sektoris kasvab vajadus kvalifitseeritud infoturbespetsialistide järele, sest praegu on kompetentsus valdavalt väheste selle alaga tegelevate inimeste käes. Infoturbealast süvendatud väljaõpet ei pakkunud 2007. aasta lõpu seisuga Eestis ühegi avalik-õigusliku ega eraülikooli õppekava ei bakalaureuse-, magistri- ega doktoriõppe tasandil. Infoturbe korraldamise oskusi pole seni õpetatud ka kutsehariduse raames. Infoturbe praktiline kompetentsus on kogunenud erasektorisse, eeskätt pankadesse. Eesti kriitilise infrastruktuuri institutsioonide küsitlus 2007. aastal näitas, et suurimaks puuduseks infoturbe vallas peetakse kvalifitseeritud tööjõu nappust.

Infoturbealane väljaõpe ja täienduskoolitus Eestis on kujunenud spontaanselt ja enamasti ilma riikliku toetuseta. Tartu Ülikooli ja Tallinna Tehnikaülikooli õppekavas on krüptograafia kursusi, samuti mõned üldisemad andmeturbekursused, kuid need ei kata infoturbevaldkonda kogu selle ulatuses. Infoturbe õpetamine ja praktika IKT-erialadel on ebapiisav ning ülikoolides napib kogemustega õppejõude laialdasema õpetuse alustamiseks. IKT-õppekavades puudub infoturbealane spetsialiseerumine. Praktilisi kursusi pakuvad vähesel määral erafirmad, sageli tuleb ajakohast koolitust nõutada välismaalt.

Teaduslik kompetentsus on heatasemelise kõrghariduse pakkumise eelduseks. Infoturbealased teadusuuringud Eestis piirduvad peaasjalikult krüptograafiavaldkonnaga, kus Eesti teadlased on saavutanud maailmatasemel tulemusi ning loonud innovaatilisi rakendusi, nagu turvaline avalike teenuste pakkumine kodanikele X-tee toel, hästitoimiv ajatemplite süsteem ja digitaalallkirjade kasutamine. Selle ala arendustööd ja teenuseid pakuvad mõningal määral ka IT-firmad. Seega on Eesti lähtepositsioon hea: vastavad uurimisrühmad on Tallinna Tehnikaülikooli Küberneetika Instituudis ja Tartu Ülikoolis olemas, kuigi uuringute ja arendustöö edendamiseks tuleks nende rahastamist tunduvalt suurendada.

Küberjulgeoleku puhul ei saa kaitsetegevust eraldada arendustegevusest ja teadustegevusest. Teadusuuringud on olulised eelkõige seetõttu, et infosüsteemide kaitsemeetmete rakendamine on kiirelt arenev kõrgtehnoloogiline valdkond. Kaitse pahavara vastu saab olla edukas ainult pahavara uute versioonide kiire avastamise ja neutraliseerimise korral. Eelisjärjekorras tuleb arendada uuringuid intelligentse kaitsetarkvara alal ning küberrünnete ja -kaitse matkimist nii küberohutuse tagamise kui ka väljaõppe otstarbel. Seda suunda toetab kaitseväe side- ja infotehnoloogia väljaõppe- ja arenduskeskuse (KV SIVAK) juures tegevust alustanud NATO

[10] Arvutikaitse 2009 kodulehekülg: http://www.arvutikaitse.ee/

Küberkaitse Kompetentsikeskus. Kompetentsikeskuse kaudu on Eestil vahetu side NATO küberkaitsestruktuuridega, sealhulgas ka vastavate teadus- ja arendusasutustega. 2008. aastal algab Eesti ülikoolides ka TTÜ ja Kaitseväe Ühendatud Õppeasutuste, KV SIVAKi ning loodava NATO kompetentsikeskuse ühiste jõududega toimuv küberkaitsealane koolitus magistriõppe tasemel.

3.4 Õigusruum küberjulgeoleku tagamisel

3.4.1 Rahvusvaheline õigus

Küberruumi kasutus on maailmapraktikas nii riikidesiseste kui ka rahvusvaheliste õigusaktidega vähe reguleeritud. Rahvusvahelist õigust kui riikide ühise tahte väljendust ja sellisena riigisisese õiguse kujunemise lähtekohta ei ole otseselt küberjulgeolekut puudutavates küsimustes seni veel loodud. Kuna tegemist on kiiresti areneva valdkonnaga, ei ole jõutud seni lahti mõtestada ka kõiki võimalikke küberohte. Pidevalt arenevad nii ohud küberruumis kui ka nende tõrjumiseks kasutatavad meetmed.

Rahvusvahelise õiguse instrumente eksisteerib küll üldküsimuste, näiteks terrorismivastase võitluse ja kuritegevuse vastu võitlemise kohta, kuid puudub üldine regulatsioon küberohtude ennetamise ja tõkestamise kohta. Puudulik on ka käesoleva valdkonna mõisteaparaat. Mitmeid mõisteid, nagu näiteks kübersõda, küberrünnak, küberterrorism, kriitiline informatsiooni infrastruktuur, ei ole üheselt määratletud. Nimetatud mõisteid kasutatakse laialdaselt kogu maailmas, kuid nende sisu on olenevalt kontekstist erinev.

Vaadeldes avalikku Internetti globaalse võrgustikuna, on paratamatult selge, et sellega seonduvate küsimuste reguleerimine üksnes ühe riigi suveräniteedi piires on väheefektiivne. Kuna iga riik võib ise otsustada koostöö üle küberrünnetega seoses algatatud kriminaalasjade uurimisel, võib väita, et juriidilised lahendused küberruumi kaitseks saavutavad oma eesmärgi eeldusel, et neid saab kas rakendada ainult ühe riigi piires või et nende rakendamine on võimalik koostöös teiste riikidega. Siit nähtub küberjulgeoleku õigusliku raamistiku seos rahvusvahelise avaliku õigusega. Praegu on Eestil kriminaalasjade uurimisel võimalik koostööd teha ainult üksikute riikidega, kellega on sõlmitud vastavad õigusabilepingud. Koostöö teiste riikidega eeldab kas kahepoolsete lepingute või täiendavate rahvusvaheliste instrumentide sõlmimist. Euroopa Nõukogu Parlamentaarne Assamblee ja ka Euroopa Nõukogu (EN) 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.

Rahvusvahelises õiguses saab esile tõsta kahte rahvusvahelise õiguse instrumenti, mis käsitlevad kuritegusid arvutisüsteemide vastu. Kõige laialdasema mõjuga õigusakt on Euroopa Nõukogu arvutikuritegevuse vastane konventsioon, mis avati riikidele allakirjutamiseks 2001. aastal ja jõustus 2004. aastal. Eesti on

konventsiooniosaline alates 2003. aastast. Praegu saab konventsiooni puuduseks lugeda sellega liitunud riikide väikest arvu. Konventsiooni on ratifitseerinud 2008. aasta alguse seisuga 22 riiki ja lisaks on 22 riiki sellele alla kirjutanud. Samas ei ole mitmed ENi liikmesriigid veel jõudnud allakirjutamiseni. Positiivne on asjaolu, et konventsiooniga liitunud riikide arv kasvab pidevalt ja mitmes riigis on ratifitseerimisprotsess käimas. Tegemist on avatud konventsiooniga, millega saavad liituda ka riigid, kes ei ole ENi liikmesriigid. Sellistest riikidest on näiteks USA juba konventsiooniga liitunud, Kanada, Jaapan ja LAV on selle allkirjastanud. EN püüab konventsiooni võimalikult palju riikidele tutvustada ning julgustada neid liituma. Selle tulemusena on mitu riiki alustanud oma õigusaktide täiendamist konventsiooni eeskujul.

Euroopa Liidu õigusruum. ELi kontekstis reguleerib käesolevat teemat 2005. aastal vastu võetud raamotsus 222/2005/JSK infosüsteemide vastu suunatud rünnete kohta. Raamotsuse materiaalõiguse osa kordab põhimõtteliselt ENi konventsioonis reguleeritut. Raamotsuse puuduseks on selle kohaldatavus üksnes ELi 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.

Euroopa Liidu õiguses on mitmeid infoühiskonna arengule suunatud instrumente, mis loovad liikmesriikidele ühise platvormi riigisiseste õigusaktide väljatöötamiseks antud valdkonnas. Tuleb silmas pidada, et ELi direktiivid ei ole otseselt suunatud küberjulgeoleku tagamisele, vaid peavad silmas eeskätt siseturu huve. Direktiivid hõlmavad eeskätt järgmisi õigusvaldkondi:

- isikuandmete kaitse (95/46/EÜ ja 2002/58/EÜ);
- elektrooniline side (2002/58/EÜ);
- andmete säilitamine (2006/24/EÜ);
- avaliku sektori teabe taaskasutus (2003/98/EÜ);
- infoühiskonna teenused (2000/31/EÜ).

3.4.2 Riigisisene õigusruum

Küberjulgeoleku tagamiseks vajaliku õigusruumi kujundamisel alustati 2007. aastal analüüsi, et kaardistada õigusaktidega hõlmamata või vähekäsitletud valdkondi. Selle tulemusel on selgunud, et Eesti praegune IT-õiguspoliitika on eri ametkondade vahel killustatud ning sellest tulenevalt kohati vastuoluline. Näiteks on Eestis liberaalne infoühiskonna ja e-teenuste poliitika, samas pigem konservatiivne isikuandmete kaitse poliitika ning vaid ELi miinimumnõuetele vastav infoühiskonna teenuste regulatsioon. Samuti on eri õigusaktid vastu võetud erinevas kontekstis ja riigi erinevates arenguetappides ning infoõiguse kodifitseerimist pole seni toimunud.

