KAITSEVÄELUURE RIIGISISESE JULGEOLEKU MEETMED

SIIM ARTUR JUHT, EERIK HELDNA

Võtmesõnad: kaitseväeluure, julgeolek, kaitseväe korralduse seadus, julgeolekuasutuste seadus

Ülevaade. Artikli eesmärk on lugejale tutvustada kaitseväeluure olemust ning riigisisese julgeoleku tagamise meetmeid. Artikli fookuses on seadusandlusest tulenevad kitsaskohad, mida ilmestatakse praktiliste näidetega.

SISSEJUHATUS

Luure on teabe kogumine, mida on vaja riigi poliitika kujundamiseks, julgeolekuhuvide edendamiseks ning tegelike või võimalike vastastega tegelemiseks (Shulsky & Schmitt, 2013, p. 25). Eesti õiguses on luure legaaldefinitsioon toodud vaid kaitseväe korralduse seaduses (edaspidi KKS), kus avatakse kaitseväeluure kui luure ühe alaliigi mõiste. Samas käsitletakse luuramise vastutegevust ehk vastuluuret nii julgeolekuasutuste seaduses (edaspidi JAS) kui ka riigisaladuse ja salastatud välisteabe seaduses (edaspidi RSVS). Olgugi et kaitseväeluure kui selline on seotud otseselt vajadusega koguda teavet riigi sõjaliseks kaitseks, ei ole see tänapäevases julgeolekuolukorras võimalik ilma nn politseiliste julgeolekumeetmeteta, nagu näiteks personali süvendatud taustakontroll või andmete kogumine territooriumi vahetus läheduses viibivate isikute kohta, mis reeglina seostuvad riigisisese julgeolekuasutuse töövaldkonnaga. Vaidlused, kui kaugele võib ulatuda relvajõudude varjatud teabekogumine operatsioonide planeerimisel rahuajal ning julgeoleku tagamiseks riigi territooriumil, jõudsid 2020. aastal suurema avalikkuse tähelepanu alla. Osaliselt ulatuvad vaidluse juured nn kaitseväe luureskandaali 2007. aastal, mis tõi kaasa ühelt poolt jätkuvalt kõrged ootused kaitseväeluurele ka väljaspool traditsioonilist militaarvaldkonda, kuid samas ka pelguse piisavate volituste andmiseks. Aastaid poolikult ja etapiviisiliselt parandatud kaitseväeluure pädevuse küsimused said küll osaliselt lahendatud juunis 2020 jõustunud KKS nn luurepaketiga, millele eelnes tuline debatt seadusandlikul tasemel, mis päädis isegi vabariigi presidendi Kersti Kaljulaidi pöördumisega riigikohtusse, tunnistamaks vastuvõetud KKS-i muudatused põhiseadusevastaseks.

Vaidluse raskuskese seisnes kahes peamises asjaolus: laiemalt, kas KV-l on rahuajal ette nähtud siseriikliku mittesõjalise julgeoleku tagamise funktsioon ning kas nimetatud sätted on piisavalt õigusselged, tagamaks isikute põhiõigused, kui KV töötleb nende isikuandmeid. Viimase osas tuleb küll rõhutada, et KV puhul oli kohe algselt sätestatud varjatud teabe kogumisele kõrgemad loanõuded kui jälitus- või julgeolekuasutuste puhul. Näiteks oli eelnõu järgi varjatud jälgimise loa andmise õigus kaitseväe juhatajal ja luurekeskuse ülemal ning 24 tunni jooksul pidi toimingu teostamise andma üle kaitsepolitseiametile. Kuigi riigikohus leidis, et eelnõu on põhiseadusega vastuolus (RKPJKo nr 5-19-38, 2019, p. 112), nentis ta seda siiski pelgalt toimingust teavitamise osas, mitte põhimõttelises vaidluses, kus vabariigi president ja kaitsepolitseiamet (KAPO) nägid kitsaskohana, et kaitseväeluurega tegelev struktuuriüksus muutub sisuliselt julgeolekuasutuseks (RKPJKo nr 5-19-38, 2019, p. 58).

Olgugi, et KKS-i muudatused jõustusid viimaks suuresti algses mahus ja sõnastuses, siis tuleb autorite arvates võtta kaitseväeluure tegevuse jätkuvalt erinevat käsitlemist,

võrreldes KAPO või välisluureameti (VLA) tegevusega kui poolikut kompromissi, mis ei taga täies mahus seadusandjalt kaitseväeluurele pandud ootusi. Uurimisprobleemiks on olukord, milles kaitseväeluure volituste ja tegevuse õiguslik regulatsioon ei ole piisavalt selge ega taga kaitseväeluurele püstitatud riigisiseste ülesannete efektiivset täitmist. Milles seisnevad jätkuvad seadusandlikud kitsaskohad kaitseväe hädavajaliku julgeoleku- ja luurevõimekuse tagamisel, sellest annab artikkel loodetavasti ülevaate ning julgustab valdkonna asjatundjaid küsima, kas nende kitsaskohtadega leppimine on meie sõjalise valmisoleku ja laiemalt julgeoleku huvides. Kaitseväe luurekeskuse (LuK) sümbol öökull vajab pesa kaitsmiseks mitte ainult tugevaid tiibu, vaid ka võimalust märgata, kuulda ja talletada teavet ohtude kohta. Ka nende kohta, mis varitsevad öökulli pesa vahetus läheduses ehk kodumaal. Väga hästi on selle mõtte kokkuvõtvalt sõnastanud Eesti kaitseväeluure ülem kolonel Margo Grosberg: „Iga mees peab hoidma oma maja korras“ (Sildam, 2018).

