Riigisaladuse ja salastatud välisteabe töötlemise erisuste väljatöötamiskavatsus lähtuvalt riigi julgeolekut ähvardavast olukorrast

1. Lahendatav probleem

2022. aastal kardinaalselt muutunud julgeolekuolukorraga kohandumine nõuab Eesti riigilt riigikaitset puudutavate tegevuste veelgi paremat koordineerimist ning arendamist. Eesti julgeolek ja riigikaitse peab olema võimeline kohanema ning adresseerima akuutseid ohtusid igal ajal, laiapindselt ja kogu ühiskonda hõlmavalt ning seda toetav õigussüsteem peab olema piisavalt paindlik ja võimaldama vajalike tegevuste elluviimist kiires ajaraamis. Peame rahu ajal olema harjunud kasutama samu teabe kaitse lahendusi, mida kasutame sõja ajal.

Salastatud teabe töötlemise toimingud ning edastamise viisid ei ole riigi sõjaliseks kaitseks valmistumisel piisavalt kaasaegsed, et tagada kiire reageerimine tekkinud olukorrale ja teabe liikumine õigel ajal õigesse kohta, et tagada informatsiooniline üleolek.

Salastatud teabe töötlemist riigi tasandil reguleerivad riigisaladuse ja salastatud välisteabe seadus (RSVS), selle alusel kehtestatud Vabariigi Valitsuse 20.12.2007 määrus nr 262 „Riigisaladuse ja salastatud välisteabe kaitse kord“ (RSVKK), riikidevahelised salastatud teabe töötlemise lepingud[1] ning rahvusvaheliste organisatsioonide salastatud teabe kaitse regulatsioonid[2].

Riigisaladuse ja salastatud välisteabe (edaspidi koos *salastatud teave*) töötlemise regulatsioonid on erinevad võrreldes muu juurdepääsupiiranguga teabega, kuna sisaldavad riigi jaoks sellist tundlikku teavet, mille avalikuks tulek võib seada ohtu riigi julgeoleku ja seda kõige laiemas tähenduses. Salastatud teabe õiguslik regulatsioon on väga detailselt sätestatud. Regulatsiooni eesmärk on ära hoida kaitset vajava teabe avaldamine juurdepääsuõiguseta ja teadmisvajaduseta isikutele – rõhuasetus on ainult teabe salajasusel, mitte teabe käideldavusel ega terviklikkusel. Salastatud teabe valdkonna õigusaktid on koostatud ja kehtestatud juba rohkem kui 15 aastat tagasi ja need baseeruvad koostamise aja ohupildil ning tehnoloogial. Sellest tulenevalt on **salastatud teabe töötlemise reeglid pigem rahuaegsed, keskenduvad füüsilisest keskkonnast lähtuvatele ohtudele, ei näe ette võimalikke erisusi teabe töötlemisel erinevates süsteemides ja olukordades ega arvesta riskide juhtimisel põhineva kaitse põhimõttega.** Puuduvad paindlikud võimalused riigi sõjaliseks ettevalmistamiseks, et tagada riigi valmisolek ennetada (sh seda harjutada) ja tõrjuda riigi julgeolekut ähvardavat ohtu.

RSVS ja RSVKK kehtivad ühetaoliselt kõikides riigi eriõiguslikes kordades ning ei võimalda seetõttu kriisi eskaleerumisel salastatud teabe töötlemises erisusi.

Riigikaitseseaduse § 14 lg 3 p 3 ja § 18 lg 4 kohaselt võib Kaitseväe juhataja kõrgendatud kaitsevalmiduse ja sõjaseisukorra tingimustes, kuniks see takistab vahetult riigi sõjalist kaitsmist, küll jätta täitmata määruse (nt RSVKK), kuid RSVS-is sätestatu toodu on jätkuvalt kohustuslik täitmiseks.

RSVS-i eesmärk peaks olema kaitsta sellist teavet, mille loata avaldamine võib tekitada eri määral kahju Eesti riigi huvidele. Sealhulgas tuleb tagada, et ei oleks kitsendusi konkreetsete salastamise aluste näol ega ka nende piiritlemist (nt korrakaitse või välissuhtlemise huvidega).

[1] https://xn--vlisluureamet-bfb.ee/nsa/oigusaktid.html.
[2] https://xn--vlisluureamet-bfb.ee/nsa/regulatsioonid.html.

Seadus peaks olema piisavalt paindlik, st suunav, toetav ja võimaldav, aga määrates selged baastaseme piirid/turbemeetmed, et võimaldada reageerimist uutele oludele, ohtudele ja tehnoloogiatele. Seadus peab lisaks baastasemel normidele lähtuma riskijuhtimise kesksest kaitse põhimõttest, võimaldades teabe turvalist käitlemist. Andmekesksusel ja riskijuhtimisel põhinemine on olulised muudatused, mis vajavad toimimiseks nii teabe töötlejatelt (asutus, isik) kui ka selle töötlemise korraldamise ning järelevalvega seotud osapooltelt nn maailmavaate muutust.

Tulenevalt eeltoodust on vaja reguleerida ning kaasajastada teabe (sh salastatud teabe) töötlemise toimingud ja viisid, sh selle operatiivne edastamine (käideldavus), et tagada kiirem reageerimine tekkinud olukorrale. Vajaliku teabe (nt luureinfo) piisavalt kiire jõudmine otsustaja(te)ni on hädavajalik, et alustada toiminguid, mille kaudu saab riiki ähvardava ohu ära hoida või võimalikku tekkivat kahju vähendada või seda ennetada. Analoogselt vajavad kaitsepoliitikate kujundajad/otsustajad tehnoloogiliste ohtude eest kaitset pakkuvaid teabe kaitse terviklahendusi, millega tundlikku teavet kiiresti jagada nii riigisiseselt kui ka rahvusvaheliselt võtmeliitlastega.

Salastatud teabe kiire edastamise vajadus puudutab laiemalt kogu riigi julgeolekut ning kitsamalt salastatud teavet töötlevaid üksuseid. Antud väljatöötamiskavatsuses (VTK) vaadatakse võimalikke kitsaskohti (sõjalisest) riigikaitsest lähtuvalt, kuna riigikaitse valdkonnas tegutsevad erinevad koostööpartnerid (nt ettevõtted, ülikoolid) loovad riigisaladust *ainult* riigiasutuse jaoks. Selline koostööpartner saab selguse salastatuse taseme kohta riigiasutuse konkreetsest juhisest, tulgu see siis kas salastatud lepingu julgeolekulisast või asutuse riigisaladuse kaitse juhendist. Samas, ka teabe kaitsmise seisukohast ei tohiks kõik detailsed salastatuse alused olla avalikud, kuna **ka salastatuse taseme avalik väljanäitamine võib peegeldada riigi haavatavusi**.

