Riigikogu riigikaitsekomisjoni istungi protokoll nr 178

Tallinn, Toompea Esmaspäev, 17. november 2025

Algus 11.10, lõpp 12.08

Juhataja: Kalev Stoicescu (esimees)
Protokollija: Irene Kiil (konsultant)
Võtsid osa:
Komisjoni liikmed: Vladimir Arhipov, Enn Eesmaa, Raimond Kaljulaid, Meelis Kiili, Leo Kunnas, Alar Laneman, Priit Sibul, Peeter Tali
Komisjoni ametnikud: Aivar Engel (nõunik-sekretariaadijuhataja), Külli Jõgeda (nõunik)
Puudusid: Anti Poolamets, Mati Raidma ja Kristo Enn Vaga
Kutsutud: Justiits- ja Digiministeeriumi riikliku küberturvalisuse talituse juhataja Taavi Viilukas, küberturvalisuse õigusnõunikud Guido Pääsuke ja Raavo Palu (3. päevakorrapunkt)

Päevakord:
1. Nädala töökava kinnitamine
2. Vabariigi Valitsuse algatatud kaitseväeteenistuse seaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu (664 SE) kolmanda lugemise ettevalmistamine
3. Vabariigi Valitsuse algatatud küberturvalisuse seaduse ja teiste seaduste muutmise seaduse (küberturvalisuse 2. direktiivi ülevõtmine) eelnõu (739 SE) teise lugemise ettevalmistamine
4. Info ja muud küsimused

1. Nädala töökava kinnitamine
Riigikogu riigikaitsekomisjoni nädala (17.11.2025-23.11.2025) töökava

Komisjoni istung esmaspäev, 17.11.2025 kell 11.10
1. Nädala töökava kinnitamine
2. Vabariigi Valitsuse algatatud kaitseväeteenistuse seaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu (664 SE) kolmanda lugemise ettevalmistamine
3. Vabariigi Valitsuse algatatud küberturvalisuse seaduse ja teiste seaduste muutmise seaduse (küberturvalisuse 2. direktiivi ülevõtmine) eelnõu (739 SE) teise lugemise ettevalmistamine
4. Info ja muud küsimused

Komisjoni istung teisipäev, 18.11.2025 kell 14.00
1. Ülevaade Kaitseliidu tegevusest

Riigikaitsekomisjoni ja julgeolekuasutuste järelevalve erikomisjoni ühine väljasõiduistung
neljapäev, 20.11.2025 kell 14.15
1. Strateegilise ohuhinnangu tutvustamine

Otsustati:
1.1. Kinnitada nädala töökava (konsensus: Vladimir Arhipov, Enn Eesmaa, Raimond Kaljulaid, Meelis Kiili, Leo Kunnas, Alar Laneman, Priit Sibul, Kalev Stoicescu, Peeter Tali).

2. Vabariigi Valitsuse algatatud kaitseväeteenistuse seaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu (664 SE) kolmanda lugemise ettevalmistamine
Kalev Stoicescu ütles, et eelnõu kolmanda lugemise teksti on tehtud kolm keelelist täpsustust, millega on nõus ka eelnõu algataja esindajad.

Otsustati:
2.1. Kiita heaks eelnõu kolmanda lugemise tekst (konsensus: Vladimir Arhipov, Enn Eesmaa, Raimond Kaljulaid, Meelis Kiili, Leo Kunnas, Alar Laneman, Priit Sibul, Kalev Stoicescu, Peeter Tali).

3. Vabariigi Valitsuse algatatud küberturvalisuse seaduse ja teiste seaduste muutmise seaduse (küberturvalisuse 2. direktiivi ülevõtmine) eelnõu (739 SE) teise lugemise ettevalmistamine
Jätkati k.a 10. novembri istungil toimunud arutelu.

Kalev Stoicescu küsis Justiits- ja Digiministeeriumi esindajatelt, et kas nad vahepeal Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu esindajatega (ITL) kohtunud ning mis tulemuseni jõuti.