Artikkel ei pretendeeri mahukaks võrdlevaks õigusanalüüsiks; see vääriks eraldi magistritööd. Käesolev tekst põhineb 2021. aastal Kaitseväe Akadeemias kaitstud lõputöö uurimistulemustel ning peamine eesmärk on avada laiemale üldsusele kaitseväeluure olemust, selle sarnasust ja erinevust tsiviilluurest ja julgeoleku tagamisest ning kirjeldada näidete varal igapäevase tegevuse kitsaskohti. Artiklile lisab aktuaalsust 24.02.2022 Ukraina vastu alanud Venemaa agressioon. Lisaks tavapärasele kaitsejõudude tegevusele ning selle lahutamatuks osaks olevale luurele on oluliselt kasvanud julgeoleku tagamise aspekt, seda nii teabe-, operatsiooni- kui ka personalijulgeoleku tagamise osas.

Teema uurimise praktilisi kitsaskohti kirjeldades tuleb arvestada kaitseväeluure kui uurimisobjekti äärmise suletusega. Kui julgeoleku- ja tsiviilluure maailmast on kirjutatud nii akadeemilisi kui ka populaarteaduslikke töid, samuti ilukirjanduslikke teoseid, siis kaitseväeluure osas on olukord sootuks tagasihoidlikum.

1. LUURE JA JULGEOLEK

Taktikalisemas võtmes on luure üks seitsmest lahingufunktsioonist ning luureteavet vajatakse vastase ja lahinguruumi kohta, et juhtida üksust, võtta vastu õigeaegseid ning olukorraga ühtelangevaid otsuseid, et täita püstitatud ülesanded või saavutada soovitud lõpptulemus (United States Army, 2019, pp. 2-2–2-3). Jätame artiklis kõrvale kaitseväeluure taktikalise poole ja pöörame tähelepanu sellele osale, mis on suunatud julgeoleku tagamisele, milleks on vajalik teadlikkus ohuolukorrast ja ohtude põhjustajatest. Julgeolek on seisund, milles on kaitstud piiratud ligipääsuga teave, varustus, infrastruktuur, isikkoosseis ja tegevus erinevate ohtude eest, nt vaenulik luure- ja õõnestustegevus, sabotaaž ja terrorism jne (NATO Standardization Office, 2020, p. 116).

Luurefunktsioon toetab väekaitset, tagades eelhoiatuse võimalike ohtude kohta ning on oluline komponent vastuluure- ja julgeolekuoperatsioonide läbi viimisel (United States Army Intelligence Center and School, 2004, pp. 6–1). Väekaitse on ennetavate tegevuste, meetmete ja vahendite kogum, mille eesmärk on vähendada ohte isikkoosseisule, varustusele ning operatsioonitegevusele (NATO Standardization Office, 2020, p. 55). Luuretegevus on seega otseselt seotud kaitseväe üksuste julgeolekuga ja vajalik funktsionaalsuse ja lahingvõime säilitamiseks.

Mõnikord seostatakse julgeoleku tagamist kitsalt vastuluurega. See on õige vaid osaliselt. Väärarusaama, nagu Eestis oleks vaid üks vastuluurega tegelev asutus (KAPO), on seadusandja tegelikult ümber lükanud mitmes seaduses – RSVS-is, KKS-is ja ka JAS-is –, kus riigisaladuse kaitse kui vastuluurefunktsioon või vastuluure oma töötajate kaitseks on antud piiratud ulatuses nii VLA kui ka LuK pädevusse.

Julgeoleku tagamise eesmärgil teostab kaitsevägi riigis julgeolekuluuret, mis hõlmab erinevate luuredistsipliinide, sh vastuluure samaaegset rakendamist. Kaitseväe seisukohast on aga olulisem rääkida mitte kitsalt vastuluurest, mis on suunatud riigisaladusega kaetud teabe kaitsele, vaid julgeolekuluurest, mis on eelkõige suunatud julgeolekuohtude maandamisele riigis. Julgeolekuluure on meetmete kogum, mida kaitsevägi teostab eesmärgiga koguda ja töödelda andmeid riigi vastu suunatud vaenulike tegevuse tõkestamiseks, st juba varasemalt mainitud luure, kuritegevus, sabotaaž, õõnestustegevus ja terrorism (NATO Standardization Office, 2020, p. 116). Julgeolekuluure on äärmiselt oluline ka kaitseväe territooriumi ehk kaitseväe julgeolekuala vastu suunatud ohtude tuvastamisel ja tõkestamisel.