Arvestades Ukrainas toimuvat relvastatud konflikti, mis on tõestanud vajadust edastada teavet väga kiirelt, Kaitseväe osalemist rahvusvahelistel sõjalistel operatsioonidel (RSO), kus liitlased kasutavad laiaulatuslikult parima elektroonilise teabeturbega kaitstud sideturbelahendusi füüsilise turbe vaatest paindlikult, ning üleüldist elektroonilise teabe ja uute tehnoloogiate kasutuselevõtu suurenevat mahtu, on hädavajalik, et salastatud teabe töötlemise nõuded on piisavalt paindlikud, mis tagavad teabe kiire (ja eelkõige küberohtude vaatest turvalise) kättesaadavuse institutsioonidele, kellel on seda teavet informatsioonilise üleoleku saavutamiseks vaja.

Riigi kaitseplaanide läbipõimumine NATO plaanidega ja riigi osalemine RSO-del toob välja vajaduse viia nõuded vastavusse teiste riikide ja organisatsioonidega. Lisaks teabe töötlemise samasusele peavad ühildatavad olema ka salastatud teabe töötlemise süsteemid. Sellest tulenevalt tuleb kaaluda lähenemist, et RSVS-is oleksid salastatuse tasemed defineeritud nii nagu Euroopa Liidu (EL) ja NATO julgeolekureeglites[3]. Kõik NATO teabe kaitse normid lähtuvad selgelt sõnastatud eesmärgist tagada teabe kaitsega informatsiooniline üleolek, st teave peab olema õigel ajal õiges kohas, samal ajal kui vastasele peab teabe käideldavuses tekitama võimalikult suured takistused. Teabe kaitse reeglid peavad lähtuma spetsiifilise asutuse/üksuse riskidest ja konkreetse kasutatava tehnoloogilise lahenduse omadustest võimaldades asukoha/üksuse põhist paindlikku teabe käitlemist ja kaitset. Lisaks teabe salajasusele tuleb

[3] TÄIESTI SALAJANE: teave ja materjal, mille loata avaldamine võib väga tõsiselt kahjustada Eesti Vabariigi olulisi huve; SALAJANE: teave ja materjal, mille loata avaldamine võib tõsiselt kahjustada Eesti Vabariigi olulisi huve; KONFIDENTSIAALNE: teave ja materjal, mille loata avaldamine võib kahjustada Eesti Vabariigi olulisi huve; PIIRATUD: teave ja materjal, mille loata avaldamine võib negatiivselt mõjutada Eesti Vabariigi olulisi huve.

samaväärselt arvestada nii teabe käideldavuse (õigel ajal õiges kohas/teave on olemas) kui ka terviklikkuse (teavet ei tohi moonutada) nõuete täitmisega.

Seoses Eestis viibivate liitlastega ning osalemisega RSO-del on Kaitseväel esinenud olukordi, kus arusaamad salastatud teabe töötlemisest on erinevad. See tekitab täiendava koordinatsiooni vajaduse, mis on omakorda ajakulu, mida kriitilistes olukordades, kus otsused tuleb vastu võtta hetkega, riik endale lubada ei saa. Kaitsevägi osaleb RSO-l *Inherent Resolve* alates 2023. aastast ning käesolevaks hetkeks ei ole erinevate osapooltega jõutud kokkuleppele turvaala loomise tingimustes ja vajaduses. Kaitsevägi küll lõpetab lähiajal suurema panustamise nimetatud RSO-l, kuid järgmisele RSO-le siirdumisel tõusetub antud kitsaskoht kindlasti uuesti.

Kuna riigisaladuse töötlemine on RSVS-is iga asutuse jaoks detailselt ning ühetaoliselt sätestatud ning võimalikke olukorrast ning asutusest lähtuvaid erisusi ei ole piisavalt ette nähtud, siis ilma riigis kehtivat regulatsiooni põhjalikult muutmata, ei ole võimalik teabe töötlemises erandeid teha. Jäik regulatsioon[4], olukorraspetsiifiliste riskidega mittearvestamine ning teabe salastamine lähtuvalt detailselt seaduses sõnastatud sättest võib tekitada olukorra, kus teabe salastamisel ei arvestata tegelike ohtudega ega kahjuliku mõjuga, mida teabe kompromiteerimine võib tekitada riigi julgeolekule. Jäikus võib tekitada olukorra, kus rahuajal on teave salastatud, aga kõrgendatud kaitsevalmiduse välja kuulutamisel ei pea olemasolev või loodav teave olema enam salastatud, kuna seda teavet võib olla vaja töödelda ka väljaspool (sh ajutist) turvaala, samas peab ligipääs teabele olema jätkuvalt ikkagi piiratud[5]. Samasugune oht valitseb ka vastupidisel juhul ehk rahuajal kehtivate nõrgemate meetmete tõttu juba tõenäoliselt kompromiteeritud teabe salastamine kriisi- või sõjaolukorras on minetanud oma eesmärgi teabe kaitse tagamisel. Tänane paindumatu ning ühetaoline seadusandlus on tekitanud olukorra, kus teabe õigeaegse/kiire kohalejõudmise nimel kaldutakse pigem teavet alasalastama – tundlik teave märgistatakse „asutusesiseseks kasutamiseks“, kuna sisuliselt ei ole võimalik käideldavuse huvides täita seadusandluses kehtestatud jäikasid füüsilise kaitse norme.