Taavi Viilukas ütles, et kolmapäeval toimunud kohtumine keskendus ITLi ettepanekutele. Vaadati läbi kõik ettepanekud, millest viie ettepanekuga arvestati. T. Viilukase sõnul lepiti kokku jätkukohtumine, sest on ettepanekuid, mida ei saa aktsepteerida ning ettepanekuid, millega jätkatakse tööd või mille käsitlemine lükatakse tulevikku. Küberintsidendi mõiste sisustamise osas oldi ITLiga ühel meelel, et seda ei ole võimalik kiiresti lahendada.

Guido Pääsukese sõnul arutati ITLiga kohtumisel järelevalvega seotud mõisteid. Kolme mõiste puhul arvestati ITLi ettepanekutega sisuliselt. Mõistet „järelkontroll“ saab arvestada, seda tehakse üldjuhul olulistele üksustele. „Eelkontrolli“ ei defineerita, kuna nii eel- kui järelkontroll on üks kontrolliosa ning „sihipärane turvaaudit“ võiks olla defineeritud. Tegemist on võrgu- ja infosüsteemi andmetoimikute sõltumatu läbivaatusega.

Kalev Stoicescu küsis, et kas ITL oli nõus sellega.

Guido Pääsuke vastas, et ITLi ettepanek oli sõnastada küll „sihipärane turvaaudit“, aga nad ei olnud 100% nõus sõnastuse ettepanekuga. „Turvalisuse kontrolli“ osas oli ettepanek see seadusesse tuua, kuid ITL soovis seda näha teises versioonis. G. Pääsuke sõnas, et kuna NIS2 ehk küberturvalisuse teine direktiiv läheb organisatsioonipõhiseks, kajastada võimalust, et riske hinnataks teenusepõhiselt, nagu täna. Vabariigi Valitsuse määrusega saaks sätestada, et

terve organisatsioon ei peaks karme nõudeid rakendama, vaid võimalusel n-ö teenusepõhiselt. Seda varieerumist sai NIS2 sõnastuse kaudu lubada.

Raavo Palu selgitas, miks on eelnõus kasutatud sõnu „pisteline järelevalve“, mitte „pisteline kontroll“ (ITLi ettepanek p 3.2.) ning mis on sõnade „pisteline järelevalve“ olemus ja sisu. R. Palu ütles, et küberturvalisuse 2. direktiivi artikli 32 lg 2 punktid a ja c kasutavad sõnastusi „sealhulgas pistelisi kontrolle“ kui ka sätestavad *ad hoc* auditite kasutamist. Oluliste üksuste puhul on direktiivis punkti a osas sarnane sõnastus, kuid nende suhtes kehtivates nõuetest puuduvad sõnad „sealhulgas pistelisi kontrolle“ kui ka punkt c sisu tervikuna (vt artikli 33 lõiget 2, ennekõike selle punkti a). Seega on nende sõnastuste kasutamine vajalik ainult ülioluliste üksuste korral. Eelnõu § 1 punktiga 44 tekitatakse KüTS § 16^1 lõige 1^1, mille punktis 1 on kasutatud sõnastust „pisteline järelevalve“. Samu sõnu on kasutatud ka eelnõu § 1 punktiga 46 tekitatava KüTS § 17 lõike 1^1 punktis 1. Eelnõus on sõnadega „pisteline järelevalve“ hõlmatud direktiivi sõnastuse mõttes nii „pistelised kontrollid“ kui ka „*ad hoc* auditid“. Kui kasutada ainult sõna „pisteline kontroll“, siis ei pruugi olla koheselt selge, et see hõlmab ka *ad hoc* auditeid. Seetõttu on kasutatud eelnõus sõnastust „pisteline järelevalve“ nende kahe olukorra sisustamiseks. See siiski ei tähenda, et mõlemat meedet tuleb kindlasti kasutada, kui toimub pisteline järelevalve. R. Palu selgitas ka, miks on kasutatud sõnu „sihipärane turvaaudit“, mitte „korrapärane ja sihipärane turvaaudit“ (ITLi ettepanek p 3.2.). Sihipärase turvaauditi kui meetme kasutamise sätestavad kaks artiklit - küberturvalisuse 2. direktiivi artikli 32 lg 2 punkt b ja artikli 33 lg 2 punkt b. Nende kahe punkti erinevuseks on see, et ülioluliste üksuste suhtes tehakse „korrapäraseid ja sihipäraseid turvaauditeid“, kuid oluliste üksuste puhul „sihipäraseid turvaauditeid“. Eelnõud koostades analüüsiti ja hinnati, kas on vajadus tekitada identsed sõnastused ka eelnõuga, sh kui minna seda teed, siis mis on nende kahe sõnastuse vahe ja mis on neil ühist. Kui sõnu „korrapärased ja sihipärased turvaauditid“ grammatiliselt analüüsida, siis see võib tähendada, et on olemas „korrapärased turvaauditid“ kui ka „sihipärased turvaauditid“. Selline lähenemine võib tekitada veel rohkem segadust, et mis on nende kahe erinevus ja mis on neil ühist. Seetõttu otsustati eelnõu koostamisel selle kasuks, et kasutatakse eelnõu § 1 punktide 44 ja 46 sõnastustes „sihipärane turvaaudit“ tagamaks, et eelnõu tekst ja sisu oleks ühe sõnastuse ja mõttega. Direktiiv ei defineeri ega selgita, mida üldse tähendab „sihipärane turvaaudit“. Sel põhjusel on eelnõu üheks muudatusettepanekuks ka ettepanek tekitada „sihipärase turvaauditi“ definitsioon. Kuid kuidas võetakse üle sõna „korrapärane“, sh kuidas see kohaldub ainult ülioluliste üksuste korral? Eelnõu juures on määruste kavandite fail, milles on ministri määruse kavand nimega „Sihipärase turvaauditi korraldamise täpsemad tingimused ja kord“. Tolle määruse kehtestamise volitusnormideks on KüTS § 161 lõige 2 ja § 17 lõige 2. Selles määruses on sätestatud, et sihipärast turvaauditit võib teha üliolulise üksuse suhtes korrapäraselt. Ehk sõna „korrapärased“ võetakse üle ministri määrusega ega ole kuhugi „kadunud“.