2. RIIGISISESED JULGEOLEKUOHUD

Eesti kaitsevägi on eelkõige oma olemuselt suunatud välisvaenlase tõrjumisele ja Eesti julgeolekupoliitika kohaselt on sõjalise kaitse eesmärk ennetada ohte ja vajadusel neid tõkestada või tõrjuda (Kaitseministeerium, 2017, lk 10). Kiirelt muutuvas julgeolekukeskkonnas peab olema valmis reageerima ka ebatavalistele ehk siis mittekonventsionaalsetele ohtudele, mis samuti muutuvad aina levinumaks ning võivad Eesti julgeolekut mõjutada samaväärselt traditsiooniliste ohtudega (Kaitseministeerium, 2017, lk 4). Traditsiooniline oht on välisriigist lähtuv konventsionaalset laadi oht ning riigisisesed ohud liigituvad ebatavaliste ohtude alla.

Ebatavalist ohtu iseloomustab asümmeetriline lähenemine või tavatute võitlusviiside kasutamine, mida on raske tuvastada. Sellise võitlusviisi vastu on keeruline rakendada ennetusmeetmeid või seda operatiivselt neutraliseerida. Asümmeetriat kasutades üritatakse rakendada oma tugevust vastaspoole nõrkuse vastu, et haarata initsiatiiv ja saavutada otsustav eelis (Eaton, 2002). Seda tüüpi oht üritab luua olukorda, kus saavutatakse ebaproportsionaalselt suur võit kulutatud ressurssi või panust arvestades. Asümmeetriline oht üritab peituda ja sulanduda ümbritsevasse keskkonda.

Lisaks asümmeetrilisele ohule on käibel ka teine sarnane mõiste, nn hübriidoht. Hübriidohud tekivad tavaliselt keskkonnas, kus sõjalises mõttes konventsionaalsed ja mittekonventsionaalsed ohud põimuvad irregulaarsete ja asümmeetriliste ohtudega (Development, Concepts and Doctrine Center, 2011, pp. 1–4). David Kilculleni hinnangul on tulevikuohtude kirjeldamisel oluline tunnusjoon nende hübriidsus, st ohtude alaliigid sulanduvad üha enam kokku ja riiklikud ning mitteriiklikud osalejad rakendavad asümmeetrilist sõjapidamist. (Kilcullen, 2013, lk 107) Keeruline on eristada asümmeetrilist ohtu hübriidohust, sest tänapäevaseid konflikte iseloomustab ohtude põimumine ning mõlema ohu taga võivad olla nii riiklikud kui ka mitteriiklikud konfliktist osavõtjad.

Rekkedali järgi iseloomustab asümmeetrilist sõjapidamist samuti tugevuste kasutamine vastase haavatavuste vastu tavatul viisil (Rekkedal, 2006, p. 135). Selliste rünnakute läbiviijad esindavad neljanda põlvkonna sõjapidamist, taotledes efekti pigem strateegilisel või poliitilisel tasandil (Phelan, 2011). Eelmainitud efektide saavutamise nimel kahjustatakse tsiviilühiskonna toimimist, rünnatakse kriitilisi haavatavusi ja raskuskeset (Szafranski, 2002). Asümmeetrilisteks ohtudeks võivad olla ka riiklike luureteenistuste värvatud isikud, kes koguvad infot kaitseväe kohta (Kaitsepolitseiamet, 2020, lk 27). Halvemal juhul võib olla värvatud organisatsiooni enda teenistuja või töötaja.

Ebatavaliste ohtude näidetena sõjaväe kontekstis saab tuua organiseeritud kuritegevuse ning teenistujate sidemed sellega, nt Colombia sõjaväelaste info müümine narkokartellidele (Harber, 2009), sõjaväeteenistujate relvamüük Venemaa Föderatsioonis (Ryabikhin & Viktorova, 2004) või Eestis ebaseaduslikus relvaäris osalenud tegevväelane (2017). Teine riik võib kasutada ära riigisisest organiseeritud kuritegevust hübriidsõja elemendina riikliku julgeoleku ohustamiseks, nt Venemaa Föderatsioon Georgias (Darchiashvili, 2018). Asümmeetrilised ohud on samuti kohalikest elanikest koosnevad mitteformaalsed relvastatud või terroristlikud formeeringud, keda võib välisriik toetada ja/või juhtida, nt 2014. aastal Krimmis ja Ida-Ukrainas Venemaa Föderatsiooni kureeritud rahvaväelased (Westerlund & Norberg, 2016). Eelmainitud rahvaväelasi kasutati kombineeritult meedia ja teiste vahenditega üheaegselt nii taktikalise, operatiiv- kui ka strateegiliste eesmärkide saavutamiseks, mõjutades ukrainlaste kriitilisi haavatavusi kui ka raskuskeset (Veljovski *et al.*, 2017).