Õigusanalüüsi tulemusena on selgunud vajadus järgnevate õigusaktide muutmiseks, täiendamiseks või kooskõlastamiseks:

Karistusseadustik. 2007. aastal tehtud õigusanalüüs näitas, et selles seaduses kehtestatud süüteokoosseisud ei kata küberjulgeoleku vajadusi, seda eeskätt sanktsioonide ning menetluse osas. Karistusseadustikku lisati süüteokoosseisude täiendused, et välistada olukorda, kus küberrünnete erinevad viisid on katmata või kus sanktsioon on teost hoidumiseks ebapiisav või ei võimalda kuritegu uurida. Olulise muudatusena täiendati seaduses terrorikuriteo koosseisu juhuks, kui seaduses käsitletud arvutikuriteod on toime pandud terroristliku eesmärgiga.

Elektroonilise side seadus. Elektroonilise side seadusest tulenevad nõuded elektroonilise side üldkasutatavatele võrkudele ja teenustele. Seadus sätestab elektroonilise side teenuste osutamise üldised tingimused ning määrab kindlaks turuosaliste miinimumkohustused andmeturbe, lõppkasutajatega sõlmitavate lepingute ja teiste kohustuste osas. Seega on tegemist õigusaktiga, millest lähtuvad kõige üldisemad nõuded informatsiooni infrastruktuurile.

Et saavutada olukorda, kus on kindlaks määratud riigi ja sideteenuste osutajate kohustused riigi julgeoleku tagamisel, on seaduses vaja sätestada sideteenuste osutajate kohustused kriitilise informatsiooni infrastruktuuri kaitsmisel. Logide võrdlemine sideteenuste osutajate poolt kogutud andmetest lähtudes ei ole otstarbekas, sest seaduses puuduvad logimise alused ja kord. Täpsustada oleks vaja logimiskohustusega seotud teemasid, sealhulgas kohustatud subjekte, kohustuse ulatust ja tähtaegu, aga ka sellega seonduvate kulude katmist. Arvestades seda, et võrkude turvalisus sõltub paljus ka lõppkasutaja teadlikkusest ja suutlikkusest oma arvutit kaitsta, vajavad täpsustamist nõuded lõppkasutajale. Kuna nimeserverid on kriitilise informatsiooni infrastruktuuri osa, on selles osas samuti vajalik regulatsiooni täiendamine.

Isikuandmete kaitse seadus. Isikuandmete kaitse seadus seondub kõigi juhtudega, kus konkreetsete meetmete võtmiseks on vajalik töödelda isikuandmeid. Praegu kohaldub see üldseadusena kõigile isikuandmete töötlemise juhtudele ning mis tahes isikuandmete töötlemiseks on vajalik seadusest tulenev selge alus. Seadus laieneb toimingutele, mida tehakse füüsilise isiku kohta käivate andmetega. Samuti sätestatakse selles andmete käideldavuse, tervikluse ja konfidentsiaalsuse tagamiseks vajalikud üldised organisatsioonilised, tehnilised ja füüsilised turvameetmed.

Küberjulgeoleku seisukohalt tuleb kaaluda erandi tegemist isikuandmete kaitse seaduse kohaldamisest juhul, kui isikuandmeid töödeldakse riigi julgeoleku huvides. Vastavat erandit lubab seaduse lähtekohaks olev ELi isikuandmete kaitse direktiiv 95/46/EÜ, kuid sisuliselt ka Euroopa Nõukogu sellekohane konventsioon ETS 108.

Kaaluda tuleks isikuandmete kaitse seaduse kohaldamisest erandi tegemist julgeolekuküsimustes ja kriitilise informatsiooni infrastruktuuri kaitse vajadusteks. Küsimus julgeoleku tagamise huvides erandi tegemisest

isikuandmete töötlemisele võiks saada lahendatud kas erandiga kõnealuses seaduses või eriregulatsiooniga kriitilise infrastruktuuri kaitset käsitlevates õigusaktides.

Koostöös Justiitsministeeriumi ja Andmekaitse Inspektsiooniga tuleb lahendada erandi ulatuse küsimus: lähtuvalt direktiivist soovitatakse erandeid vaid teatud nõuetest.[11]

Lisaks on vaja näha ette isikuandmete töötlemise alused õiguskaitseorganitele preventiivsetel ning reaktiivsetel eesmärkidel. Tuleb kaaluda kriitilise infrastruktuuri ettevõtete puhul delikaatsete isikuandmete töötlemiseks ette nähtud registreerimiskohustusega sarnase kohustuse rakendamist, et muuta turvameetmed ja nende kohaldamine läbipaistvamaks ning ühtlustada kaitse taset. Et parandada teabe liikumise operatiivsust asutuste vahel, tuleb täpsustada teabe vahetamise ja avalikustamise korda.

Avaliku teabe seadus. Avaliku teabe seadus teenib paralleelselt nii riigivõimu kvaliteetse teostamise kui ka põhiseaduses sätestatud infovabaduse realiseerimise eesmärki. Selles reguleeritakse avalikule teabele juurdepääsu võimaldamise aluseid ja korda, muuhulgas nõudeid teabevaldajate veebilehtede sisule. Seadus sätestab avaliku Interneti rolli riigi ja kodaniku vahelises suhtlemises ning võib kujuneda riigihaldusele koormavaks järjekordsete küberrünnakute korral, kuivõrd selles ei sisaldu otseseid aluseid näiteks veebilehele juurdepääsu piiramiseks või teabenõude täitmata jätmiseks. Seadus tuleb tervikuna läbi töötada, arvestades selle rakendatavust olukorras, kus riigi informatsiooni infrastruktuur on vaid osaliselt toimiv.

Muuhulgas on vaja täpsustada andmekogudest andmete saamise aluseid ja andmete ristkasutust preventiivsetel ning reaktiivsetel eesmärkidel. Niisuguse andmevahetuse õiguslike aluste olemasolu võimaldaks operatiivselt vahetada ja analüüsida rünnetega seonduvat informatsiooni. Otstarbekas on luua alus riigi ja kohalike omavalitsuste veebilehtedele või nende osadele juurdepääsu piiramiseks teatud tingimuste ilmnemisel. Kriitilise infrastruktuuri asutustele ja ettevõtetele tuleb kehtestada auditiskeem, mis hõlmab isikuandmete kaitse seaduse, avaliku teabe seaduse, infoühiskonna teenuse seaduse ja elektroonilise side seaduse täitmise kontrolli.

Infoühiskonna teenuse seadus. Infoühiskonna teenuse seaduses reguleeritakse Interneti-teenuse pakkujate vastutuse piiramist teenuse sisu eest, rämpspostiga seonduvat ning üldiseid nõudeid infoühiskonna teenuse osutamisele. Viimased on vajalikud selleks, et intsidendi korral oleks tagatud võimalus kontakteeruda veebilehe pidajaga. Seaduse peamine probleem on selle lakoonilisus ning üldine seostamatus Eesti õigusruumiga. Näiteks

[11] Liikmesriigid võivad artikli 6 lõikes 1, artiklis 10, artikli 11 lõikes 1 ja artiklites 12 ja 21 sätestatud kohustuste ja õiguste ulatuse piiramiseks võtta vastu õigusakte, kui sellised piirangud on vajalikud, et kindlustada:

a) riigi julgeolek; b) riigikaitse; c) avalik kord; d) kuritegude või reguleeritud kutsealade ametieetika rikkumiste ennetamine, uurimine, avastamine ja nende eest vastutuselevõtmine; e) liikmesriigi või Euroopa Liidu olulised majanduslikud või rahanduslikud huvid, sealhulgas raha-, eelarve- ja maksuküsimused; f) jälgimine, kontrollimine ja regulatiivne funktsioon, mis on kas või ajutiselt seotud avaliku võimu teostamisega punktides c, d ja e osutatud juhtudel; g) andmesubjekti kaitse või teiste isikute õiguste ja vabaduste kaitse.

saab rämpsposti eest karistada vaid infoühiskonna teenuse osutajat, järelevalve seaduse täitmise üle on hajutatud ning sanktsioonid mittemotiveerivad. Samuti puuduvad selged õiguslikud alused, mis reguleerivad andmete edastamist Interneti-teenuse pakkuja poolt või klientide pahavaraga nakatunud arvutite Interneti-ühenduse sulgemist.

Arvestades seda, et kõige otsesem ülevaade võrgus toimuva üle on just Interneti-teenuse osutajatel, on otstarbekas sätestada neile ulatuslikum koostöökohustus ja kriitilise infrastruktuuri puhul ka kontrollikohustus ning viia regulatsioon kõrgemale ELi direktiivi 2000/31 miinimumist.

3.5 Rahvusvaheline koostöö

Küberohtude globaalse iseloomu tõttu on küberruumi keeruline piiritleda riigipiiridega ning küberjulgeoleku tagamise eelduseks on tihe laiapinnaline rahvusvaheline koostöö. Üleilmse küberkultuuri teke on võimalik ainult siis, kui küberjulgeoleku alasesse koostöösse on kaasatud riigid, rahvusvahelised organisatsioonid, erafirmad ja neid ühendavad assotsiatsioonid, arvutiekspertide ja korrakaitseorganite rahvusvahelised koostöövõrgustikud, akadeemilised asutused, vabaühendused jne. Seoses sagenenud küberrünnakutega erinevates riikides on küberjulgeolek tõusnud mitmete rahvusvaheliste organisatsioonide ning riikide tähelepanu keskmesse. Paljudes riikides on loodud uued institutsioonid, mis tegelevad riigi küberruumi haavatavuse jälgimise, ohusuuniste analüüsi ning infotehnoloogia kasutuse turvalisuse tõstmisega. Rahvusvaheline koostöö mitmepoolses raamistikus on muutumas küberruumi julgeoleku ja kaitse oluliseks eestvedajaks.