Olukord, kus riigisaladuse töötlemise nõuded ja salastamise aluste sõnastused on täpselt ette antud, viib selleni, kus nt teatud meetodeid ja taktikaid harjutav Kaitseväe üksus võib seada ohtu riigisaladuse salajasuse[6]. Kehtiva regulatsiooni üldise põhimõtte kohaselt tuleb riigisaladust töödelda üldjuhul turvaalal, kuid **teabe kogumiseks kasutatavaid meetodeid ja taktikaid ei saa alati praktiseerida üksnes turvaalal**. Samuti tuleb uute sõjaliste võimearenduste juures arvestada riigisaladust sisaldava süsteemi komponendiga süsteemi sees, mida ei ole võimalik hoiustada ega käidelda turvaalal. Analoogselt tekib rahvusvaheliste kaitsepoliitikate kujundamisel EL-is ja NATO-s olukord, kus piiratud tasemel kaitset vajavat riigisaladust (Eesti riigi seisukohad EL ja NATO poliitika kujundamisel, mida organisatsioonid käsitlevad, nt piiratud tasemel teabena) ei ole jäiga seaduse oludes muudmoodi võimalik kaitsta, kui nimetada see ümber EL või NATO salastatud teabeks. **Ajutise turvaala loomine väga suure ala ulatuses (nt harjutusväljak, linn, veekogu) ei ole aga realistlik.**

Tulenevalt tehnoloogia hüppelisest arengust ja sellega kaasnevatest uutest ohtudest nenditi juba 2021. aastal koostatud Riigikaitse arengukavas (RKAK) aastateks 2022-2031, et infotehnoloogia kiire areng on märkimisväärselt suurendanud küberluure ja -ründe võimeid, samuti toimepidevuse takistamist ning seeläbi riigi majanduse nõrgestamist. Agressioon küberruumis on muutunud tavapäraseks — küberründe läbiviimine on kauge vahemaa tagant

[4] nt konkreetne salastatud teabe aluse sõnastus.
[5] nt teave on salastatud kuni mobilisatsiooni välja kuulutamiseni (sidumine kindla sündmuse saabumisega).
[6] nt kaitseväeluuret teostava Kaitseväe struktuuriüksuse poolt teabe varjatud kogumisel kasutatavad meetodid, taktika ja vahendid ning neid kajastav teave salajasel tasemel teave, mida tuleb salastada kuni 50 aastaks.

lihtsam ning ressursse säästvam kui füüsilise ründe läbiviimine. Seetõttu on mitmekordselt suurenenud küberkaitse/teabeturbe olulisus. Tehisintellekti ja robootika ning muude uute tehnoloogiate arendamine ja kasutamine on kaasa toonud mehitamata lennuvahendite ja -tehnika kasutamise relvakonfliktis[7]. Teisest küljest on elektroonilisel kujul akrediteeritud töötlussüsteemis olevat teavet märkimisväärselt lihtsam kaitsta kui paberkandjal olevat teavet. Tänane kehtiv seadusandlus ei loo piisavaid võimalusi elektroonilise teabeturbe kaitsevõimalusi kasutada – näiteks ei ole võimaldatud korraldatud viisil turvalisust tagades piiratud tasemel töötlussüsteemide kasutamine väljaspool administratiiv- ja turvaala.

Muudatused on toimumas ka muudes riiklikes regulatsioonides. Näiteks hiljuti heakskiidetud küberturvalisuse strateegias on samuti välja toodud, et muutunud julgeolekuolukorra tõttu tuleb järgnevatel aastatel üle vaadata küberturvalisuse, teabekaitse ja kriisiohje õigusruum, et see vastaks parimale praktikale, lähtuks riskijuhtimise kesksest teabe kaitsest ning tagaks Eesti riigi teenuste ja toimimise turvalisuse kõikehõlmavalt[8] – nii salastatud kui salastamata teabe kontekstis.

Antud teema on aktuaalne ka ülikoolides, nt TalTechi arvutisüsteemide instituudi teadlased teevad tehisintellekti rakendamisel koostööd Ukraina Rahvusliku Tehnikaülikooliga. Nii mõnelgi korral on kerkinud üles mure, kuidas saaksid ukrainlased jagada sõjakoldest kogutud andmeid teadlastele vajalikul kujul. Tsiviilandmete jagamisega on lihtsam, kuna selleks on olemas kõigile kättesaadavad andmebaasid[9]. Selliste olukordade lahendamiseks on vaja muuta salastatud teabe kaitse normid konkreetsetest juhtumitest ning riskijuhtimise põhimõtetest lähtuvaks.

Tehnoloogia areng ei ole enam seotud kitsalt digilahendustega, vaid igapäevaeluga üldiselt. Eesti riik on digiriik, kus andmed on elektroonilisel kujul. Teisisõnu, küberturvalisus kontseptsioonina ei ole enam vajalik üksnes tehnoloogiate kaitsmiseks, vaid ühiskonna toimimiseks ja selle tulevikukindluse tagamiseks[10].

Julgeolekukeskkond on pidevas muutumises, tähendades riigikaitseliste küsimuste laienemist valdkondadesse, kus neid varem ei esinenud[11]. Riikliku teabe kaitsesse peab jõudma laiapindse kaitse põhimõte. Riigi julgeoleku tagamiseks on õigusaktide muutmisel vaja hinnata muudatustega kaasnevat koosmõju ka teiste seadustega ning seda kasvõi juba sõnavara ühtlustamisest lähtuvalt.

Käesoleva VTK raames tõusetub riigikaitselisele teabele avaliku teabe seaduse (AvTS) alusel kehtestatud juurdepääsupiirangu aluste ning juurdepääsupiirangu tähtaja piisavuse küsimus, kuna VTK koostamise ajal kehtivate AvTS-s põhimõtete järgi võib riigi julgeoleku tagamise seisukohast kaitset vajav teave jääda piisava kaitseta.

AvTS jõustus 01.01.2001. ja on üldjoontes, nagu ka RSVS, (paber)dokumendi keskne ning reguleerib detailselt teabe asutusesiseseks kasutamiseks määramise aluseid, arvestamata seejuures kiire tehnoloogia- ja digiarenguga kaasas käivaid teabe töötlemise viise erinevates lahendustes ja töötlussüsteemides. AvTS-i eesmärk on tagada Eesti Vabariigi põhiseaduse (PS) §-s 44 sisalduva informatsioonivabaduse ja ametiasutuste informeerimiskohustuse põhimõtte

[7] Riigikaitse arengukava 2022-2031 (lk 8).
[8] Küberturvalisuse strateegia 2024-2030 (lk 6).
[9] https://taltech.ee/uudised/teadlane-arutleb-missugused-moodsa-kubersoja-eetilised-aspektid-ja-kas-me-suudame-ennast.
[10] Viide 7 (lk 8).
[11] EV PS kommenteeritud väljaanne X peatükk, kättesaadav: https://pohiseadus.ee/sisu/3603.

elluviimine. Kui seadus ei sätesta teisiti, siis on PS §-is 44 sätestatu nn „igaühe õigus“, mis tähendab, et nimetatud õigused on võrdselt Eesti kodanikuga ka Eestis viibival välisriigi kodanikul ja kodakondsuseta isikul. AvTS on seotud ka Euroopa Nõukogus vastu võetud ja jõustunud ametlikele dokumentidele juurdepääsu Euroopa Nõukogu konventsiooniga[12] (nn Tromsø konventsiooniga), mille Eesti ratifitseeris 2016. aastal. Konventsiooni eesmärk on tagada igaühe õigus pääseda taotluse korral juurde avaliku võimu kandjate valduses olevatele ametlikele dokumentidele[13], andes samas õiguse piirata juurdepääsu, kui piirangud on seaduses täpselt sõnastatud ning demokraatlikus ühiskonnas vajalikud ja proportsionaalsed[14].