Kalev Stoicescu küsis, et kas mujal seadusandluses ei ole analoogselt kontrolle või auditeid defineeritud. Kas erinevates valdkondades on terminid ühtlustatud?

Taavi Viilukas vastas, et Euroopa Liidu poolt on tulnud mõisted, mida ei ole ette ära defineeritud ning mida Euroopa Komisjon ise ei täpsusta. Dilemma on selles, et kas defineerida uusi mõisteid või mitte. Kui ise definitsioone luua, ei pruugi need ühtida Euroopa Komisjoni mõttega. Seega võiks hoiduda ülemäära jäikade definitsioonide kehtestamisest ning oodata Euroopa Komisjoni suuniseid. T. Viilukas lisas, et kohtumised olulise

koostööpartneri ITLiga jätkuvad, kuna arutamist vajavaid teemasid on rohkem.

Guido Pääsuke selgitas trahvide piirmääradega seonduvat.

Kalev Stoicescu märkis, et k.a 10. novembri istungil kohtus riigikaitsekomisjon kaasatutega, kus lepiti kokku jätkata arutelu. Ministeeriumi esindajad lubasid ITLiga nende ettepanekuid arutada, leida lahendusi ning pakkuda välja tänaseks istungiks juhtivkomisjoni muudatusettepanekute projektide sõnastusi. K. Stoicescu küsis, et kas saab minna muudatusettepanekute arutamise juurde või soovib ministeerium veel jätkata arutelu ITLiga. Tuleb arvestada, et eelnõu seadusena jõustumine on 2026. aasta 1. jaanuar ja direktiiv pidanuks olema Eesti õigusesse täies mahus üle võetud 2024. aasta oktoobris.

Raavo Palu sõnul võib liikuda muudatusettepanekute arutamise juurde, ITLiga jätkuvad arutelud paralleelselt edasi. Euroopa Liidust on tulemas uusi õigusakte, mida peab Eesti õiguses täpsustama.

Kalev Stoicescu sõnul on oluline arvestada kaasatute, eriti ITLi soovide ja arvamustega. Vajadusel saab täpsustada eelnõust tulenevaid rakendusakte ning pärast arutuse all oleva eelnõu seadusena jõustumist muuta küberturvalisuse seadust.