Küberjulgeoleku temaatika on rahvusvahelise üldsuse jaoks alles üsna uus. Kuigi arenenud tööstusriigid teadvustavad teravalt küberjulgeoleku probleeme ning on ammu asunud tegelema oma infosüsteemide kaitsmisega, on rahvusvaheliste kokkulepete saavutamine küberjulgeoleku küsimustes globaalses mastaabis keeruline. Esiteks on riikidel väga erinev IT-lahenduste rakendamise tase, lisaks raskendavad valdkonna kiire areng ning riigisiseste huvigruppide surve rahvusvaheliste õigusaktide ja normide kehtestamist. Enne rahvusvaheliste juriidiliste instrumentide väljatöötamist tuleb riikide vahel pidada põhjalikke konsultatsioone ning uute instrumentide loomine on seetõttu väga aeganõudev protsess. Samas eeldab küberjulgeoleku rahvusvaheline olemus hästi toimivaid rahvusvahelise õiguse instrumente, mitme- ja kahepoolset koostööd küberkuritegevuse vastases võitluses ja küberkaitse- ning infoturbealaste koostöövõrgustike toimimist.

Rahvusvahelises õiguses valitseb olukord, kus ainus otseselt küberkuritegude ennetamisele ja lahendamisele suunatud dokument on Euroopa Nõukogu arvutikuritegevuse vastane konventsioon. Konventsiooni puuduseks on eeskätt asjaolu, et sellega ühinenud riikide arv pole väga suur, mistõttu riikide koostöö küberkuritegevuse alastes kriminaalasjades on piiratud. Samuti lähtub konventsioon eeldusest, et arvutikuriteod on eeskätt varavastased kuriteod ning pannakse toime üksikürituste na. Eesti kogemus aga näitab, et sisuliselt võidakse arvuteid ja võrke nii rahvaalgatuse korras kui ka organiseeritult kasutada riigi toimimise takistamiseks ning propaganda eesmärgil.

Küberjulgeoleku tagamiseks tuleb 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.

Seoses 2007. aasta kevadel toimunud rünnakute ja nende käigus saadud kogemustega, aga ka meie endi järgnenud algatustega oodatakse Eestilt rahvusvahelisel tasandil suurt panust ja mõningatel juhtudel ka protsesside eestvedamist. Seetõttu tuleb eelnevalt eritleda meie panustamise potentsiaali, suutlikkust ning ressursse, mida oleme võimelised ja valmis eraldama rahvusvahelistes algatustes osalemiseks. Rahvusvahelisel tasandil ollakse väga huvitatud Eesti ühiskonna keskmisest kõrgemast IT-seotusest tulenevatest kogemustest ja meie jaoks on tähtis rahvusvahelise küberjulgeoleku alase teadlikkuse tõstmine ning koostöiste ennetus- ja kaitsemeetmete toetamine.

Eesti on asunud aktiivselt tegelema küberjulgeoleku alaste algatuste elluviimisega nii rahvusvahelistes organisatsioonides kui ka kahepoolse koostöö kaudu. Eesti oli 2008. aastal vastu võetud NATO küberkaitsepoliitika üks algatajaid. Samuti on peetud konsultatsioone Euroopa Nõukoguga küberkuritegevusega võitlemise teemal ja ELi institutsioonidega kriitilise informatsiooni infrastruktuuri kaitse ühiste põhimõtete väljatöötamiseks ning küberjulgeoleku rõhutamiseks Euroopa julgeolekut käsitlevates strateegiadokumentides. 2008. aastal on Eestil kavas tõstatada küberjulgeoleku teema Euroopa Julgeoleku- ja Koostööorganisatsiooni (OSCE) julgeolekufoorumi eesistujana. Eesti on olnud aktiivne ka Ühinenud Rahvaste Organisatsiooni (ÜRO) ja selle eriorganisatsioonide küberjulgeoleku ja IT-alastes algatustes. Eesti liitumisel Majanduskoostöö ja Arengu Organisatsiooniga (OECD) 2009. aastal tekib institutsionaalne võimalus kogemuste vahetamiseks ka selle organisatsiooni raames.

Jätkuv laiaulatuslik tegevus rahvusvahelistes organisatsioonides on väga vajalik, et teadvustada küberjulgeoleku probleeme ning juhtida teiste riikide kõrge poliitilise tasandi tähelepanu sellele teemale. Paljudes riikides on ikka veel juurdunud arusaam, et tegu on tehnilise küsimusega, mis ei vaja poliitilist tähelepanu. Kuid ainult poliitilise tähelepanu abil on võimalik algatada küberjulgeoleku tagamiseks vajalike rahvusvaheliste normide ja õigusaktide väljatöötamist ning teha riikide vahel koostööd.

Infotehnoloogia üldise arenguga kaasnenud kuritegevuse tõus võrgukeskkonnas on praeguseks muutunud rahvusvahelise küberjulgeoleku kõige laiaulatuslikumaks probleemiks. Kuna virtuaalkeskkonnas puuduvad füüsiliselt tajutavad tõkked ning IT-kuritegude efektiivsel lahendamisel on oluline tegur aeg, siis on õiguskaitseorganite omavaheline koostöö ning operatiivne infovahetus kriitilise tähtsusega. Seetõttu on vajalik tihe koostöö Eesti õiguskaitseorganite ja Interpoli, Europoli ning teiste küberkuritegevuse vastase võitlusega tegelevate valitsusvaheliste organisatsioonide ja erialavõrgustike vahel.

Lisaks rahvusvahelistes organisatsioonides ning kahepoolsete suhete raames tehtavale riikidevahelisele koostööle tuleks tähelepanu pöörata ka infosüsteemide turvalisusega tegelevatele IT-ettevõtetele, rahvusvahelist erasektorit koondavatele assotsiatsioonidele ning teistele analoogsetele eraühendustele. Eesti era- ja avaliku sektori infoturbeekspertide koostöökogemus on ka rahvusvahelises praktikas hea näide, mida tuleks teiste riikidega jagada. Koostöövõrgustikel on keskne roll üleilmse küberruumi turvalisuse tagamisel, sest vastastikuse usalduse alusel töötavad ekspertide võrgustikud võimaldavad ekspertteavet ja informatsiooni tõhusalt vahetada.

Soodustada tuleb Eesti osalust ka rahvusvahelistes uurimis- ja teadusvõrgustikes, pöörates põhitähelepanu Eesti ülikoolide IT- ja infoturbealase kompetentsuse suurendamisele ja koostööle rahvusvaheliselt tunnustatud teaduskeskuste ja uurimisinstituutidega. Eesti ülikoolide sidemetel rahvusvaheliste akadeemiliste võrgustikega on suur tähtsus IT- ja infoturbealase õppe- ja teadustöö arendamisele, mis mõjutab otseselt riigi küberjulgeoleku tagamist tippspetsialistide ettevalmistamise kaudu.

Üleilmse küberjulgeoleku tugevdamisel on Eesti jaoks oluline aktiivne tegutsemine rahvusvahelistes organisatsioonides.

ÜHINENUD RAHVASTE ORGANISATSIOON

ÜROs tuleb kogu ÜRO liikmeskonnale teadvustada, et tegemist ei ole ainult tehnoloogiliselt arenenud ja digitaliseerunud riikide probleemiga, vaid üleilmse küsimusega. Seetõttu tuleks püüelda küberkuritegevuse ja küberrünnete moraalset hukkamõistu üleilmsel tasandil. Prioriteetselt tuleks käsitleda kübervaldkonda puudutavaid resolutsioone ja riigid peaksid välja töötama oma vastavad seisukohad ja otsima neile laiemat rahvusvahelist toetust, eelkõige samameelsetelt riikidelt.

ÜRO eriorganisatsioonidest tegelevad küberjulgeoleku küsimusega Interneti Haldamise Foorum (*Internet Governance Forum* – IGF) ja Rahvusvahelise Telekommunikatsiooniliidu (*International Telecommunication Union* – ITU) kõrgetasemeline ekspertgrupp. 2006. aastast on Eesti e-valitsemise vanemekspert lähetatud ÜRO Koolitus ja -uuringukeskuse (*United Nations Institute for Training and Research - UNITAR)* peakorterisse Genfis.

EUROOPA LIIT

Küberjulgeoleku tagamine ning küberkuritegevuse vastane võitlus puudutavad kõiki EL liikmesriike. ELi ühine õigusruum ning institutsioonid, samuti liikmesriikide vaheline koostöö loovad aluse küberkuritegevuse edukaks ennetamiseks ja tagajärgede haldamiseks. ELis alustati küberkuritegevuse haldamist juba 1999. aastal. ELi Tampere programmis mainiti esmakordselt kõrgtehnoloogiaga seotud julgeolekut ning Euroopa Liidu Nõukogu võttis vastu Euroopa Nõukogu arvutikuritegevuse konventsiooni puudutava ühispositsiooni. Olulisemad vastuvõetud õigusaktid on:

- nõukogu otsus lastepornograafia leviku tõkestamiseks Internetis (2000);

- komisjoni teatis „Turvalisema infoühiskonna poole, parandades informatsiooni infrastruktuuride turvalisust ja võideldes arvutikuritegevuse vastu” (2001);
- raamotsus infosüsteemide vastu suunatud rünnakute kohta (2005).