Seoses rahvusvahelise julgeoleku olukorra muutumisega vaadati 2015. aastal üle juurdepääsupiirangu alused riigi julgeoleku tagamise seisukohalt ning 2016. aastal jõustunud muudatusega lisandus AvTS § 35 lõikele 1 punkt 3^1. Muudatuse põhjuseks oli kõrgendatud oht, et Kaitseväe teenistujate, kellel on juurdepääs riigikaitselisele teabele, vastu võivad huvi tunda ka välisriikide eriteenistused või organisatsioonid. Kaitseväe personali puudutava detailse teabe kättesaadavus lihtsustab selliste isikute ja organisatsioonide võimalikku tegevust ning see võib potentsiaalselt seada teenistujad ebasoovitava välise surve või mõjutuste alla ning sealtkaudu mõjuda negatiivselt riigi julgeolekule tervikuna[15]. Rahvusvaheline julgeolekuolukord muutus taaskord oluliselt 24.02.2022, mil algas täiemahuline sõda Ukrainas. See loob vajaduse hinnata õigusaktidest tulenevat teabejulgeoleku tagamise meetmete piisavust.

Riigikaitse korraldamisel lähtutakse ülesannete jäävuse põhimõttest, mille kohaselt ei jaotata kriisi- või sõjaajal ümber asutuste või ministeeriumide ülesandeid või pädevusi, vaid iga pädev asutus peab olema valmis tegutsema oma vastutusvaldkonnas erinevates kriisolukordades[16]. Lahinguvalmiduse seisukohast saab üksuse võitlusvõimele ja võimekusele hinnangu anda, omades ülevaadet üksuse isikkoosseisust, varustusest, väljaõppest, reageerimiskiirusest, operatiivkavadest jms tervikuna[17]. Asutusesiseseks kasutamiseks tunnistatud teabe puhul on võimalik kehtiva seaduse alusel juurdepääsupiirang kehtestada maksimaalselt kümneks (5+5) aastaks, mis ei pruugi riigikaitselise teabe (sh personali andmed, töötlussüsteemide tehnilise ja turvameetmeid käsitlev teave, turvameetmed, töömeetodid, ülesannetega seotud isikud, jmt) puhul olla piisav. Teabe avalikuks tegemine pärast seadusest tuleneva tähtaja lõppu võib riigi kaitset ja -julgeolekut tagavale asutusele tuua kaasa haavatavuse. Tulenevalt riigikaitse planeerimise protsessi pikaajalisusest tekib olukord, kus teabele juurdepääsu piiramise vajadus jääb püsima ka pärast seaduses kehtestatud võimaliku maksimaalmäära lõppu. Analoogsed asutusesiseks kasutamiseks mõeldud teabe kaitset reguleerivad EL/NATO õigusaktid ei kehtesta teabele automaatselt kehtivuse lõpu tähtaega, vaid võimaldavad vajadusel korral antud küsimust täpsemalt reguleerida asutuse spetsiifiliste juhendite näol.

Lisaks loob kehtiv õigus olukorra, kus asutuse loodud teabele tuleb viie aasta järel anda hinnang, kas juurdepääsupiirangu kehtestamise põhjus püsib. Põhjuse püsimisel tuleb asutuse juhi otsusel[18] seda tähtaega pikendada kuni viie aasta võrra. Hinnangu teabe sisule saab anda teabe looja või valdkonna eest vastutav isik, mis arvestades Kaitseväe rotatsioone ja dokumentide hulka aastas (u 50 000) ei ole alati võimalik. Tähtaja pikendamisest tuleb teada anda kõigile dokumendi adressaatidele. Antud olukord toob asutusele kaasa ebaproportsionaalselt suure halduskoormuse, mis ei ole tulenevalt ressursside piiratusest mõistlik ning mistõttu kannatab riigikaitsjate põhiülesannete täitmine.

[12] Ametlikele dokumentidele juurdepääsu Euroopa Nõukogu konventsioon.
[13] Ametlikele dokumentidele juurdepääsu Euroopa Nõukogu konventsioon art 2 p 1.
[14] Ametlikele dokumentidele juurdepääsu Euroopa Nõukogu konventsioon art 3 p 1.
[15] Vt ka Kaitsepolitseiameti 2016 ja 2018. aasta aastaraamatud ja Välisluureameti 2019. aasta raport.
[16] EV PS kommenteeritud väljaanne X peatükk, kättesaadav https://pohiseadus.ee/sisu/3603.
[17] Peamiselt on tegemist juurdepääsupiiranguga teabega AvTS § 35 lõike 1 $p3^1$ mõistes.
[18] AvTS § 40 lg 3.

Samuti on erinevate teenuste konsolideerimine toonud kaasa olukorra, kus erinevad asutused töötlevad teavet teise asutuse jaoks ja teise asutuse, mh teenistujate, taristu jne kohta. Näiteks Kaitseväele osutab personaliteenust Kaitseministeeriumi valitsemisalasse kuuluv Kaitseressursside Amet ning hangete ja taristuga seonduvat korraldab Riigi Kaitseinvesteeringute Keskus. Samas töötlevad mõlemad asutused teavet, mis on oma olemuselt Kaitseväe teave (riigikaitse rajatised, Kaitseväe rahu- ja sõjaaja koosseis jne), st teabe looja ja omanik on Kaitsevägi. AvTS sätete sisustamisel (muutmisel) ei saa sellest tulenevalt teabe kaitsel lähtuda teabe sisu omaniku[19] kohustusest, vaid oluline on teabe julgeolekut tagada läbi kaitstava teabe sisu.