Vaadati läbi juhtivkomisjoni muudatusettepanekud:

1. Täiendada eelnõu § 1 punktiga 6 muudetavat §-i 2 uue punktiga 14 ja muuta järgnevat numeratsiooni vastavalt:

„14) järelkontroll – järelevalve, mis on seotud küberintsidendile tagantjärele reageerimisega või küberintsidendi tekkimise vahetule ohule täiendava kontrolliga, lähtudes tõenditest, vihjetest või teabest, millega on juhitud järelevalveasutuse tähelepanu küberintsidendile või selle vahetu tekkimise ohule, avalikult kättesaadavast teabest, või teabest, mis on saadud või loodud järelevalveasutuse muu ülesande täitmisel;“.

Selgitus**:** *infotehnoloogia valdkonnas tegutsevaid ettevõtjaid koondav esindusorganisatsioon Eesti Infotehnoloogia ja Telekommunikatsiooni Liit (edaspidi ITL) on Riigikogu riigikaitsekomisjonile saatnud seaduseelnõu 739 SE menetluse raames kirja, milles muuhulgas juhitakse komisjoni tähelepanu, et järelevalvega setud mõistete osas puudub selgus. Mõistete reaalne sisustamine ja ühene arusaam on ITL sõnul vajalik nii järelevalveasutusele kui ka neile, kelle üle järelevalvet teostatakse. Eelnõu subjektidel peab olema võimalik eelnõust aru saada, millised õigused on Riigi Infosüsteemi Ametil (edaspidi RIA) ja millised subjektil. Riigikaitsekomisjon palus 10.11.2025 toimunud avalikul koosolekul eelnõu algataja esindajal Justiits- ja Digiministeeriumil (edaspidi JDM) kujundada tõstatatud küsimuses oma seisukoht ning võimalusel leida ka kokkulepe märkuse esitanud ITL-iga.*

Küberturvalisuse 2. direktiiv eristab üliolulise üksuse ja olulise üksuse järelevalve korraldust. Olulise üksuse suhtes tehakse ennekõike järelkontrolli. Seetõttu on vajadus ka defineerida selle järelevalve korralduse olemust.
Järelevalve korralduse hõlmab nii korrakaitseseaduse alusel toimuvat riiklikku järelevalve menetlust kui ka Vabariigi Valitsuse seaduse alusel toimuvat haldusjärelevalve menetlust. Mõlemat liiki menetluse puhul kohalduvad ka üldised haldusmenetluse nõuded ja põhimõtted, mis on sätestatud haldusmenetluse seaduses.
Tagantjärele reageerimine lähtub vähemalt ühest järgmisest märgist (lähtudes küberturvalisuse 2. direktiivi põhjendusest 122):

1) tõendid, vihjed või teave, millele on juhitud järelevalveasutuse tähelepanu (näiteks märgukiri, kaebus, mõne teise ametiasutuse edastatud teade või olulise mõjuga küberintsidendi korral esitatud esmane teade või intsidenditeade);
2) avalikult kättesaadav teave (näiteks üksuses on toimunud küberintsident, millest pole järelevalveasutust teavitatud, kuid üksus on otsustanud teavitada avalikkust);
3) teave, mis on saadud või loodud järelevalveasutuse muu ülesande täitmisel (näiteks Eesti internetiaadresside ruumis olevate ning Eesti maatunnusega seotud domeenide vaatluse käigus; tegemist on olukorraga, kus kontrollitakse, kas üksus on lõpetanud varem tuvastatud rikkumised ja viinud tegevuse vastavusse kehtivate nõuetega ehk tagatakse, et järelevalve käigus seatud kohustused ja tingimused on täidetud).
Järelkontrolli käigus võidakse kasutada näiteks selliseid järelevalvemeetmeid nagu: sihipärane turvaaudit (üliolulise üksuse ja olulise üksuse korral) ja turvalisuse kontrolli (üliolulise üksuse ja olulise üksuse korral).

Riigikaitsekomisjon
Juhtivkomisjon: ARVESTADA TÄIELIKULT (konsensus: Vladimir Arhipov, Enn Eesmaa, Raimond Kaljulaid, Meelis Kiili, Leo Kunnas, Priit Sibul, Kalev Stoicescu, Peeter Tali).