Mitteriiklikud organisatsioonid võivad omavahel koostööd teha ja samaaegselt mõjutada mitme riigi julgeolekut, st üks koolitab teise organisatsiooni liikmeid, tarnib relvastust ning vastutasuks aidatakse operatsioone korraldada, nt Euroopas tegutsenud terroriorganisatsioonid Punase Armee Fraktsioon (RAF) ja Punane Brigaad (BR) said tuge Palestiina Vabastusorganisatsiooni (PLO) käest (Karmon, 2005, pp. 105–106). Eeltoodud näide iseloomustab hästi ka selliste ohtude mobiilsust ning võimet kujutada ohtu piiriüleselt. Ohtude paindlikkus ja muutlikkus nõuab järjepidevat süstemaatilist info kogumist ja töötlemist, et kujundada adekvaatne hinnang eelmainitud ohu kohta.

Ebatavalist ohtu kujutavad organisatsioonid omavad tihti ka luure- ja vastuluurevõimekust, mida kasutatakse riiklike institutsioonide vastu, nt Colombia Revolutsioonilised Relvajõud (edaspidi FARC) rajas IT-abi pakkuva ärivõrgustiku sõjaväebaaside ligidal, et parandusteenuse pakkumise kaudu saada ligipääs teenistujate arvutitele ja seal olevale infole (Gentry & Spencer, 2010). Põhja-Iirimaal tegutsenud Iiri Vabariiklik Armee (edaspidi IRA) kasutas kaitsvat vastuluuret kohaliku elanikkonna kontrollimiseks, personali- ja tegevusjulgeoleku tagamiseks ning ründavat vastuluuret Ühendkuningriigi julgeolekujõudude liikmete ja informaatorite tuvastamiseks Põhja-Iirimaal ning Briti sõjaväeluure, julgeolekuteenistuse (MI5) ja salaluureteenistuse (MI6) töötajate tuvastamiseks Lääne-Saksamaal (Ilardi, 2010). Ühendkuningriigi relvajõudude ja julgeolekuasutustele kujutasid riski oma riigi kodanikud, kes luurasid nende järele teise NATO liikmesriigi territooriumil. IRA tegutsemine on hea näide, kuidas riigisisene asümmeetriline oht võib ohustada tegelikult teises riigis paiknevaid jõustruktuuride liikmeid ja seeläbi mõjutada üleüldist julgeoleku olukorda nii Ühendkuningriigis kui ka Põhja-Iirimaal.

Tihtipeale loovad tavatut ohtu kujutavad organisatsioonid normisüsteemi eesmärgiga hoida inimesi oma kontrolli all ja seeläbi luua võimustruktuur (Kilcullen, 2013, lk 128) – nn võistleva juhtimise teooria. Selle teooria kohaselt peibutatakse ja meelitatakse inimesed osa võtma organisatsiooni tegevusest ja selle kaudu üritatakse neid võõrandada riigivõimust. Kaitseväe mõistes on tegu otseselt personali julgeolekuga seotud ohuga. Kui nimetatud ohu tõrjumiseks sätestatud meetmed ei ole piisavad või, veelgi hullem, erinevate vastutajate pädevused ja nende piirid on ähmased ja peavastutaja (antud juhul kaitsevägi) ei saa õigel ajal vajalikke vastumeetmeid rakendada, siis võib võimalik tagajärg olla väga tõsine. Lähemalt käsitleme seda küsimust taustakontrolli puudutavas osas, kuid etteruttavalt tuleb tõdeda, et personalijulgeoleku tagamiseks mõeldud taustakontrolli regulatsioon ei vasta täies mahus eelpool loetletud ohtude tõrjumiseks.

Artikli raames ei ole piiratud mahu tõttu võimalik lõpuni ära defineerida riigisiseseid asümmeetrilisi või hübriidohte, vaid on mõistlik välja tuua iseloomulikud jooned, mis aitavad sellise ohu ära raamistada. Ohtude lõplik kataloogiseerimine ei ole otstarbekas, kuna sellist tüüpi ohu iseloomulikud jooned ongi ajas muutumine ja raske tuvastamine.