Tulenevalt eeltoodust ning tuginedes PS §-ile 44 ja Tromsø konventsioon artikli 3 lõikele 1 on vaja analüüsida AvTS muutmist või kaaluda eriseadusesse[20] riigikaitselisele teabele pikema juurdepääsutähtaja määramise võimaluse (mh ilma vajaduseta pikendada seda viie aasta möödudes teabe loomisest) sissetoomist analoogselt politsei ja piirivalve seadusele[21]. Lahenduseks võib olla ka AvTS-is terviklikult loobuda teabe tähtajalisusest ning võimaldades seda reguleerida valitsemisala siseste juhistega. Asutusesesiseseks kasutamiseks teavet reguleeriv seadus ning RSVS peaksid olema omavahel suuremas seoses, st AvTS-i nõuded peaks olema võimalikult suures osas baasiks (kindlasti mitte vasturääkivad) salastatud teabe kaitsel. Sellest põhimõttest lähtumist näeb ette ka riigi küberturvalisuse strateegia.

Sõjalise riigikaitse seisukohast on vaja muuta paindlikumaks järgmised probleemkohad:

<u>Probleem nr 1.1.</u> Salastamisele paindlikkuse loomine (sh tähtaegadele).

Erinevaid salastatud plaane ja kavasid saab koostada kinnises infosüsteemis, kuid nende harjutamine ning reaalne elluviimine võib olla RSVS-st ning RSVKK-st lähtuvalt salastatud teabe töötlemine, mis tohib toimuda selleks spetsiaalselt loodud alal (nt turvaala). Salastatud teabe töötlemine on üldjuhul rangelt seotud turvaalaga ning teabe kaitsemeetmete rakendamine on arusaadavalt kohustuslik. Näiteks teatud operatiivse ja/või taktikalise teabe sisu on oma olemuselt salajane ainult lühikest aega, kuna teave on aktuaalne ja kasutatav lühiaegselt (näiteks sihtmärgid, teatud võime asukoht ja/või paiknemisala jms).

Paindlikumad meetmed on seaduses vajalikud seoses sõjalise kaitsetegevuse ettevalmistamisega ja harjutamisega ning riigikaitse operatsiooniplaneerimise ja –juhtimise korraldamisega.

Seega tuleks kaaluda salastamise aluste üldsõnalist määratlemist:

- *„TÄIESTI SALAJANE: teave mille loata avaldamine võib väga tõsiselt kahjustada Eesti Vabariigi olulisi huve;*
- *SALAJANE: teave, mille loata avaldamine võib tõsiselt kahjustada Eesti Vabariigi olulisi huve;*
- *KONFIDENTSIAALNE: teave, mille loata avaldamine võib kahjustada Eesti Vabariigi olulisi huve;*
- *PIIRATUD: teave, mille loata avaldamine võib negatiivselt mõjutada Eesti Vabariigi olulisi huve.“*

[19] nn asutuse juhi vastutus.
[20] Nt Kaitseväe korralduse seadus (KKS).
[21] PPVS § 8 lg 7, Käesoleva paragrahvi lõikes 6 nimetatud teabe puhul võib Politsei- ja Piirivalveameti peadirektor juurdepääsupiirangu tähtaega pikendada viie aasta kaupa, kui juurdepääsupiirangu kehtestamise põhjus püsib, kuid mitte kauemaks kui 30 aastaks alates dokumendile juurdepääsupiirangu kehtestamisest.

Lisaks tuleks salastatuse tähtaja määramisel lähtuda kaalutlemisest ehk integreerida õigusakti paindliku salastamise põhimõte, mille kohaselt tuleb riigisaladuse salastamisel lähtuda ohtudest ja riskidest, st toimub riskipõhine lähenemine. Mis tähendab, et juba salastamise alus peaks formaalse sõnastuse asemel olema riskijuhtimise keskne ning seda peaks eelkõige hindama teabe omanik.

Salastatuse tasemete määramine **tuleks seega viia asutuste salastatud teabe kaitse juhenditesse**, kus iga asutus saab *oma* teabele seada sellise taseme ja tähtaja, mida ta teabe kaitsmiseks vajalikuks peab. Selline lähenemine loob võimaluse teatud salastamise aluste sisu kaitseks.

Praegu tuleb see RSVKK-st, mis on Vabariigi Valitsuse määrus ja selle muutmise peab läbi rääkima mitmete riigiasutustega. Selline põhimõtteline muudatus toob kaasa vajaduse ümber vaadata riigisaladuse salastatuse taseme ja tähtaja muutmise eest vastutavate asutuste ülesanded. See omakorda tähendab, et ka asutuste riigisaladuse kaitset korraldavate isikute ülesanded ja pädevus tuleb üle vaadata, kuna just nendele isikutele/institutsioonidele kuulub asutuste loodud teabe salastamise kompetents.

Veel on võimaluseks riigikaitse riigisaladuse sätete puhul kaaluda sõnastada salastamistähtaeg konkreetse tegevuse ja/või sündmuse saabumisega, kuna salastatud kaitseplaan või tegevusplaan on koostatud konkreetse sündmuse jaoks ning tõenäoliselt selle sündmuse saabumisel tekib vajadus seda teavet töödelda ka väljaspool turvaala ja salastatud teabe töötlussüsteeme, st salastatus võiks lõppeda/kustuda automaatselt (st, muutub avalikuks või juurdepääspiiranguga asutusesiseseks kasutamiseks). Seega tuleks kaaluda, et regulatsioon näeks ette ka võimaluse, kus teabe salastatus lakkab olemast läbi tegevuse (st, ei toimu salastatuse kustutamist), kuna avalikustatud teavet uuesti ei salastata.

Eesmärk on muuta teatud tunnustele vastava salastatud teabe töötlemine paindlikumaks, kuna see vajab läbi harjutamist või rakendamist nt avalikus ruumis või teatud sündmuse toimumisel.

<u>Probleem nr 1.2.</u> Salastatud teabe hävitamine.

Salastatud teabe hävitamine on oma olemuselt väga tugevalt seotud teabekandjaga (paberkandja, välismäluseade), isiku- (register) ja asukohakesksusega (turvala), kuid need lahendused ei ole rakendatavad sõjaliseks otstarbeks loodud ja salastatud teavet kandvate elementide hävitamise puhul (nt salastatud teavet kandev rakett, miin, laskemoon, lahingumoon).

Elektroonilisel kujul oleva salastatud teabe hävitamine vajab koostöös parimate tehnoloogiaekspertidega lahenduse leidmist, et tagada teabe kaitstus. Täna puudub selgus meetodite osas, mis tagaksid elektroonilise teabe täieliku hävitamise. Detailsem teave hävitamise meetodite kohta vajab ise kaitset.