2007. aasta mais avaldas Euroopa Komisjon teatise „Küberkuritegevuse vastase võitluse üldise poliitika kujundamine” ning 8.–9. novembril 2007 võttis justiits- ja siseasjade nõukogu vastu küberkuritegevusega võitlemise teemalised järeldused. Leiame, et on oluline kujundada ELi ühtset, laiaulatuslikku ja selget küberkuritegevuse vastase võitluse poliitikat, mis peaks hõlmama võimalikult paljusid nimetatud teemaga seotud valdkondi. Poliitikas tuleb selgelt eristada riigi julgeolekumõõdet ja majanduskeskkonda puudutavat osa ning teisalt üksikisiku õigusi ja turvalisust puudutavat osa. Ühtse poliitika väljatöötamise aluseks peaks olema avatud ja arengut võimaldav lähenemine.

Vajalike tegevustena ELis näeme õiguskeskkonna täiendavat analüüsi nii küberruumi turvalisuse kui ka küberkuritegude vastase võitluse küsimustes. Täiendavalt tuleks analüüsida küberkuritegevuse mõju ELi konkurentsivõimele ning ELi seadusandliku baasi vastavust uutele ohtudele, aga ka ELi õigusakte, mis käsitlevad otseselt riigi kui terviku huvide vastu suunatud küberründeid.

ELis 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, ELi 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).*

NATO

NATOs on välja töötatud NATO küberkaitsepoliitika ja küberkaitsekontseptsioon. NATO küberkaitse põhimõtete väljatöötamisel lähtuvad liikmesriigid NATO solidaarsuseprintsiibist, mis on kooskõlas liitlaste suveräänsusega. Teisisõnu, eesmärgiks on saavutada olukord, kus NATO liitlased oleksid võimelised ja valmis vajadusel üksteisele küberrünnakute tõrjumisel abi osutama ning kus kõik NATO liikmesriigid arendaksid oma riigisisest küberkaitsevõimet. Selles kontekstis on Eesti huvitatud tihedamate kahe- ja mitmepoolsete koostöövõrgustike loomisest NATO kui organisatsiooni sees ning ei välista analoogsete kontaktide loomise vajadust ka NATO partnerriikidega, kui selleks saavutatakse vastav NATO otsus.

EUROOPA NÕUKOGU

Euroopa Nõukogu arvutikuritegevuse konventsioon jõustus 2004. aastal. See sisaldab erinevate küberkuritegevuse vormide definitsioone ja loob aluse õiguskoostööks konventsiooni osalisriikide vahel. Konventsiooniosaliseks saamise järel peavad riigid täiendama vastavalt konventsiooni sätetele oma õigusakte. Eraldi kontrollimehhanisme ette nähtud ei ole. Konventsioon on ühinemiseks avatud ka riikidele, kes ei ole ENi liikmed.

Konventsiooni laiemaks tutvustamiseks ja sellega ühinemise hõlbustamiseks on loodud eraldi projekt „Küberkuritegevuse projekti elluviimine“ (*Implementation of the Project on Cybercrime)*. Projekti eesmärk on tutvustada ENi arvutikuritegevuse konventsiooni, aidata sellega ühineda ning toetada konventsiooni ideoloogia üleilmset levikut.

Arvestades ENi liikmesriikide hulgas valitsevat arvamust, on praegu esmatähtis keskendada jõupingutused sellele, et laiendada arvutikuritegevuse konventsiooni kui peamise seda teemat käsitleva rahvusvahelise õigusakti osaliste ringi. Kuni seda pole saavutatud, ei toeta paljud riigid uute lepingute või lisaprotokollide väljatöötamist. See ei välista siiski, et Eesti esitab tulevikus mõne hästi põhjendatud algatuse olemasoleva õigusliku aluse täiendamiseks, kui täiendav analüüs seda vajalikuks peab.

Olenemata sellest, kas uusi juriidilisi algatusi esitatakse või jäädakse olemasolevate dokumentide raamidesse, on tähtis, et riigid kindlustaksid oma õigussüsteemis rahvusvahelise koostöö ja infovahetuse takistamatu toimimise ning arendaksid välja õigusliku aluse, mis hõlbustaks ulatuslike küberrünnakute korral poliitilisi konsultatsioone ja infovahetust kõikidel tasanditel.

EUROOPA JULGEOLEKU- JA KOOSTÖÖORGANISATSIOON (OSCE)

OSCEs seostatakse küberjulgeoleku temaatikat peamiselt terrorismiohuga. Eestil on plaanis tõstatada küberjulgeoleku teema organisatsiooni julgeolekukomitees või julgeolekualasel koostööfoorumil, mille eesistujaks Eesti on 2008. aasta kevadest sügiseni. Lisaks kavatseb Eesti esitada küberjulgeoleku eriteemana OSCE Parlamentaarse Assamblee põhiistungjärgu päevakorda.

MAJANDUSKOOSTÖÖ JA ARENGU ORGANISATSIOON

Majanduskoostöö ja Arengu Organisatsioonis (OECD) tegelevad küberjulgeolekuga info-, arvuti- ja sidepoliitika komitee (*Committee for Information, Computer and Communications Policy)* ning selle alltöörühmad, sealhulgas info turvalisuse ja privaatsuse töörühm (*Working Party on Information Security and Privacy)*. Komitee on võtnud vastu mitu soovitust, näiteks 2002. aastal „Soovitused infosüsteemide ja -võrkude turvalisuse tagamiseks” („*Recommendation Concerning Guidelines for the Security of Information Systems and Networks”)* ning 2007. aastal „Soovitused piiriüleseks koostööks privaatsust kaitsvate seaduste jõustamisel” („*Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy”*).

OECD nõukogu ministrite kohtumisel 16. mail 2007 kiideti heaks OECD laienemisstrateegia ning otsustati kutsuda liitumisläbirääkimistele viis riiki, sealhulgas Eesti. Eesti liitumisprotsess OECDga kestab ligikaudu kaks aastat ning selle perioodi jooksul on Eestil võimalik OECD töös osaleda piiratult. Praegu osaleb Eesti info-, arvuti- ja sidepoliitika komitee ning selle alatöörühmade töös vaatlejana. Pärast OECDga liitumist on võimalik töösse lülituda täies mahus. Liitumisläbirääkimiste käigus hindab komitee muuhulgas Eesti suutlikkust edendada infosüsteemide ja -võrkude kasutamise turvalisust ning vastava teadlikkuse tõstmist.

ERIALASED ORGANISATSIOONID JA RAHVUSVAHELISED KOOSTÖÖVÕRGUSTIKUD

Küberruumi turvalisuse tagamisel on tähtis infovahetus ja rahvusvahelisel tasandil toimib see kõige tõhusamalt koostöövõrgustike abil. Tänu taolistele koostöövõrgustikele on võimalik operatiivselt tegutseda küberjulgeoleku tagamisel ja küberkuritegevuse vastu võitlemisel. Nii era- kui avaliku sektori erialaste koostöövõrgustike kaudu toimub IT alaste uuenduste, parimate praktikate ning muu ekspertteabe vahetus. Küberjulgeoleku alase ekspertteabe vahetus eeldab tihedat koostööd rahvusvaheliste andmeturbe, küberkaitse ja korrakaitse koostöövõrgustikega. Olulisematena võib välja tuua riikide CERTe ühendava rahvusvahelise võrgustiku, riiklike CERT agentuuride vahelise võrgustiku *(GovCERT*), korrakaitsekoostöö Interpoli ja Europoliga, kriitilise informatsiooni infrastruktuuri kaitse ja uuringutega tegelevad organisatsioonid (*Critical Information Infrastructure Protection, Common Criteria jpt.)*

4 Eesmärgid ja meetmed küberjulgeoleku taseme tõstmisel Eestis

Riigi kui terviku küberruumi haavatavuse vähendamiseks on vaja, et oleksid saavutatud järgmised strateegilised eesmärgid:

- Eestis on laiaulatuslikult rakendatud astmeline turvameetmete süsteem, mis tagab Eesti riigi küberjulgeoleku eesmärkide saavutamise;
- Eesti on väga kõrge infoturbealase kompetentsuse ja teadlikkusega riik;
- infosüsteemide turvalist ja laialdast kasutamist toetab proportsionaalne regulatsioon;
- Eesti on üks juhtivaid riike rahvusvahelises koostöös küberjulgeoleku tagamisel.

Iga nimetatud eesmärgi saavutamiseks on kindlaks määratud vastavad tegevusvaldkonnad. Valdkondades on omakorda defineeritud meetmed, mis koondavad endas eesmärkide saavutamiseks vajalikke tegevusi.

4.1 Turvameetmete süsteemi arendamine ja üleüldine rakendamine

Eesti vastu suunatud küberrünnakute analüüsid tõstsid esile vajaduse töötada välja spetsiaalne riiklik küberjulgeolekut tagav turva- ja vastumeetmete süsteem. Küberjulgeoleku turvameetmete süsteemi rakendamine tagab tegevusplaanid küberrünnakutele reageerimiseks ja kahjustatud infosüsteemide kiireks taastamiseks. Samuti sätestab küberjulgeoleku turvameetmete süsteem vastutegevuse riigi küberjulgeolekut ja kaitsevõimet ohustavate küberrünnakute korral ning kaitsemeetmed operatiivseks rakendamiseks Eestis ja rahvusvaheliselt.