2. Täiendada eelnõu § 1 punktiga 6 muudetavat §-i 2 uue punktiga 25 (uue numeratsiooni järgi punktiga 26) ja muuta järgnevat numeratsiooni vastavalt:

„26) sihipärane turvaaudit – võrgu- ja infosüsteemi andmike ja toimingute sõltumatu läbivaatus ning uurimine, et kontrollida võrgu- ja infosüsteemi turvameetmete adekvaatsust, vastavust kehtivale infoturvapoliitikale ja tööprotseduuridele, avastada turvarikkeid ning soovitada võimalikke järelduvaid meetme-, poliitika- ja protseduurimuudatusi;“ .

Selgitus: *küberturvalisuse 2 direktiivi artikli 32 lõike 2 punkt b sätestab: „Liikmesriigid tagavad, et pädevatel asutustel on elutähtsate üksustega seotud järelevalveülesannete täitmisel nende üksuste suhtes vähemalt järgmised õigused: b) teha korrapäraseid ja sihipäraseid turvaauditeid, mida teeb sõltumatu organ või pädev asutusi“. Küberturvalisuse 2. direktiivi artikli 33 lõike 2 punkt b sätestab: „Liikmesriigid tagavad, et pädevatel asutustel on oluliste üksustega seotud järelevalveülesannete täitmisel kõnealuste üksuste suhtes vähemalt järgmised õigused: b) teha sihipäraseid turvaauditeid, mida teeb sõltumatu organ või pädev asutus“. Paraku ei selgita küberturvalisuse 2. direktiiv, mida peetakse silmas sihipärase turvaauditi all, mistõttu defineeritakse see termin eelnõus.*
Turvaaudit (ingl security audit) ja turvalisuse kontroll (ingl security scan) on sisult erinevad tegevused. Näiteks on AKITis turvaaudit määratletud rahvusvaheliste standardite ISO 7498 ja ISO/IEC 2382 kohaselt kui „süsteemi andmike ja toimingute sõltumatu läbivaatus ja uurimine süsteemi turvameetmete adekvaatsuse kontrolliks, kehtivatele poliitika[te]le ja tööprotseduuridele vastavuseks, turvarikete avastamiseks ning võimalike järelduvate meetme-, poliitika- ja protseduurimuudatuste soovitamiseks“. Turvarike on lahknevus kehtivast turvapoliitikast.
Sihipärast turvaauditit tehakse näiteks siis, kui järelevalveasutuse või auditeeritud organisatsiooni koostatud riskianalüüsi või muu asjakohase teabe põhjal on tekkinud vajadus auditit teha.
Seoses sihipärase turvaauditi tegemisega on oluline selgitada ka seda, et turvaauditit tellides ei delegeerita avalik-õigusliku ülesannet. Turvaaudit on välise isiku (IT-audiitori) poolne auditeeritava üksuse küberturvalisuse meetmete hindamine. RIA tellib selle hindamise audiitorilt, kuid tema antav hinnang ei ole ametile siduv. RIA kasutab seda hinnangut enda edasises järelevalvemenetluses ja otsustab selle põhjal nt ettekirjutuse tegemise vajalikkuse üle, kuid järelevalve tegemise õigus avalikku ülesannet täites jääb siiski talle kui pädevale asutusele. Seega avaliku ülesande delegeerimist välisele isikule ei toimu. Seetõttu ei sõlmita IT-audiitoritega ka halduslepingut, vaid need audiitorid, kelle teenuseid hakkab RIA tulevikus kasutama, leitakse riigihanke teel ning nendega sõlmitakse eraõiguslikud teenuse osutamise lepingud.