Eesmärk on muuta hävitamise regulatsioon paindlikumaks ja kaasaegsemaks lähtuvalt tänasest tehnoloogilisest reaalsusest, mis lubaks salastatud teavet hävitada ka mitte traditsioonilisel viisil või annaks võimaluse teatud olukordades lugeda salastatud teave hävitatuks, kuigi füüsilised tõendid selle kohta puuduvad.

<u>Probleem nr 1.3.</u> Piiratud tasemel salastatud teabe töötlemine väljaspool administratiivala ning konfidentsiaalsel ja kõrgemal tasemel salastatud teabe töötlemine väljaspool turvaala.

Kehtiva õiguse kohaselt on salastatud teabe töötlemine <u>avalikus ruumis</u> piiritletud riigikaitse riigisaladuse puhul konkreetselt teabe liigiga[22] ning teatud nõuetele vastava teabetöötlussüsteemiga. Samas töötlussüsteemide hankimisel juba arvestatakse vajadusega, et süsteemis on võimalik vajaduse korral (eriolukordades või nendeks ettevalmistudes) töödelda salastatud teavet. Sellest tulenevalt on vaja hinnata riigikaitse riigisaladuse sätete juures teabe töötlemise vajadust kriisisituatsioonides operatiivselt ja tõrgeteta, ehk luua õigusakti paindlikkus.

Nt Kaitseväes toimub teabe töötlemine kehtiva õiguse kohaselt (Kaitseväe korralduse seaduse § 50) kontrollitud keskkonnas, st Kaitseväe julgeolekualadel, mis hõlmab ka ajutisi julgeolekualasid ning erinevaid sõidukeid, ehk tegemist ei ole avaliku ruumiga klassikalises mõttes.

Riik on soetanud erinevaid salastatud teavet sisaldavaid relvasüsteeme (meremiinid, rannikukaitse, mitmikraketiheitjad, keskmaa õhutõrje) ning kehtiva õiguse alusel tuleb süsteeme käidelda kui salastatud teabekandjaid ehk need peavad paiknema ja olema hoiustatud turvaaladel. Raketid, meremiinid, relvasüsteemid jne võetakse arvele salastatud teabekandjatena, kuna raketid sisaldavad salastatud teabega osiseid, samas kehtiva regulatsiooni kohaselt on problemaatiline nt meremiinide veeskamine, kuna puudub konkreetne turvaala. Lisaks eksisteerib probleem nt salastatud relva tulistamisel vastase kontrollitud alale, kui laeng ei lõhke. Kas tegu on salastatud teabe avaldamisega ning sellest peaks välisteabe puhul teavitama teabe omanikku – välisriiki?

Lahenduseks on regulatsioonides baastasemel normide uus kokkuleppimine, mis võimaldaks eelkõige füüsilise turbe normide paindlikkust juhul, kui töötlev üksus on riske hinnanud, mõelnud läbi ja kehtestanud kompenseerivad meetmed ning aktsepteerinud jääkriski lähtuvalt oma kaasusest ning ohtudest, mis mõjutavad konkreetset teavet ning töötlevat üksust.

Eesmärk on näha ette täiendavad võimalused töödelda teatud salastatud teavet väljaspool turvaala riskijuhtimise põhimõttest lähtuvalt.

<u>Probleem nr 1.4.</u> Muuta RSVS (sh RSVKK) tervikuna paindlikumaks ja vähendada piiranguid, mis limiteerivad tegevusvabadust riiki valitseva julgeolekuohu likvideerimisel või mis ei ole üheselt mõistetavad.

Riigikaitse riigisaladuse tunnustele vastavat teavet peab olema võimalik töödelda julgeolekualadel, st kontrollitud keskkonnas. Vastasel juhul on takistatud salastatud teabe operatiivne edastamine. Mõistlik on seega RSVS ja RSVKK-sse tuua administratiiv- ja turvaala kõrvale täiendavalt mõiste „julgeolekuala“. Antud muudatus aitab Kaitseväel paremini valmistuda nt sõjaseisukorraks. Ilmselt tuleb siis ka muuta Kaitseväe korralduse seadust ja lisada Kaitseväe julgeolekualade nimekirja relvasüsteemid ning mõtestada laiemalt julgeolekuala eesmärk (Kaitseväe isikkoosseisu-, teabe-, taristu- ja vara- julgeoleku tagamine).

[22] RSVKK § 103 lg 2[1], Kaitsevägi võib töödelda kuni salajasel tasemel salastatud operatsiooniplaanimist ja operatsioonijuhtimist käsitlevat riigikaitse riigisaladust või selle sisule vastavat salastatud välisteavet avalikus ruumis, kui sellise teabe edastamine on vajalik rahvusvahelises sõjalises koostöös osalemiseks või riigi sõjaliseks kaitsmiseks ning kasutatakse avalikus ruumis töötlemiseks ette nähtud akrediteeritud süsteemi.

Töötleval üksusel peab olema võimalus hinnata, mis on salastatud teave lähtuvalt töötleva üksuse vajadusest. Samaaegselt tuleb kaaluda ka asutusesiseseks kasutamiseks teabe juurdepääsupiirangu tähtaja pikkust, kuna AvTS-is toodud 5+5a juurdepääsupiirangu tähtaja põhimõte ei pruugi olla piisav olulise teabe kaitsel. Regulatsioonid peavad võimaldama juurdepääsupiirangu ühetaolist tähtaega. Täpsustamist vajab ka salastamistähtaja möödumisel teabe hindamine lähtuvalt püsivast teabe kaitse vajadusest (ei toimu aktiivset avalikustamist).

Suuremat paindlikkust vajab ka RSO keskne salastatud teabe kaitse, eriti olukorras, kus tegevus toimub juhtriigi või -riikide egiidi all. Sellisel puhul peaks tekkima võimalus lähtuda juhtriigi salastatud teabe kaitse reeglitest (NATO ja EL teabe töötlemisel tuleb nagunii lähtuda nende organisatsioonide töötlemise reeglitest). Suurema paindlikkuse loomiseks võiks olla olukord, kus RSO-del toimub salastatud teabe töötlemine seda juhtiva riigi poolt etteantud reeglite järgi (sh füüsilised nõuded), kuna ka välisriikide salastatud teabe kaitsemeetmete eesmärk on takistada salastatud teabele juurdepääsuõigust ja teadmisvajadust mitteomavatele isikutele.