Küberjulgeoleku turvameetmete süsteem käsitleb tegevusi organisatoorse koostöö, füüsilise turbe ja tehniliste meetmete valdkonnas. Tehnilised meetmed peavad hõlmama tegevusi kõigi kriitilise informatsiooni infrastruktuuri teenuste pakkumisel kasutatavate süsteemide ja platvormide jaoks. Turvameetmete rakendamine on oluline, sest küberjulgeoleku probleemide kasv ei tohiks takista info- ja kommunikatsioonitehnoloogial olemast ka edaspidi üheks Eesti majanduse olulisemaks kasvumootoriks

Riigiasutused kasutavad infoturbe tagamiseks ISKE kolmeastmelist turvameetmete süsteemi. Kriitilise informatsiooni infrastruktuuri jaoks töötatakse välja astmeline küberjulgeoleku turvameetmete süsteem.

Indikaator eesmärgi täitmisest: aastaks 2013 on kriitilise informatsiooni infrastruktuuri küberjulgeoleku turvameetmete süsteem täielikult rakendunud.

Eesmärgi saavutamiseks keskendutakse kolmele meetmele:

- kriitilise informatsiooni infrastruktuuri (KII) kaitse;

- turvameetmete süsteemi arendamine ja rakendamine;
- organisatsioonilise koostöö tugevdamine.

Meede 1: kriitilise informatsiooni infrastruktuuri (KII) kaitse

Kriitilise informatsiooni infrastruktuuri kaitse meede koondab järgmisi tegevusi:

- **kriitilise infrastruktuuri teenuste määratlemine**. Eesmärgiks on kirjeldada teenuseid, mis tagavad igapäevase elutegevuse – koordineerib Siseministeerium;
- **kriitilise informatsiooni infrastruktuuri teenuste määratlemine**. Eesmärgiks on kirjeldada informatsiooni infrastruktuuri teenuseid, mis tagavad kriitilise infrastruktuuri toimimise – Siseministeerium koos Majandus- ja Kommunikatsiooniministeeriumiga;
- **kriitilise infrastruktuuri ja kriitilise informatsiooni infrastruktuuri vahelise sõltuvuse määratlemine**. Eesmärgiks on määratleda kriitilise infrastruktuuri teenuste otsene sõltuvus kriitilise informatsiooni infrastruktuuri teenustest – Siseministeerium koos Majandus- ja Kommunikatsiooniministeeriumiga;
- **kriitilise informatsiooni infrastruktuuri teenuste hindamine**. Eesmärgiks on välja töötada ühtne metoodika kriitilise infrastruktuuri infosüsteemide ja neid toetavate teenuste haavatavuse hindamiseks ning kehtestada standardsed riskianalüüsi meetodid nii elutähtsate sektorite kui ka ettevõtete tasandil – Siseministeerium, Majandus- ja Kommunikatsiooniministeerium, Kaitseministeerium;
- **küberjulgeoleku ohuhinnangute koostamine**. Eesmärgiks on koguda ja töödelda informatsiooni olukorrast küberruumis, et planeerida ennetustegevusi ja vajalikke ning piisavaid meetmeid küberjulgeolekut ohustavate rünnakute korral. Kriitilise infrastruktuuri riskianalüüside põhjal koostatud perioodilised ohuhinnangud lülitatakse olemasolevasse riikliku julgeoleku tagamise protsessi – Siseministeerium ja Kaitseministeerium.

Meede 2: turvameetmete süsteemi arendamine ja rakendamine

Turvameetmete süsteemi arendamine ja rakendamine koondab järgmisi tegevusi:

- **turvameetmete arendamine, uuendamine ja täiendamine**. Eesmärgiks on:
    - määrata kindlaks kriitilise infrastruktuuri täiendavate (st lisaks andmeturbenõuetest tulenevate) infoprotsesside talitluspidevust ja infosüsteemide taastet tagavad turvalahendused ning vastavad turvameetmed – Kaitseministeerium, Majandus- ja Kommunikatsiooniministeerium;
    - määratleda minimaalne vajalik informatsiooni infrastruktuuri funktsionaalsus ja kindlustada selle olemasolu kriisisituatsioonis – Kaitseministeerium, Siseministeerium, Majandus- ja Kommunikatsiooniministeerium;

- määrata kindlaks kriitilise infrastruktuuri infosüsteemide vastu suunatud rünnete korral eriolukorras lubatavad vastumeetmed, sh luure- ja ründemeetmete rakendatavuse põhimõtted ning nendele vastavalt võimalikud vastumeetmed – Kaitseministeerium, Siseministeerium, Majandus- ja Kommunikatsiooniministeerium;
- töötada välja infoturbemeetmete majanduslikku otstarbekust ja optimaalsust tagav metoodika ning määrata kindlaks selle rakendamiseks vajalikud tegevused – Kaitseministeerium, Majandus- ja Kommunikatsiooniministeerium;
- töötada välja turvalahenduste rünnatavuse kontrollimetoodika ning määrata kindlaks selle rakendamiseks vajalikud tegevused – Kaitseministeerium, Majandus- ja Kommunikatsiooniministeerium;
- arendada nii kriitilise infrastruktuuri kui ka riigi tasandil EMI-rünnete tuvastamise ja seire süsteeme – Siseministeerium, Majandus- ja Kommunikatsiooniministeerium.

- **Turvameetmete rakendamine nii era- kui avalikus sektoris**. Eesmärgiks on kasutada ajakohaseid ja tõhusaid turvameetmeid. Oluline on:
  - tugevdada Interneti infrastruktuuri;
  - suurendada juhtimissüsteemide (SCADA-juhtimissüsteemide [12]) turvalisust;
  - testida KII serveriruumide vastu suunatud RF EMI-ründe[13] kindluse taset;
  - testida KII infotöötlusseadmete (serverid, tööarvutid, sideseadmed jms) vastu suunatud RF EMI-ründe kindluse taset.
- **Järelevalve korraldamine turvameetmete rakendamise üle**. Iga infosüsteemi omanik peab rakendama vajalikke ja piisavaid turvameetmeid. Kriitilise infrastruktuuri turvameetmete elluviimise järelvalvet koordineerivad Siseministeerium ja Majandus- ja Kommunikatsiooniministeerium koostöös kriitilise infrastruktuuri erinevate sektorite eest vastutavate ministeeriumidega.

Meede 3: organisatsioonilise koostöö tugevdamine

Organisatsioonilise koostöö tugevdamise meede koondab järgmisi tegevusi:

- luua Vabariigi Valitsuse julgeolekukomisjoni alakomisjoni juurde küberjulgeoleku strateegia eesmärkide elluviimise eest vastutav nõukogu;
- määrata kindlaks riigi infosüsteemide turvalisuse eest vastutava struktuuriüksuse ülesanded Majandus- ja Kommunikatsiooniministeeriumi valitsemisalas ning asuda neid täitma, et tagada riskianalüüside koostamine eri tasanditel: riigi tasandil ning kriitilise infrastruktuuri asutuste ja

[12] SCADA - rahvusvaheliselt käibelolev lühend tööstuses, energiamajanduses ja mujal kasutatavate automatiseeritud juhtimissüsteemide kohta (SCADA – ingl.k. *Supervisory Control and Data Acquisition)*

[13] RF EMI – ingl k. *radio frequency electro-magnetic impulse,* raadiolainetel töötava sagedusega elektromagnetiline häiritus

ettevõtete tasandil. Asjakohaste turvameetmete kindlaksmääramise, valimise ja järelevalve nende rakendamise üle tagab Majandus- ja Kommunikatsiooniministeerium.

- täiustada hädaolukorraks valmisoleku seaduse alusel koostatavat ministeeriumide riskianalüüside metoodikat ja rakendada seda küberjulgeoleku aspektist – vastutab Siseministeerium koos Majandus- ja Kommunikatsiooniministeeriumiga;
- luua eksperttöörühm infoturbeprobleemide tuvastamiseks, ressursivajaduse hindamiseks ja operatiivseks infovahetuseks. Eksperttöörühm annab infoturbealase sisendi Vabariigi Valitsuse julgeolekukomisjoni küberjulgeoleku nõukogule – vastutab Majandus- ja Kommunikatsiooniministeerium;
- parandada intsidentide analüüsimise võimet – vastutavad Majandus- ja Kommunikatsiooniministeerium ning Kaitseministeerium;
- õigusalaste ettepanekute väljatöötamise eest vastutab Kaitseministeeriumi juures loodud küberjulgeoleku strateegia komisjon koostöös Justiitsministeeriumiga;
- koordineerida küberjulgeoleku alast teavitustegevust ja määrata riigisisese teavitustöö eest vastutav keskne asutus – koordineerivad Majandus- ja Kommunikatsiooniministeerium, Kaitseministeerium ja Välisministeerium.

4.2 Infoturbealase kompetentsuse suurendamine

Vajaliku küberjulgeoleku alase kompetentsuse saavutamine seab järgmised eesmärgid väljaõppe ja teadusuuringute osas:

- tagada infoturbealase väljaõppe kvaliteet ja kättesaadavus, et saavutada piisav kompetentsus nii avalikus kui ka erasektoris, kehtestada ühtsed infoturbealase pädevuse nõuded IT-töötajatele ning luua vastav täiendusõppe- ja atesteerimissüsteem;
- intensiivistada küberjulgeolekuks vajalikke uuringuid ning arendustööd, et tagada riigi kaitsevõime antud valdkonnas, tõhustada rahvusvahelist teadusalast koostööd ning kindlustada pädevus kõrgtasemel väljaõppe pakkumiseks.

Indikaator eesmärkide täitmisest: aastaks 2013 on küberjulgeoleku valdkonna magistriõppe läbinud vähemalt 200 õppurit, infoturbe kursuste osakaal suureneb bakalaureuseõppes 50%.