Samas ei ole sihipärase turvaauditi puhul mõeldud ainult turvahaavatavuse tuvastamist (vrd küberturvalisuse 2. direktiivi artikli 11 lõike 3 punktiga e), vaid laiemat kontrolli, tuvastamaks järelevalvemenetluse raames, kas küberturvalisuse seaduses (edaspidi KüTS) sätestatud, selle alusel või küberturvalisuse 2. direktiivi artikli 21 lõike 5 või artikli 23 lõike 11 alusel kehtestatud nõudeid on rikutud.
Küberturvalisuse 2. direktiiv näeb ette, et ainult sihipärase turvaauditi kulud jäävad üldjuhul järelevalvatava üksuse kanda, kui selle teeb sõltumatu organisatsioon (vt direktiivi artikli 32 lõike 2 kolmanda lõigu teist lauset ning artikli 33 lõike 2 kolmanda lõigu teist lauset). Sellega seotud sätete kohta vt eelnõukohase KüTS § 16 lg 1^1 p 2 ja lg 1^2 kui ka § 17 lg 1^1 p 2 ja lg 1^2, sh ka nende sätete alusel ette nähtud määruse kavandit.

Riigikaitsekomisjon
Juhtivkomisjon: ARVESTADA TÄIELIKULT (konsensus: Vladimir Arhipov, Enn Eesmaa, Raimond Kaljulaid, Meelis Kiili, Leo Kunnas, Priit Sibul, Kalev Stoicescu, Peeter Tali).

3. Täiendada **e**elnõu § 1 punktiga 6 muudetavat §-i 2 uue punktiga 30 (uue numeratsiooni järgi punktiga 32) ja muuta järgnevat numeratsiooni vastavalt:

„32) turvalisuse kontroll – võrgu- ja infosüsteemi tehniline ning korralduslik uurimine, et tuvastada võrgu- ja infosüsteemi turvahaavatavust või võrgu- ja infosüsteemi turvameetmete nõuetele mittevastavust.;“;

Selgitus: *küberturvalisuse 2. direktiivi artikli 32 lõike 2 punkt d näeb ette: „Liikmesriigid tagavad, et pädevatel asutustel on elutähtsate üksustega seotud järelevalveülesannete täitmisel nende üksuste suhtes vähemalt järgmised õigused: d) teha vajaduse korral koostöös asjaomase üksusega objektiivsetel, mittediskrimineerivatel, õiglastel ja läbipaistvatel riskihindamise kriteeriumidel põhinevaid turvalisuse kontrolle“. Küberturvalisuse 2. direktiivi artikli 33 lõike 2 punkt c näeb ette: „Liikmesriigid tagavad, et pädevatel asutustel on oluliste üksustega seotud järelevalveülesannete täitmisel kõnealuste üksuste suhtes vähemalt järgmised õigused: c) teha vajaduse korral koostöös asjaomase üksusega objektiivsetel, mittediskrimineerivatel, õiglastel ja läbipaistvatel riskihindamise kriteeriumidel põhinevaid turvalisuse kontrolle“. Paraku ei selgita küberturvalisuse 2. direktiiv täiendavalt, mida peetakse turvalisuse kontrolliks, mistõttu defineeritakse selle sisu.*
Turvalisuse kontroll (ingl security scan) erineb oma tähenduse ja sisu poolest sihipärasest turvaauditist ehk esimese puhul tehtava toiminguga ei minda kontrollimisega sügavuti (nt ei kontrollita infosüsteemi lähtekoodi tasandil). Näiteks testitakse turvalisuse kontrolliga turvahaavatusi ning sellega ei üritata saada ebaseaduslikul viisil juurdepääsu võrgu- ja infosüsteemi, vaid tuvastada süsteemiga seotud nõrkusi ja muid turvahaavatavusi. Turvalisuse kontrolliks kasutatakse erinevaid automatiseeritud tarkvarasid, mis teostavad korduvaid rutiinseid teste ja kontrolle.
Samas ei ole turvalisuse kontrolli puhul mõeldud ainult turvahaavatavuse tuvastamist (võrdle küberturvalisuse 2. direktiivi artikli 11 lõike 3 punktiga e), vaid laiemat kontrolli, tuvastamaks järelevalvemenetluse raames, kas küberturvalisuse seaduses sätestatud, selle alusel või küberturvalisuse 2. direktiivi artikli 21 lõike 5 või artikli 23 lõike 11 alusel kehtestatud nõudeid on rikutud.