3. EESTI ÕIGUSRUUMIST TULENEVAD VÕIMALUSED JA PIIRANGUD

Eesti õigusruumis on kaitseväeluure õiguslikud alused reguleeritud kaitseväe korralduse seaduses. Autorite hinnangul on tegemist nii erisuse kui ka õigusliku killustatusega, kuna kahe teise julgeoleku- ja/või luurefunktsiooni täitva KAPO ja VLA õiguslik regulatsioon on sätestatud JAS-is. Lisaks on osa kaitseväeluure läbiviimist reguleerivaid õigusnorme samuti JAS-is, näiteks parlamentaarse järelevalve küsimused. KKS § 42 lg 1 sätestab, et kaitseväeluure teostamist ja tegevust koordineerib JAS § 10 lg 1 nimetatud komisjon. Sama sätte lg 2 kohaselt sätestatakse kaitseväeluurele ülesanded JAS § 9 lg 2 nimetatud riigi julgeolekuteabe kogumise ja analüüsimise kavas. KKS § 42 lg 3 alusel teostab riigikogu julgeolekuasutuste komisjon järelevalvet kaitseväeluure üle, ent julgeolekuasutuste komisjoni tööd valdavalt reguleerib JAS § 36 (Julgeolekuasutuste seadus, 2000). Lisaks on teabe kogumisel kasutatavad luurevolituste sisu pigem täpsemalt ära defineeritud JAS-is. Oluline on välja tuua, et viimased KKS-i redaktsioonid on siiski täpsustanud volitusi kaitseväele spetsiifilisemalt.

Oma olemuselt ja funktsioonilt sarnaneb LuK julgeolekuasutusega, ent hetkel reguleerib kaitseväeluuret, kaitseväe üldist ülesehitust ja toimimise printsiipe kirjeldav eriseadus.

Artikkel keskendub kaitseväeluure riigisisese julgeoleku meetmete pädevusele, st varasemalt välja toodud julgeolekuluurele, mida viiakse läbi Eesti Vabariigi territooriumil, et tuvastada ja ennetada riigisiseseid ohte. Selline tegevus võimaldab vältida ja vähendada võimalike ohtude realiseerumisest tekkinud negatiivseid tagajärgi kaitseväele kui ka Eesti laiemale julgeolekule.

Kaitseväeluure üldised alused on reguleeritud KKS § 36 lg 1, mis sätestab, et kaitseväeluure on teabe kogumine ja töötlemine Kaitseväe poolt (Kaitseväe korralduse seadus, 2008).

Kaitseväe riigisisesed julgeolekulised pädevused tulenevad KKS § 36 lg 1 p 3, 5 ja 6. Need kolm punkti sätestavad kaitseväeluure riigisisese töövaldkonna, mis ongi käesoleva artikli esemeks:

> 3) riigi vastu suunatud luuretegevuse ennetamise või tõkestamise riigisaladuse ja salastatud välisteabe seaduses ettenähtud juhtudel ja korras;
>
> 5) taustakontrolli tegemine, mis on täpsemalt reguleeritud alates KKS § 41^3 – 41^{10};
>
> 6) kaitseväe julgeolekuala kaitse.

Luureasutuste kooskõlastatud tegevuse ja adekvaatse infopildi huvides on seadusandja näinud ette seadusandlikud võimalused osaleda julgeolekuasutuste töös kui ka taotleda ametiabi. KKS § 39 lg 1 näeb kaitseväele ette võimaluse VLA-lt saada ametiabi JAS § 23, 25 ja 26 sätestatud volituste rakendamise osas. Eelmainitud volitused on JAS § 23 variandmete ja konspiratsioonivõtete kasutamine, § 25 sõnumi saladuse õiguse piiramine, ning JAS § 26 reguleerib kodu, perekonna- või eraelu puutumatuse õiguse piiramist (Julgeolekuasutuste seadus, 2000). Ametiabi osutamisel on kaks olulist piirangut, st KKS § 39 lg 1 kohaselt tohib ametiabi taotleda ainult riigi sõjalise kaitsmise eesmärgil ehk KKS § 36 lg 1 p1 sätestatud eesmärgil, mis on olemuselt suunatud Eestile vaenulike välisriikide poolt loodud ohu tõrjumiseks. KKS § 39 lg 2 tuleneb küll piirang, mis sätestab, et abi antakse juhul, kui teabe kogumine muul õiguspärasel viisil ei ole võimalik või oleks ebaproportsionaalselt raske ning kogutav teave on riigi sõjaliseks kaitsmiseks vältimatult vajalik. Ehk siis paratamatult asetub kaitsevägi n-ö väiksema venna rolli, kus ta peab riigisiseselt paluma abi nende toimingute teostamiseks, milleks tal on välisriigis pädevus olemas ja mis on ometi lahutamatult seotud vajadusega tagada valmistumine riigi sõjaliseks kaitsmiseks.

Puuduliku regulatsiooni ilmekas näide on julgeolekuluure piiramine üksuste julgeoleku tagamiseks. KKS § 36 lg 2 sätestab ka piirangu, et missioonil viibiva üksuse kaitseks ei tohi teavet koguda või töödelda Eesti kodaniku kohta, välja arvatud kaitseväkke kandideerija, teenistuja, töötaja või julgeolekualale juurdepääsu taotleva isiku kohta.