Eesmärgi saavutamiseks keskendutakse kahele meetmele:

- küberkaitse alase väljaõppe korraldamine
- teadus- ja arendustegevuse intensiivistamine

Meede 1: küberkaitse alase väljaõppe korraldamine

Küberkaitse alase väljaõppe korraldamine koondab järgmisi tegevusi:

- küberkaitse ja infoturbe eriala õppe korraldamine kõigil tasemetel.

- küberkaitse ja infoturbe alase täiendusõppe korraldamine.
- infoturbe ja küberkaitse alaste kompetentsusnõuete kehtestamine nii avaliku kui ka erasektori töötajatele ning vastava atesteerimise korraldamine.
- kriisisituatsioonides tegutsemise valmiduse suurendamine nii era- kui avalikus sektoris. Eesmärgiks on valmistada ette eri osapoolte koostöö kriisiolukordades tegutsemiseks. Selleks:
    - lülitada küberjulgeoleku tagamise operatiivtegevuskava riigi kriisijuhtimissüsteemi;
    - korraldada ennetustegevust ja kriisijuhtimist Vabariigi Valitsuse tasemel;
    - korraldada ohuhinnangute põhjal koostatud õppusi kriisisituatsioonides tegutsemiseks ning osaleda aktiivselt rahvusvahelistel õppustel.

  Vastutajad: Kaitseministeerium, Majandus- ja Kommunikatsiooniministeerium, Haridus- ja Teadusministeerium

Meede 2: teadus- ja arendustegevuse intensiivistamine

- määratleda küberkaitsealaste teadmiste kogum, arvestades nii Eesti kui ka rahvusvahelist kogemust;
- toetada küberkaitsealaseks kompetentsuseks vajalikku teadus- ja arendustegevust;
- tegelda Eestisse loodava NATO Küberkaitse Kompetentsikeskuse arendamise, rahvusliku teadusalase kompetentsuse kasvatamise ning teadlaskogukonna rahvusvahelisemaks muutmisega.

4.3 Küberjulgeolekuks vajaliku õigusruumi kujundamine

Küberjulgeoleku tagamiseks vajaliku õigusruumi kujundamisel on eesmärgiks luua piisav õigusraamistik küberkuritegevuse vastu võitlemiseks, kriitilise infrastruktuuri küberkaitse tagamiseks ning infoturbe standardite kehtestamiseks kõikidele arvutikasutajatele.

Peamised tegevused õigusruumi kujundamisel:

- küberjulgeoleku ja küberkuritegevusega seotud õigusalaste definitsioonide väljatöötamine;
- küberjulgeoleku tagamiseks vajalike õigusaktide ettevalmistamine ja rakendamine, sh kohustuslike turvameetmete ja standardite juurutamine kriitilise infrastruktuuri ettevõtetele ja infoturbealaste miinimumnõuete kehtestamine kõigele infosüsteemidele;
- olemasoleva seadusandluse täiendamine küberjulgeoleku tagamise aspektist;
- kriitilise infrastruktuuri küberkaitseks vajalike õigusaktide väljatöötamine;
- initsiatiivid küberjulgeolekualase rahvusvahelise õiguse loomisel ja arendamisel.

4.4 Rahvusvahelise koostöö arendamine

Käesoleva strateegia eesmärkideks rahvusvahelise koostöö valdkonnas on Eesti kogemustest ja ühiskonna infotehnoloogiaalasest seotusest tulenevate teadmiste jagamine ning selle pinnal rahvusvahelise teadlikkuse tõstmine ning koostöiste ennetus- ja kaitsemeetmete toetamine. Küberjulgeoleku tagamisega seotud rahvusvahelise koostöö arendamisel seab strateegia järgmised eesmärgid:

- saavutada rahvusvaheline moraalne hukkamõist küberrünnetele, mis häirivad inimeste elu ja ühiskonna toimimist, jälgides samas, et võitlus küberohtudega ei saaks üldtunnustatud inimõiguste ja demokraatlike vabaduste piiramise ettekäändeks;
- saavutada võimalikult laiapindne ühinemine küberkuritegevust ja -ründeid käsitlevate rahvusvaheliste konventsioonidega ning nende sisu jõudmine rahvusvahelise üldsuse teadvusse;
- osaleda rahvusvahelise küberjulgeoleku poliitika väljatöötamisel ja jõustamisel, samuti üleilmse küberkultuuri kujundamisel;
- arendada küberjulgeolekuga tegelevaid rahvusvahelisi koostöövõrgustikke ja tõhustada nende toimimist.

Indikaator eesmärkide täitmisest: Eesti on 2010. aastaks esitanud vähemalt ühe uue küberjulgeoleku alase algatuse või osalenud niisuguse algatuse väljatöötamisel rahvusvahelistes organisatsioonides ning toetanud aktiivselt koostöövõrgustike tööd saatkondade võrgu abil maailmas.

Rahvusvahelise koostöö eesmärkide saavutamiseks vajalike tegevuste elluviimist koordineerib Välisministeerium.

Tegevused küberjulgeoleku tagamisega seotud üldise rahvusvahelise koostöö tõhustamiseks:

- tutvustada laiapinnaliselt küberjulgeoleku ja -kaitse valdkonna probleeme, viidates neile kui globaalsetele probleemidele;
- kutsuda riike üles ratifitseerima ENi küberkuritegevuse konventsiooni ja luua konventsioonile laiem kõlapind;
- osaleda erialakonverentsidel, -seminaridel ja -foorumeil ning käsitleda seal järjepidevalt küberjulgeoleku probleeme;
- toetada küberjulgeoleku ja -kaitsega tegelevate rahvusvaheliste ettevõtete, assotsiatsioonide, rahvusvaheliste korporatsioonide, teadusasutuste ja vabaühenduste tegevust;
- propageerida valdkonna parimaid tavasid ja tõhustada nende levikut rahvusvahelisel tasandil;
- nimetada Eesti esindajad küberjulgeoleku ja -kaitsega tegelevate rahvusvaheliste organisatsioonide ekspertgruppidesse.

Tegevused rahvusvahelistes organisatsioonides:

ÜRO

- osaleda aktiivselt infoühiskonna maailma tippkohtumise ja Interneti Haldusfoorumi töös, esineda igal aastakonverentsil kõnega, juhtida töögruppi või osaleda selles;
- osaleda oma esindajate ja ekspertidega ITU küberturvalisuse kõrgetasemelise ekspertgrupi töös;
- osaleda aktiivselt Rahvusvahelise Telekommunikatsiooniliidu Globaalse Küberjulgeoleku foorumi tegevuses.

Euroopa Nõukogu

- kutsuda kõiki riike, nii ENi liikmesriike kui ka teisi riike üles ühinema ENi küberkuritegevuse konventsiooniga;
- tutvustada laiemalt konventsiooni, mis on praegu ainus õiguslikult siduv rahvusvaheline dokument maailmas, keskendudes esmalt Euroopa riikidele;
- toetada ENi küberkuritegevuse vastast projekti „Küberkuritegevuse projekti elluviimine" (*Implementation of the Project on Cybercrime)*, mille eesmärgiks on tutvustada ENi küberkuritegevuse konventsiooni, aidata sellega ühineda ning toetada konventsiooni ideoloogia üleilmset levikut;
- eritleda konventsioonile lisaprotokollide koostamise võimalusi ja vajadust;
- kaasata Eesti esindajaid ENi Parlamentaarses Assamblees tegelema küberkuritegevuse valdkonnaga ning tegema sellealast tutvustustööd.

Euroopa Liit

- töötada tugevdatud operatiivkoostöö tekkimise nimel Euroopa Liidu liikmesriikide õiguskaitse- või kohtuasutuste vahel, parandada ja hõlbustada koostööd liikmesriikide küberkuritegevuse üksuste, muude pädevate asutuste ja teiste ekspertide vahel;
- osaleda aktiivselt küberkuritegevuse vastases koostöös, sealhulgas Euroopa Liidu ühiste seisukohtade kujundamises rahvusvahelisel tasandil;
- uurida koos liikmesriikidega nende infoinfrastruktuuri vastu suunatud kooskõlastatud ja laiaulatuslikke ründeid, et neid ennetada ja nende mõjusid neutraliseerida. See peaks hõlmama ka vastastikust koordinatsiooni ning kogemuste vahetamist;

- algatada, täiendada ja toetada rahvusvahelisi projekte, mis vastavad komisjoni poliitikale selles valdkonnas, olla aktiivne Euroopa Kaitseagentuuri raames tehtavas kübervaldkonna arendus- ja uurimistöös.

OSCE

- tõstatada küberjulgeoleku ja -kaitse temaatika julgeolekuga tegelevates OSCE struktuurides (näit julgeolekualasel koostööfoorumil);
- kasutada OSCE Parlamentaarset Assambleed kübertemaatika tutvustamisel ja korraldada organisatsiooni raames temaatilisi seminare ning konverentse.

NATO

- rakendada NATO küberkaitsepoliitikat;
- kindlustada NATO Küberkaitse Kompetentsikeskuse loomine Eestis ning keskuse akrediteerimine NATO poolt;
- tihendada küberjulgeoleku ja -kaitse alast teaduskoostööd NATO Teadusuuringute ja Tehnoloogia Organisatsiooniga ning NATO Juhtimise, Konsultatsioonide ja Kommunikatsiooni Organisatsiooniga;
- luua NATO liikmesriikide vaheline kahe- ja mitmepoolne ning vajadusel ka NATO liikmesriikide ja partnerriikide vaheline vastav koostöö- ja teabevõrgustik.

OECD

- osaleda liitumiseelsel perioodil võimalikult aktiivselt info-, arvuti- ja sidepoliitika komitee ning selle alatöörühmade töös ning juhtida tähelepanu küberjulgeoleku ja -kaitse temaatikale;
- liitumisjärgselt algatada vastavalt vajadusele küberjulgeolekut ja -kaitset käsitlevaid arutelusid ning soovituste väljatöötamist.