Riigikaitsekomisjon
Juhtivkomisjon: ARVESTADA TÄIELIKULT (konsensus: Vladimir Arhipov, Enn Eesmaa, Raimond Kaljulaid, Meelis Kiili, Leo Kunnas, Priit Sibul, Kalev Stoicescu, Peeter Tali).

4. Muuta eelnõu § 1 punktiga 16 §-i 7 täiendavat lõiget 6 ja sõnastada see järgmiselt (muudatus alla joonitud):

„(6) Käesoleva paragrahvi lõike 5 alusel kehtestatud määruses võib täpsustada alalisi

asjakohaseid ja proportsionaalseid tehnilisi, tegevuslikke ja korralduslikke turvameetmeid ning rakendamise nõudeid ja tingimusi, sealhulgas võib võtta arvesse käesoleva seaduse § 3 lõigetes 2-5 nimetatud tegevusalasid.“.

Selgitus: *ITL on teinud 739 SE menetluse käigus ettepaneku „lähtuda nõuete rakendamisel ka küberturvalisuse 2. direktiivis rõhutatud riskipõhisusest ehk võimaldada subjektidel määratleda, kus ja millised on tema organisatsioonis olulisemad riskid ja võtta kasutusele vastavad meetmed“ ITL leiab, et „selle täienduse lisamine on vajalik, et siduda nendes sätetes toodud kohustused ehk KüTS-i alusel kehtestatud turvameetmed ettevõtete ja asutuste konkreetsete teenustega, mille osutamise tõttu nad on KüTS-i mõistes üliolulised või olulised üksused. Sellega jäetakse ettevõtetele ja asutustele õigus ise hinnata, mis on nende vaatest kriitiline ja lähtuda tehtud riskihinnangutest“.*
JDM toetab esitatud ettepaneku mõtet. Vabariigi Valitsuse eelnõus on ettenähtud valitsusele volitusnorm võrgu ja infosüsteemi küberturvalisuse nõuete kehtestamisel täpsustada alalisi asjakohaseid ja proportsionaalseid tehnilisi, tegevuslikke ja korralduslikke turvameetmeid ning rakendamise nõudeid ja tingimusi. Tagamaks selgust, et Vabariigi Valitsusel on õigus nende nõuete kehtestamisel arvesse võtta ka tegevusalasid, mille osutamise tulemusel tekib ettevõtjal küberturvalisuse nõuete järgimise kohustus, täiendatakse volitusnormi. Täienduse kohaselt võib Vabariigi Valitsus arvestada KüTS § 3 lõigetes 2-5 sätestatut. Nimetatud lõigetes on loetletud tegevusalad, millel tegutsev ettevõtja loetakse üliolulisteks või oluliseks üksuseks. Muudatus katab ka neid toiduvaldkonnaga seotud täpsustusi, mida tehakse KüTS § 7 lõike 8 alusel antava määrusega. Seega muudatus võimaldab Vabariigi Valitsusel ette näha paindlikust organisatsioonidele turvameetmete rakendamisel.

Riigikaitsekomisjon
Juhtivkomisjon: ARVESTADA TÄIELIKULT (konsensus: Vladimir Arhipov, Enn Eesmaa, Raimond Kaljulaid, Meelis Kiili, Leo Kunnas, Priit Sibul, Kalev Stoicescu, Peeter Tali).

5. Muuta eelnõu § 1 punktiga 42 §-i 14 lisatava lõiget 6 ning sõnastada see järgmiselt (muudatus alla joonitud):

„(6) Riigi Infosüsteemi Amet:
1) võib järelevalve tegemisel prioriseerida käesolevas seaduses sätestatud ülesannete täitmist, arvestades riski- või ohuprognoosipõhist lähenemisviisi;
2) teeb üliolulise üksuse suhtes riiklikku ja haldusjärelevalvet;
3) teeb olulise üksuse suhtes riiklikku ja haldusjärelevalvet järelkontrollina, kui järelevalveasutusel on alust arvata, et oluline üksus ei järgi käesolevas seaduses ning ennekõike käesoleva seaduse §-des 7 ja 8 sätestatud nõudeid.“