Eelmainitud sätte avamine on oluline, kuna formaalne tõlgendus seab hübriidohu ennetamisel piirangu, sest teavet ei koguta Eesti kodaniku kohta. Sõjalise operatsiooni piirkonnas terrorikuriteo toimepanemise kavatsusega viibiv Eesti kodanik võib arusaadavalt kujutada missiooniüksusele ohtu, kuid kaitseväeluurel ei ole võimalik iseseisvalt ja kiiresti tuvastada või hinnata eelmainitud isikust lähtuvaid ohte. Ilmestamiseks toovad autorid teoreetilise näite: Eesti kodanikust ja mittekodanikust resident reisivad terrorikuriteo toimepanemise eesmärgil Malisse. Kui väekaitse eest vastutav LuK saab selle kohta teabe, siis formaalselt ei tohiks ilma kahtlusaluselt Eesti kodanikult saadud loata tema kohta teavet koguda ega ka näiteks teda varjatult baasi ehk julgeolekuala vahetus läheduses jälgida. Samas puudub taoline piirang mittekodanikust residendi osas. Eriti kurioosne oleks olukord, kui mõlemad isikud liiguksid julgeolekuala vahetus läheduses koos ja teoreetiliselt peaks Eesti kodanik andma iseenda varjatud jälgimiseks loa, tuvastamaks, kas ta ikka soovib oma seljakotis olevat lõhkeseadeldist baasi väravasse paigaldada. Teatavasti on terrorirühmitustega ühinenud nii Eesti kodanikke kui ka Eesti mittekodanikest residente. Samas puuduks selline teabekogumise piirang, kui Eesti kodanikku oleks kaitseväeluurel vajalik jälgida selleks, et hankida teavet sõjalise operatsiooni läbiviimise kohta. Vaevalt et seadusandja eesmärk oli panna sisuliselt väekaitse funktsioon VLA-le, kes on pädev teostama vastuluuret missiooniüksuste kaitseks. Lisaks kerkib küsimus, kas on üldse otstarbekas jagada missiooniüksuste vastuluure ja julgeolekuülesandeid mitme asutuse (LuK ja VLA) vahel.

Samuti on kurioosne piirang, mis annab LuK-le välisriigis volituse kuulata pealt sidekanalite kaudu peetavaid kõnelusi, välistades siiski asukohas toimuvate kõneluste salvestamise, sest mõlemad tegevused piiravad võrdselt sõnumisaladust. Veelgi enam, Eesti kohus ei saakski anda luba sõnumisaladuse piiramisele välisriigis. Igal juhul oleks kaitseväe luuraja teise riigi territooriumil tegutsedes asukohariigi seaduse vaatest kurjategija. Sellest johtuvalt on autorite seisukoht, et välisriigis teabe kogumisele seatud detailsed piirangud ei kanna endas reaalset eesmärki tagada tegevuse seaduslikkus. Asjaolu, et luurevolitusi on KKS-is püütud kirja panna oluliselt detailsemalt kui JAS-is, ongi autorite hinnangul kaasa toonud õiguslike lünki või vastuolulisi regulatsioone. Võrdluseks sätestab Ühendkuningriigi välisluuret reguleeriv *Secret Intelligence Service Act* artikkel 7, et kui isik paneb väljaspool Briti saari asjaomase ametkonna loal tegutsedes toime teo, millele võib järgneda kriminaalvastutus, siis ei võeta teda selle loa tõttu vastutusele (Secret Intelligence Service Act, 1994). Nimetatud sõnastus kannab endas mõlemat eesmärki; ühelt poolt antakse tegutsemiseks luba pädeva ametkonna poolt, teisalt ei piirata luureametnike tegevust sisuliselt tarbetute nõuetega. Siinkohal on oluline juhtida tähelepanu, et karistusseadustik kehtib ka välisriigis teenistuskohustusi täitva kaitseväelase suhtes. Kuna artikkel keskendub kaitseväeluure riigisisestele ülesannetele julgeoleku tagamisel, ei ava autorid seda teemat sügavamalt.

3.1. Riigi vastu suunatud luuretegevuse ennetamine või tõkestamine riigisaladuse ja salastatud välisteabe seaduses ette nähtud juhtudel ja korras

Kaitseväeluure esimene töövaldkond riigisisese julgeoleku tagamisel on riigi vastu suunatud luure ennetamine või tõkestamine riigisaladuse ja salastatud välisteabe seaduses ette nähtud juhtudel ja korras vastavalt KKS § 36 lg 1 p 3 (Kaitseväe korralduse seadus, 2008). Riigisaladuse kaitse esmane ja laiem eesmärk on takistada kõrvaliste isikute ligipääsu juurdepääsupiiranguga infole. See on otseselt seotud kaitseväe julgeoleku aluseks oleva teabe julgeoleku tagamise funktsiooniga. Vaenuliku luuretegevusega võivad tegeleda nii Eesti kodanikud kui ka residendid, kes üritavad saada ligipääsu tundlikule teabele. Lisaks ei tohi unustada julgeolekuohtu, mis võib lähtuda kaitseväe enda teenistujatest või töötajatest, kelle on värvanud vaenulik luureteenistus või riigiväline organisatsioon.