4.5 Küberjulgeoleku alane teavitustegevus

Teavitustegevuse eesmärgid on:

- küberkeskkonnast pärinevate ohtude ning infoturbeteadlikkuse ja -taseme tõus kõigi arvutikasutajate hulgas;
- turvalise arvutikasutuse ja infoturbe põhitõdesid puudutavate teadmiste jõudmine võimalikult paljude sihtgruppideni ühiskonnas;

- Eesti küberjulgeoleku alaste seisukohtade tuntus nii riigisiseselt kui ka rahvusvahelisel tasandil ning koostöövõrgustike tõhus toimimine meedia toetusel.

Tegevused eesmärkide saavutamiseks:

- korraldada küberjulgeoleku tagamisel kogu ühiskonda hõlmavat teavitustööd koordineeritud koostöös erasektoriga. Põhilisteks sihtgruppideks on tavakasutajad, kesk- ja väikeettevõtted, kohalike omavalitsuste ja riigiasutuste töötajad, õpilased ja üliõpilased;
- küberjulgeoleku ning arvutikaitse alaste suunatud meediakampaaniate ning sotsiaalse reklaami programmide elluviimine;
- era- ja avaliku sektori koostööprojekti „Arvutikaitse 2009" eesmärkide ja tegevuste toetamine;
- küberkultuuri teadvustamine igas Eesti asutuses ja ettevõttes tippjuhtide ning keskastme juhtide koolitamise kaudu, et rõhutada Interneti ja arvuti turvalise kasutamise põhimõtteid kõikidel elualadel.
- Eesti küberjulgeoleku alaste seisukohtade ning kogemuste tutvustamine rahvusvahelisel tasandil

Vastutajad: Majandus- ja Kommunikatsiooniministeerium, Välisministeerium, Kaitseministeerium

5 Strateegia rakendamine ja rahastamine.

Kaitseministeeriumi juhitud komisjon koostöös Haridus- ja Teadusministeeriumi, Justiitsministeeriumi, Majandus- ja Kommunikatsiooniministeeriumi, Siseministeeriumi ja Välisministeeriumiga esitab “Küberjulgeoleku strateegia 2008–2013” Vabariigi Valitsusele kinnitamiseks. Strateegia elluviimiseks koostatakse rakendusplaan, mis seotakse valitsusasutuste poolt koostatavate organisatsioonipõhiste ja valdkondlike arengukavadega. Rakendusplaan 2008-2010 esitatakse Vabariigi Valitsusele kolme kuu jooksul alates strateegia kinnitamisest valitsuses.

Rakendusplaani koostamisel esitavad eri ametkonnad ning strateegia koostamiseks moodustatud töögrupid oma ettepanekud tegevusplaanide ja eelarveliste vahendite kohta strateegia erinevates valdkondades püstitatud eesmärkide saavutamiseks. Rakendusplaanid koostatakse kahes etapis: esimene aastateks 2008–2010, teine aastateks 2011–2013.

„Küberjulgeoleku strateegia rakendusplaani 2008–2010” koostamise eest vastutab Kaitseministeeriumi juhitud ametkondadevaheline komisjon koostöös Haridus- ja Teadusministeeriumi, Justiitsministeeriumi, Majandus- ja Kommunikatsiooniministeeriumi, Siseministeeriumi ja Välisministeeriumiga ning erasektori esindajatega.

Strateegia elluviimist ja tulemuslikkust hakkab hindama VV julgeolekukomisjoni alakomisjoni juurde moodustatav küberjulgeoleku nõukogu, mis koondab eri ametkondade esindajaid ning eksperte. Küberjulgeoleku nõukogu valvab strateegia eesmärkide elluviimise järele ning esitab iga-aastased aruanded strateegia täitmise ning rakendusplaanide eesmärkide saavutamise kohta Vabariigi Valitsusele. Küberjulgeoleku nõukogu koosseis, kooskäimise kord ning ülesanded sätestatakse strateegia rakendusplaanis.

5.1 Prognoositavad ressursid

Alates 1. jaanuarist 2008.a. rakendunud ISKE määrusega on kõigile Eesti riigi- ja kohalike omavalitsuste asutustele kohustuslik tagada oma infosüsteemide toimimiseks vajalik turvameetmete rakendamine ning selleks vajalikud summad on asutused oma IT turvapoliitika planeerimisel ette näinud. Allolev tabel ei kajasta seega asutuste infosüsteemide normaalseks toimimiseks ettenähtud ressursse, vaid strateegia eesmärkide elluviimiseks vajalikke lisaressursse. Osa lisaressurssidest kajastuvad juba ministeeriumide eelarveplaanides perioodil 2008-2013, kuid 132,8 miljonit EEK oleks vaja planeerida täiendava ressursina.

Meede		2008	2009	2010	2011	2012	2013	Kavan-datud sum-mad	Täien-dav sum-ma	kokku
Tegevusvaldkond 1: küberkaitse turvameetmete rakendamine										
Meede 1.1: kriitilise informatsiooni infrastruktuuri (KII) kaitse	planeeritud	12,5	23	5	5	3	3	51,5		**91,5**
	allikas	10 (ESF-MKM), 2,5 (MKM-RIA)	20 (ESF-MKM) 3 (MKM-RIA)	MKM-RIA	MKM	MKM	MKM			
	lisaraha			10	10	10	10		40	
Meede 1.2: turvameetmete süsteemi arendamine ja rakendamine	planeeritud	2,5	1	1	1	1	1	7,5		**17,5**
	allikas	MKM-RIA eelarve	MKM-RIA eelarve	MKM-RIA eelarve	MKM-RIA eelarve	MKM-RIA eelarve	MKM-RIA eelarve			
	lisaraha		2	2	2	2	2		10	
Tegevusvaldkond 2: infoturbe alase kompetentsi tõstmine										
Meede 2.1: küberjulgeolekuks vajalike uuringute ning arendustööde korraldamine	planeeritud	9	9	9	9	9	9	54		
	allikas	KaM eelarve	KaM eelarve	KaM eelarve	KaM eelarve	KaM eelarve	KaM eelarve			
	lisaraha		6	6	6	6	6		30	**84**
Meede 2.2: küberkaitse alase väljaõppe korraldamine	lisaraha		3	6,2	6,2	6,2	6,2		27,8	**27,8**
Meede 2.3: kriisisituatsioonides tegutsemise võimekuse arendamine nii era kui avalikus sektoris	planeeritud	2,5	2	2	2	2	2	12,5		**23,5**
	allikas	MKM-RIA eelarve	MKM-RIA eelarve	MKM-RIA eelarve	MKM-RIA eelarve	MKM-RIA eelarve	MKM-RIA eelarve			
	lisaraha		2	3	2	2	2		11	
Tegevusvaldkond 3: küberjulgeolekuks vajaliku õigusruumi kujundamine	lisaraha		1	1	1				3	**3**
Tegevusvaldkond 4: rahvusvahelise koostöö arendamine	planeeritud	2	2	2	2	2	2	12		**12**
	allikas	VM, KM	VM, KM	VM , KM	VM, KM	VM, KM	VM, KM			
Tegevusvaldkond 5: teavitustegevus	planeeritud	6	6	5	5	5	5	32		**43**
	allikas	ESF MKM RIA	ESF MKM RIA	ESF MKM RIA	ESF MKM RIA	ESF MKM RIA	ESF MKM RIA			
	lisaraha		5	2	2	1	1		11	
							Kokku:	**169,5**	**132,8**	**302,3**

LISA 1. EESTI KRIITILISE INFRASTRUKTUURI VALDKONNAD

- Energiarajatised ja -võrgud: elektrienergia, nafta ja gaasi hoidmine, ladustamisrajatised ja töötlemistehased, edastamis- ja jaotussüsteem.
- Side ja infotehnoloogia: telekommunikatsioon, edastus- ja teavitussüsteemid, tarkvara, riistvara ja võrgud, kaasa arvatud Interneti infrastruktuur
- Rahandus: pangandus, väärtpaberid ja investeeringud.
- Tervishoid: haiglad, tervishoiurajatised, laborid ja ravimid, otsingu-, pääste- ja kiirabiteenistused.
- Toit: ohutus, tootmisvahendid, hulgimüük ja toiduainetööstus.
- Vesi: veehoidlad, puhastusjaamad ja veevõrgud.
- Transport: lennujaamad, sadamad, ühendveorajatised, raudtee- ja massitransiidivõrgud, liikluse juhtimissüsteemid.
- Ohtlike kaupade tootmine, ladustamine ja transport: keemilised, bioloogilised, radioloogilised ja teised ohtlikud materjalid.
- Riigiasutused: kriitilised teenistused, rajatised, infovõrgud, riiklikku julgeolekut ja kaitsevõimet tagavad infosüsteemid, ressursid, andmekogud ja õiguslikku tähendust omavad kohturegistrid ning rahvuslikud kultuuriobjektid.

LISA 2. Mõisted, määratlused ja lühendid

Ajatempel - on digitaalne tõend, mis võimaldab objektiivselt kindlaks teha mingi digitaalse andmekogumi loomise aja.

Andmekaitse ehk **andmeturve** - meetmete rakendamine kaitsmaks andmeid nende volitamatu sihiliku või juhusliku avalikustamise, muutmise või hävitamise eest

Andmekogu – ühendtermin andmebaaside kohta, mis hõlmab riigi põhiregistrid, riiklikud registrid, kohalike omavalitsuste registrid, riigiasutuste ja kohalike omavalitsuste muud andmekogud ja ka avalik- ja eraõiguslike isikute poolt peetavad andmekogud.