Selgitus: *Muudatusega vähendatakse erinevate terminite kasutamist ja seetõttu muutub seaduse rakendamine ka selgemaks üksustele kui ka selle sätte rakendajale. Üliolulise üksuse suhtes tehakse ennekõike eel- ja järelkontrolli, kuid olulise üksuse suhtes ennekõike järelkontrolli. Muudatusettepanekus 1 on esitatud selgitused järelkontrolli kohta, kuid koos eelkontrolliga moodustab järelkontroll riikliku ja haldusjärelevalve tavapärase üldise korralduse, mida on võimalik eelnõu tulemusena kasutada ainult üliolulise üksuste suhtes. Seetõttu puudub vajadus eraldiseisvalt defineerida eelkontrolli sisu eelnõuga, sh ka seda eelnõus eraldi välja tuua. Eelkontroll on näiteks järelevalvetoiming või nende kogum, mis tehakse korrakaitseseaduse alusel enne küberintsidendi toimumist ehk tegemist on ennetava järelevalvega, mis on seotud ohu ennetamise ja ohukahtluse korral ohu väljaselgitamisega. Eelkontrolli käigus võidakse kasutada näiteks selliseid järelevalvemeetmeid nagu pisteline järelevalve ehk juhuaudit või pisteline kontroll (üliolulise üksuse puhul), sihipärane turvaaudit (üliolulise üksuse ja olulise üksuse puhul) ja turvalisuse kontroll (üliolulise üksuse ja olulise üksuse puhul). Muudatusega tehakse ka keelelisi parandusi sättes toodu selgemaks väljendamiseks.*

Riigikaitsekomisjon
Juhtivkomisjon: ARVESTADA TÄIELIKULT (konsensus: Vladimir Arhipov, Enn Eesmaa, Raimond Kaljulaid, Meelis Kiili, Leo Kunnas, Priit Sibul, Kalev Stoicescu, Peeter Tali).

Otsustati:
3.1. Teha ettepanek võtta eelnõu täiskogu päevakorda 03.12.2025 (konsensus: Vladimir Arhipov, Enn Eesmaa, Raimond Kaljulaid, Meelis Kiili, Leo Kunnas, Priit Sibul, Kalev Stoicescu, Peeter Tali).
3.2. Kui teine lugemine lõpetatakse, teha ettepanek võtta eelnõu täiskogu päevakorda ja viia läbi lõpphääletus 10.12.2025 14:00 (konsensus: Vladimir Arhipov, Enn Eesmaa, Raimond Kaljulaid, Meelis Kiili, Leo Kunnas, Priit Sibul, Kalev Stoicescu, Peeter Tali).

Priit Sibula hinnangul võiks ka riigikaitsekomisjon saada ülevaate sellest, kuhu jõutud on, pärast ministeeriumi ja ITLi omavahelisi kohtumisi, nt järgmise aasta märtsis-aprillis.

Kalev Stoicescu arvates on see mõistlik ettepanek.

Taavi Viilukas lubas täpsema kuupäeva edastada komisjonile käesoleva nädala jooksul.

4. Info ja muud küsimused
Arutati kodanike M.M ja H. P. komisjonile saadetud kirju ning Eesti Meremeeste Sõltumatu Ametiühingu saadetud märgukirja.

Raimond Kaljulaidi arvates võiks kaitsetööstuse fondi loomisega ja sellest raha eraldamisega seonduvalt kutsuda riigikaitsekomisjoni istungile valdkonna esindajana majandus- ja tööstusministri.

Meelis Kiili leidis, et kutsuda tuleks ka Kaitseministeeriumi esindaja, kellel on valdkonnaga kokkupuude.

Kalev Stoicescu ütles kokkuvõtvalt, et mõlema ministeeriumi valdkondade asekantslerid võiksid tulla riigikaitsekomisjoni istungile 2026. aasta jaanuaris.

Otsustati:
4.1. Vastata avaldajatele (konsensus: Vladimir Arhipov, Enn Eesmaa, Raimond Kaljulaid, Meelis Kiili, Leo Kunnas, Priit Sibul, Kalev Stoicescu, Peeter Tali).

(allkirjastatud digitaalselt)
Kalev Stoicescu
juhataja

(allkirjastatud digitaalselt)
Irene Kiil
protokollija