KKS § 36 lg 1 p 3 tuleb vaadelda koos RSVS § 22 lg 1, 2 (Riigisaladuse ja salastatud välisteabe seadus, 2007) ja kaitseväe põhimääruse § 13 lg 2 p 5 ja 6 (Kaitseminister, 2022). RSVS § 22 lg 1 kohaselt korraldab kaitseväes ja kaitseliidus riigisaladuse ja salastatud välisteabe kaitset LuK, mille pädevus tuleneb kaitseväe põhimääruse § 13 lg 2 p 5. RSVS § 22 lg 2 määrab ära ülesanded, mida peab LuK täitma riigisaladuse kaitsel. Põhimääruse § 13 lg 2 p 6 sätestab LuK järelevalve kohustuse riigisaladuse ja salastatud välisteabe seaduses ja selle alusel antud õigusaktide nõuete täitmise üle. Täpsemalt on LuK poolt kaitstav teave reguleeritud riigisaladuse ja salastatud välisteabe kaitse korras, mis sätestab ära riigisaladuse alaliigid, nt riigikaitse ja infrastruktuuri riigisaladus (Vabariigi Valitsus, 2021).

RSVS § 16 lg 5 ja 6 seostub personali julgeolekuga, mille eesmärgiks on maandada nii personalist lähtuvaid kui ka personalile suunatud ohtusid.

3.2. Riigi vastu suunatud luuretegevuse ennetamisel või tõkestamisel kasutatavad vastuluurevolitused

Volituste analüüsist selgub, et riigisiseselt on LuK õigused vaenuliku luuretegevuse ennetamisel piiratud.

Luurevolituste analüüsis keskenduvad autorid kõige tähtsamatele õigustele riigisisese julgeoleku tagamise kontekstis. KKS § 37 lg 1 alusel on võimalik kasutada signaalluure volitust. Selline võimalus võib osutuda vajalikuks, kui riigisisene asümmeetriline oht kasutab suhtlemiseks väljaspool üldkasutatavat Eesti vabariigi territooriumil asuvat elektroonilise side võrku. Piirangu mõistes tähendab õigusnorm seda, et Eesti vabariigi territooriumil asuvas üldkasutatavas võrgus edastatavaid või levivaid signaale ei

ole LuK-l võimalik koguda ning kaitsevägi peaks pöörduma ametiabi taotlusega julgeolekuasutuse poole. KKS § 37 lg 1 p 3 kohaselt on LuK-l võimalus teha isikuandmete päringuid erinevatesse andmekogudesse ning hinnata juurdepääsupiiranguta või juurdepääsupiiranguga info põhjal, kas isik võib kujutada julgeolekualast ohtu.

KKS § 37 lg 2 alusel on väljaspool Eesti Vabariigi territooriumi tegutsemiseks võimalik isikuid küsitleda, kaasata neid salajasse koostööse, kasutada variandmeid ja konspiratsioonivõtteid, sh teeselda eraõiguslikku juriidilist isikut, tema struktuuriüksust või organit või äriühingu filiaali ning kasutada variisikut. Selle sätte kohaselt on LuK-l võimalik ette valmistada välismaal toimuvaid luureoperatsioone Eesti vabariigi territooriumil ning luua endale teabe kogumiseks sobiv kattevari. Riigisisese asümmeetrilise ohu kontekstis on see relevantne õigus, sest võimaldab teavet koguda välisriigist juhitud mitteriiklike ohtude kohta, nt 2014. aastal Krimmis ja Ida-Ukrainas Venemaa Föderatsiooni juhitud võitlejad (Westerlund & Norberg, 2016). Eesti Vabariigis sarnase liikumise tekkimise korral oleks kaitsevägi üks institutsioonidest, mida võidakse kasutada eelmainitud asümmeetrilise ohu neutraliseerimisel ning seetõttu oleks vaja koguda teavet sarnast tüüpi ohtude võimekuse kohta ka välismaal.

KKS § 37^1 lg 4^2 p 3 ja lg 4^4 koosmõjul tekib salajase kaastöötaja volituse rakendamise osas vastuolu, sest Kaitsevägi peab KKS § 37^1 lg 4^4 alusel teavitama KAPO-t oma salajase kaastöötaja varjatud jälgimise otsusest. Varjatud jälgimine on antud juhul vajalik, et hinnata salajase kaastöötaja sobivust ja usaldusväärsust. Käesolev õigusnorm tähendab sisuliselt seda, et kaitsevägi peab informeerima KAPO-t salajase kaastöötaja olemasolust ning seeläbi suurendab teadjate ringi. KKS § 37^1 lg 2 järgi on salajast koostööd tegema kaasatud isik, kelle seotus kaitseväega ei ole kolmandate isikutele teda (Kaitseväe korralduse seadus, 2008). Seega on nimetatud regulatsioon olemuslikult kaitseväe luure-eesmärke kahjustav kuna erinevalt kahest teisest, luure ja vastuluurefunktsiooni täitvast asutusest, KAPO-st ja VLA-st, on kaitsevägi teatud juhtudel sunnitud paljastama kõige tundlikuma meetodi – inimallika kasutamise – osapoolele, kellel puudub teadmisvajadus. Küsimus ei ole väheses usalduses ega asutuste nn konkurentsis, vaid pelgalt rangelt järgitavas teadmisvajaduse põhimõttes.