Samuti tuleb läbi mõelda **hübriidteabe**, st erinevate (nii riigisiseste kui ka välisriigi) asutuste koosloodud teabe, loomise ja salastamise kontseptsioon. Sh tuleks paberi/dokumendi kaitsmise asemel üle minna **teabe kaitsmisele** (*data centric security*), kuna (rahvusvahelistest organisatsioonidest) NATO on võtnud selge suunise teabe kesksele kaitsele üleminekuks, st tulevikus soovitakse IT-süsteemides kasutusele võtta sellised tehnilised lahendused, mis kaitsevad teabe killukesi, mitte enam dokumenti kui sellist.

RSVS-is peaksid olema defineeritud ainult üldisemad ja teemade põhised salastatuse alused, nt:

- „**horisontaalselt**“/valdkonnaüleselt/asutusteüleselt, sh võimaldama teatud **paindlikkust** (nt reguleerima miinimumtaseme ja/või võimalike tasemete vahemiku);
- „**vertikaalselt**“/valdkonnapõhiselt/asutusesiseselt, mis lähtuks rohkem valdkonna ja asutuse **spetsiifikast** ning lähtuma rohkem asutuse enda riskihinnangust.

Eesmärk on arusaadavalt sõnastada teatud teabe salastamise alused, et rakendajal oleks üheselt selge, milline teave vastab riigisaladuse tunnustele.

Eesmärk on võimaldada nt Kaitseväel erikorra ajal töödelda konkreetse sündmusega seotud riigikaitse riigisaladust Kaitseväe poolt kontrollitud aladel, tagades teadmisvajaduse ja juurdepääsuõiguse printsiibid.

Probleem nr 1.5. Salastatud teabe normide muutmine lähtuvalt vajadusest teavet kiirelt töödelda, nn pilvlahenduses teabe töötlemise läbimõtlemine.

Riigi valmisolek ennetada ja vajaduse korral ka tõrjuda julgeolekut ähvardavat ohtu, tähendab pidevat teabe analüüsi ning vajaduse korral ka salastatud tasemel koostatud plaanide uuendamist. Seega peaks salastatud teabe muutmise regulatsioon olema paindlik ning esmajärjekorras seadma eesmärgiks teabe kiire edastamise vajaduse, et adekvaatselt reageerida tekkinud ohule (nt üksuse kaitseplaani muutmine ja selle edastamine üksustele).

Vaja on kaaluda, millistel tingimustel võiks toimuda salastatud teabe töötlemine nn pilvlahenduste ja -teenuste abil – kas kasutada riigi kontrolli all olevaid pilvlahendusi või kaaluda ka teatud teabe liikide puhul hübriidpilve kasutamist, st riigi tundlikke andmeid haldab erasektor. Hübriidpilvelahenduse kasuks otsustamisel peab analoogselt NATO normidele läbi

mõtlema riigisisesed hübriidlahenduse teabeturbe nõuded, mida peab erasektor andmete haldamisel järgima.

Lisaks peab välja töötama turbenõuded tehisintellekti (AI[23]) kasutuselevõtu võimaldamiseks Kaitseväe salastatud töötlussüsteemides, et tagada sõjalise tehisintellekti arendamine (mehitamata sõidukid ja süsteemid, lahingujuhtimine, küberoperatsioonid jmt). Kaitseministeeriumi valitsemisala, sh Kaitseväe, aga ka laiemalt kogu kaitsetööstuse, tehnoloogilise arengu suuna seadmine peab arvesse võtma meie tõenäolise vastase tehnoloogilist arengut. Meie töötlussüsteemides kasutatavad tehisintellekti lahendused peavad olema turvalised ning tagama sõjapidamises vaenlasest üleoleku.

Eesmärk on muuta salastatud teabe töötlemine kiiremaks, et salastatud teabe töötlemine arvestaks infotehnoloogia arengust tulenevate võimalustega – seadusandlus peab käsikäes tehnoloogiaga looma selleks võimalused, mitte kujunema takistuseks.

<u>Probleem nr 1.6.</u> Salastatud teabe jälgitavus.

Riigikaitse on üha rohkem laiapõhjalisem ja lõimunud, seda mitte ainult teiste riigiasutustega, vaid ka rahvusvaheliste organisatsioonide ning teiste riikidega. See tekitab olukorra, kus salastatud teavet on aina rohkem ja seda on vaja liigutada erinevate salastatud töötlussüsteemide vahel. Teabe liigutamine erinevate süsteemide vahel ning sellega tutvumine isikute poolt peab olema jälgitav, samas juba kord salastatud teabekandjate registris registreeritud teavet ei peaks selle liigutamisel mitme süsteemi vahel uuesti salastatud teabekandjate registris registreerima. Hetkel see siiski toimub, st et üks teabekandja võib saada ühe või mitu registreerimise numbrit, mis on aga ebamõistlik. Töötlussüsteemide logid peavad olema inimloetavad ning samaaegselt tagama andmete registreerimise metatasandil ja teabe turvalise liigutamise töötlussüsteemide üleselt ilma inimese ülemäärase sekkumiseta.

Eesmärk on vähendada teabe registreerimiste ja töötlussüsteemide vahel liigutamisega kaasnevat halduskoormust.

2. Eesmärgid

VTK peamiseks eesmärgiks on juhtida tähelepanu kitsaskohtadele, mis (ebamõistlikult) piiravad salastatud teabe töötlemist, ning leida nendele lahendusi. Vaja on saavutada olukord, kus salastatud teave liigub institutsioonide/asutuste vahel võimalikult kiiresti vajalike otsuste tegemiseks, samas tegemata järeleandmisi teabe kaitse meetmetes, st tagada teabe salajasus, käideldavus ning terviklikkus, lähtuvalt riigi julgeolekut ähvardavatest ohtudest.

Integreerida õigusakti paindliku salastamise põhimõte, mille kohaselt tuleb riigisaladuse salastamisel lähtuda ohtudest ja riskidest ehk toimub riskipõhine lähenemine, kus eesmärk on riskide ja ohtude kaudu määrata konkreetse teabe võimalik salastamise vajadus[24] (sh selle salastatuse tase ning salastatuse tähtaeg).

[23] *Artificial intelligence* masinapõhine süsteem, mis selgesõnaliste või kaudsete eesmärkide saavutamiseks tuletab antud sisendi põhjal väljundeid, näiteks ennustusi, sisu, soovitusi või otsuseid, millel võib olla mõju füüsilistele või virtuaalsetele keskkondadele

[24] Nt nagu on kasutusel NATO direktiivis „Directive on Security of NATO Classified Information“ (lk 3).

Samuti vaadata üle eelkõige riigikaitselise teabe, kuid ka muu, riskipõhise salastamise ja käitlemise võimalused ning luua teabe töötlemise võimalused lähtudes põhimõttest, et õige teave oleks õigel ajal õigel kasutajal.