Autentimine (identifitseerimine) – protseduur, mille käigus tehakse kindlaks teenuse kasutamist taotlev isik või infosüsteem.

Autoriseerimine – protseduur, mille käigus tehakse kindlaks teenust taotleva autenditud isiku või infosüsteemi õigus teenust kasutada. Kasutajainfo süsteem autoriseeritakse vastavalt selle kuuluvusele teatud kasutajagruppi.

Etalonturbe meetmed - katalogiseeritud ja valimismetoodikaga varustatud turvameetmed, mille hulgast tehtav valik sõltub turvaklassist ja andmeid töötleva infosüsteemi koostisest.

Infoallika autentsus – omadus, mis võimaldab infoallikat verifitseerida ja usaldada.

Informatsiooni infrastruktuur – andmed, protsessid, protseduurid, vahendid, rajatised ja tehnoloogia informatsiooni loomiseks, kasutamiseks, edastamiseks, säilitamiseks ja hävitamiseks.

Infosüsteem – andmeid töötlev, salvestav või edastav tehniline süsteem koos selle talituseks vajalike vahendite, ressursside ja protsessidega.

Infoturve – turvameetmete loomise, valimise ja rakendamise protsesside kogum. Infoturbe kolm komponenti on andmete käideldavus, terviklus ja konfidentsiaalsus.

- **Andmete käideldavus** - on eelnevalt kokkulepitud nõutaval tööajal kasutamiskõlblike andmete õigeaegne ja hõlbus kättesaadavus selleks volitatud tarbijaile (isikutele või tehnilistele vahenditele).
- **Andmete terviklus -** on andmete õigsuse, täielikkuse ja ajakohasuse tagatus ning päritolu autentsus ja volitamatute muutuste puudumine.
- **Andmete konfidentsiaalsus -** on andmete kättesaadavus ainult selleks volitatud tarbijaile (isikutele või tehnilistele süsteemidele) ning kättesaamatus kõigile ülejäänutele.

Infovara – varad, mille hulka kuuluvad andmed, andmebaasid, rakendustarkvara, süsteemitarkvara, arvutid, serverid, marsruuterid, kommutaatorid, andmekandjad jmt.

IP aadress – arvuti või muu võrku ühendatud seadme aadress, mida kasutatakse seadmete identifitseerimiseks ja sidepidamiseks IP ja muude protokollide poolt.

Koosvõime – infosüsteemide ja nende poolt toetatavate tegevusprotsesside võime vahetada andmeid ja ühiselt kasutada informatsiooni ning teadmisi.

Koosvõime raamistik – infosüsteemide tegevust puudutavate standardite ja juhendite kogum, mida organisatsioonid järgivad üksteisega suhtlemisel.

Kriitiline infrastruktuur – varad, teenused ja süsteemid või nende osad ja süsteemide vahelised ühendused, mille hävitamine, kahjustamine või hõivamine võib ohustada inimeste elu või tervist või tuua kaasa vara, teenuse, süsteemi või nende osade hävimise või ulatusliku majandusliku kahju ning põhjustada ühiskonna turvatunde vähenemist, vähendada riigi usaldusväärsust, kahjustada riigi mainet ja halvata riigi toimimist.

Kriitiline informatsiooni infrastruktuur – informatsiooni infrastruktuuri komponendid, mis on kas ise kriitilised või mis on hädavajalikud kriitilise infrastruktuuri toimimiseks.

Kriitilise informatsiooni infrastruktuurid hõlmavad paljusid majandussektoreid, kaasa arvatud pangandus ja rahandus, transport, energia, kommunaalmajandus, tervishoid, toiduga varustamine ja side, aga ka valitsuse võtmeteenistusi. Mõned kriitilised elemendid nendes sektorites pole rangelt võttes infrastruktuur, vaid on võrgud või tarneahelad, mis toetavad elutähtsate toodete või teenuste jaotust. Näiteks sõltub toidu- või veevarustus meie suuremates linnastunud piirkondades teatud võtmerajatistest, kuid samuti tootjate, töötlejate, turustajate ja jaemüüjate komplekssest võrgust.

Küberjulgeolek (riigi küberjulgeolek) – antud strateegia kontekstis hõlmab mõiste *küberjulgeolek* kõiki elektroonilise teabe, teabekandjate ning -teenustega seotud toiminguid, mis mõjutavad riigi julgeolekut. Riigi küberruumi julgeoleku tagamine koosneb mitmesugustest tegevustest eri tasanditel. Peamine eesmärk on vähendada küberruumi haavatavust, st ennetada küberrünnakuid ning taastada rünnakute korral võimalikult kiiresti infosüsteemide toimimine. Küberjulgeoleku tagamiseks on oluline hinnata riigi kriitilise infoinfrastruktuuri haavatavust, panna paika vastumeetmete süsteem küberrünnakute ärahoidmiseks, määratleda ametkondadevaheline koostöö riigis ning tööjaotus era- ja avaliku sektori vahel küberrünnakute tõrjumisel, arendada rahvusvahelist seadusandlust ja institutsionaalset koostööd, teavitada avalikkust ning töötada välja küberjulgeoleku alased koolitusprogrammid.

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

Küberkaitse hõlmab erinevaid tegevusi:

- kriitilise infrastruktuuri infoturve: peamiselt infoturbestandardite kehtestamine ning nende rakendamise koordineerimine;
- riigi poliitiliste, sotsiaalsete ja majanduslike protsesside toimimiseks vajalike infosüsteemide talituspidevuse tagamine;
- kriitilise infrastruktuuri infosüsteemide turvalist toimimist toetav õiguslik regulatsioon.

Küberkuritegevus - majandusliku kasu saamise eesmärgil toime pandud järgmised kuriteod:

1) arvutisüsteemi vastu suunatud kuriteod (häkkimine, näotustamine);

2) arvutisüsteemi vahendusel toime pandud kuriteod (arvutikelmus, identiteedivargus, Interneti vahendusel vaenu õhutamine jne);

3) autoriõiguste vastu suunatud kuriteod.

Küberruum – arvutitel ja arvutisüsteemidel põhinev digitaalne ruum, mis toetab tänapäevase infoühiskonna toimimist ja koosneb peamiselt Interneti poolt võimaldatud tegevuskeskkondadest ja igapäevaste toimingute lihtsustamiseks loodud digitaalsetest andmekogudest.

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).

Küberrünnete klassifikatsioon rünnete eesmärkide alusel:

- administreerimine ja eetiline häkkimine – andmeturbe toimimiseks hädavajalik tegevus oma info- ja kommunikatsioonivõrkude töövõimelisuse tagamiseks ja testimiseks;

- häktivism – arvutisüsteemide kasutamine propagandaks ja protestiks, teostajaks on häkkerist aktivist;

- küberkuritegevus – eri raskusastmetega kriminaalne tegevus, mille põhieesmärk on majanduslik kasu;

- küberterrorism – arvutite või teiste kommunikatsioonivõrgustike abil toime pandud küberrünne, mille eesmärgiks on tekitada kaost või hävingut ning destabiliseerida ühiskonda teatud poliitiliste eesmärkide saavutamiseks;

- **kübersõda** – riiklikul tasemel toime pandud küberkuritegevus või küberterrorism, mille põhieesmärgiks on ülemvõimu saavutamine purustusi vältides, erijuhtudel ka inimkaotused.

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.

Riskianalüüs - riskianalüüsi abil uuritakse, kui tõenäoline on mingite probleemide tekkimine ja millised oleksid nende probleemide tagajärjed.

Salgamise vääramine - kontseptsioon, mille kohaselt ei saa osapool lükata tagasi teatud toimingu tegemist (näiteks dokumendile digiallkirja andmist).

Nimeserver – server, mis säilitab informatsiooni domeeninimede ja neile vastavate IP aadresside kohta**.**

Nuhkvara - tarkvara, mis paigaldatakse arvutisse ilma selle kasutaja teadmata ning on mõeldud tema tegevuste ja isikuandmete jälgimiseks ning arvuti kontrollimiseks.

Turvapoliitika - turvapoliitika on firma või riigiasutuse ametlik dokument, millesse pannakse kirja kõik kaitse eesmärgid ja üldised turvameetmed. Üksikasjalikud turvameetmed kirjeldatakse mahukamas turvakontseptsioonis.

Viirus ehk **arvutiviirus** - programm, mis pärast käivitamist kahjustab peaaegu alati nii arvutit kui ka arvutisse installeeritud tarkvara.

X-tee – universaalne turvaline andmevahetuskeskkond tagamaks riigi kodanikele andmebaaside kasutamise nende volituste piires.

Lühendid:

CERT – (*Computer Emergency Response Team)* – infoturbe intsidentide käsitlemise keskus

DNS - *(Domain Name Server)* Interneti-arvutite nimeserverid

ISP - (*internet service providers*) Internetiteenuse pakkujad

KI – kriitiline infrastruktuur

IKT – info-ja kommunikatsioonitehnoloogia

ISKE – infosüsteemide kolmeastmeline etalonturbe süsteem

IP – (Internet Protocol) interneti protokoll

IT – infotehnoloogia

SCADA – (*Supervisory Control and Data Acquisition)* rahvusvaheliselt käibel olev lühend tööstuses, transpordis, energia- ja veemajanduses ning teistes majandussektorites kasutatavate automatiseeritud juhtimissüsteemide kohta

RF EMI – (*radio frequency electro-magnetic impulse)* raadiolainete sagedusel töötav elektromagnetiline häiritus