Salastatud teabe töötlemise nõuetest on võimalik kõrvale kalduda ainult karistusseadustikus toodud õigusvastasuse kaudu. Vaja on sõnastada salastatud teabe töötlemise nõuded sõltuvalt riigis kehtestatud (eri)seisukorrast. Karistusseadustiku põhimõtte kaudu lähenemine ei ole Kaitseministeeriumi hinnangul mõistlik ning võimalikud erisused peavad olema loodud valdkondlike regulatsioonidega.

Kaitseministeeriumi valitsemisala töötlevatele üksustele on vaja anda kindlustunne, et riigi sõjaliste kaitseplaanide harjutamine ja nende rakendamine on võimalik, kartmata salastatud teabe nõuete rikkumist. Teabe looja peab saama võtta suurema vastutuse enda valduses oleva teabe kaitse üle, mis lõppkokkuvõttes tagab läbimõelduma ja efektiivsema teabe kaitse ning väldib alasalastamist.

Samuti on RKAK-is toodud mitmed olulised arendustegevused, millel on puutumus salastatud teabega, seda just lähtuvalt kasutatavast tehnoloogiast[25].
Nt seoses riigikaitse sõjaliste võimearendustega (laevatõrjeraketid, mereseiresüsteem) on tõusetunud vajadus salastatud teabe töötlemiseks väljaspool turvaala, sest tervik relvasüsteemi ei ole alati võimalik ja ka vajalik hoiustada ega kasutada turvaalal.

VTK võimalik puutumus põhiõiguste ja vabadustega on välja toodud VTK lk 4-5, aga see on minimaalne, kuna siht on reguleerida salastatud teabe töötlemist ja antud teave on oma olemuselt juba limiteeritud ligipääsuga ning selle töötlemine toimub nn suletud süsteemis, kus teabele antakse juurdepääs ainult teadmisvajaduse põhiselt.

VTK ei ole otseselt seotud EL õiguse rakendamisega.

3. Võimalikud lahendused

Kaitseministeerium leiab, et senise regulatsiooni säilitamine ei aitaks kaasa käesolevas VTK-s esile toodud probleemide lahendamisele ja eesmärgi saavutamisele. Avalikkuse teavitamise, rahastuse suurendamise ja regulatsiooni senisest tõhusama rakendamise teel ei oleks samuti võimalik probleemide lahendamisele kaasa aidata.

Mitteregulatiivsete lahendustega (nt suurem rahastus, parem teavitus) salastatud teabe töötlemise osas paindlikkust luua ei ole võimalik, kuna salastatud teabe töötlemine on õigusaktides vägagi detailselt sätestatud.

Kaitseministeeriumi hinnangul ei ole salastatud teabe töötlemise tingimustes piisavat, st uutele tehnoloogiatele kui ka ohtudele reageerimist võimaldavat paindlikkust ette nähtud, seega ei ole ilma riigis kehtivat regulatsiooni kardinaalselt muutmata, võimalik VTK-s toodud probleemkohti lahendada.

Tekkinud probleeme aitab lahendada regulatsiooni põhjalik kaasajastamine, st lahendusena tuleb muuta riigisaladuse ja salastatud välisteabe seadust ning selle aluspõhimõtteid.

[25] Viide 6 (lk 12).

Eespool nimetatud seaduse eelnõu koostamise käigus võib selguda vajadus muuta ka mõnda muud seadust või määrust (nt KKS).

4. Uuringud ja kaasatud osapooled

Uuringuid ei ole läbiviidud. Probleemkohad on esile kerkinud reaalsete tegevuste käigus ning üldise riigikaitse arendamise raames.

VTK väljatöötamisel on olnud kaasatud eeskätt Kaitsevägi. Esmast tagasisidet on saadud ka Välisluureametist, kes põhimõtteliselt toetab ettepanekut võimaldada salastatud teabe töötlemise põhjalikumat muutmist, et tagada kriisi- või sõjaolukorras teabe kaitstus, kus kõigi tänaste RSVS-s või RSVKK-s salastatud teabe kaitseks kehtestatud normide täitmine ei taga reaalselt teabe kaitset ning on viinud võimaliku alasalastamiseni.

5. Mõju

Muudatustega kaasnev täpsem mõjude analüüs valdkondade, sihtrühmade ja mõju ulatuse kaupa analüüsitakse eelnõu koostamise käigus.

Andmekesksusel ja riskijuhtimisel põhinemine on olulised muudatused, mis toimimiseks vajavad nii teabe töötlejatelt (asutus, isik) kui ka selle töötlemise korraldamise ning järelevalvega seotud osapooltelt nn maailmavaate muutust.

VTK-s väljatoodud muudatused puudutavad eeskätt asutusi, kus töödeldakse salastatud teavet, kuid eelkõige on võimalikud muudatused vajalikud sõjalise riigikaitse huvides. Seega suurimat kasu saab sellest Kaitseministeeriumi valitsemisala (eeskätt Kaitsevägi), kuid erisusi salastatud teabe töötlemisele erinevates kriisiolukordades on vaja ka teistele töötlevatele üksustele üle riigi, et tagada laiapindne riigikaitse.

Suund on lihtsustada salastatud teabe töötlemist, säilitades samas teabejulgeoleku põhimõtted. Muudatused omavad positiivset mõju töötlevate üksuste halduskoormusele, kuna teatud toimingud võivad nt ära jääda või nende toimingute tegemiseks on volitatud rohkem isikuid.

Eelnõu ettevalmistamise käigus analüüsitakse kavandatavate muudatuste mõju täiendavalt ning seda hinnatakse eelnõu seletuskirja vastavas osas.

6. Edasine väljatöötamine

VTK tagasisidena saadud ettepanekute põhjal alustatakse eelnõu väljatöötamist. Ideaalis võiks ideed ja tähelepanekud Kaitseministeeriumisse laekuda 2025. aasta esimese kvartali jooksul. Eelnõu võiks valmida sama aasta III kvartali jooksul.

Eelnõu saadetakse kooskõlastusringile arvamuse küsimiseks ning kommenteerimiseks ja täiendavate ettepanekute saamiseks kõikidele ministeeriumitele, Riigikantseleile, Kaitsepolitseiametile, Välisluureametile ja Kaitseväele.

VTK on koostanud kaitseministeeriumi julgeoleku- ja haldusosakonna juhataja asetäitja Karel Brandt (karel.brandt@kaitseministeerium.ee).