Järgmine problemaatiline koht on seotud sellega, et riigisiseselt ei ole võimalik kasutada salajast kaastöötajat riigi vastu suunatud luuretegevuse ennetamisel või tõkestamisel, olles samas pädevuse piires pandud kaitseväe kohustuseks. Kaitseväel on võimalik kasutada salajast kaastöötajat selleks, et kontrollida KKS § 41^3 lg 1 sätestatud isikute tausta (Kaitseväe korralduse seadus, 2008). Sellisel viisil salajase kaastöötaja kasutamise eesmärk on hinnata, kas tegevväelased, ametnikud, töötajad ja teenust osutavad isikud on usaldusväärsed. Salajase kaastöötaja kasutamise laiem võimalus aitaks avastada või kõrvaldada võimalikke rikkumisi riigisaladuse ja salastatud välis-

teabe käitlemisel. Samuti ei ole võimalik kasutada varjatud jälgimise luurevolitust, et ennetada või tõkestada riigisisest vaenulikku luuretegevust. Eeltoodud volituste alusel oleks LuK-l lihtsam tagada kaitseväe juurdepääsupiiranguga teabe julgeolek. Eelmainitud õiguste andmise eesmärk on anda kaitseväele piisavalt õiguslikke vahendeid, et ennetada olukordi, kus kõrvalised isikud pääseksid ligi tundlikule teabele. Vastuoluline on ka olukord, kus taustakontrollil on lubatud kasutada varjatud jälgimist, salajasi kaastöötajaid ning variandmeid ja konspiratsioonimeetmeid, jättes samas välja oluliselt väiksema riivega kontrollitava suhtlusringkonna tuvastamise nn kõnede eristuse näol. Kuigi konspiratsioonimeetmete kasutamine on taustakontrollis kahtlemata vajalik, siis kõnede eristuse puudumine sellest loetelust viitab asjaolule, et seadusandja tasemel ei ole kinni peetud põhiõiguste riive gradatsiooni põhimõttest lubada ka leebem põhiõiguste riive. Nimelt ei ole kõnede eristus erinevalt varjatud jälgimisest KrMS-i kohaselt isegi jälitustoiming. Veelgi kummalisem, et kõnede eristus kui taustakontrolli meede on lubatud näiteks sõjaväepolitseisse, kuid mitte LuK-sse kandideeriva isiku puhul. Tõlgendades KKS § 41[2] grammatiliselt, jõutakse järeldusele, et ajateenija, kes on määratud täitma sõjaväepolitsei ülesandeid, on rangemini kontrollitud, kui salastatud ametikohal teeniv tegevväelane. Kuigi riigisaladuse loa saamiseks teostatav julgeolekukontroll loomulikult maandab mitmeid personali julgeolekuriske, ei tohi tausta ja julgeolekukontrolli samastada. Riigisaladuse loa andmisest keeldumise asjaolud on ammendavalt loetletud RSVS § 32. Viimane on vastuluureline meede, taustakontroll aga tulenevalt KKS § 41[3] mõttest oluliselt laiem, hindamaks isiku sobivust kaitseväeteenistusse.

Autorid on varem välja toonud, et luuretegevuse ennetamise ja tõkestamise eesmärk on tagada teabejulgeolek. Viimase mõiste alla käib ka infosüsteemide turvalisus. Riigisaladuse ja salastatud välisteabe kaitse korra § 8 lg 1 p 16 kohaselt on üheks kaitstavaks objektiks kaitseväe kasutatav sidevõrkude ja töötlussüsteemide koondteave (Vabariigi Valitsus, 2021). Sama § lg 1 p 18 kohaselt on kaitstav ka teave, mis kirjeldab asutusesiseseks kasutamiseks mõeldud teabe töötlemisel kasutatavate sidevõrkude ja töötlussüsteemide turvameetmeid ja ülesehitust (Vabariigi Valitsus, 2021). LuK jaoks tähendavad eeltoodud õigusnormid seda, et tagada tuleb kaitseväe infosüsteemide tundliku teabe julgeolek.

Asümmeetrilist ohtu kujutav vastane võib üritada tungida töötlussüsteemidesse või sidevõrkudesse, et pääseda ligi infole, mis paljastaks kaitseväe kriitilised haavatavused. Lähtudes KKS § 36 lg 1 p 3 tulenevatest luurevolitustest on autorite hinnangul LuK-l raske ennetada või tõkestada riigisisest ohuallikat, mis üritab tungida infosüsteemidesse või kasutada kaitseväe infosüsteeme teabehankeks. Lisaks on kaitse alla jääva teabe kategooriad piiratud ning ei hõlma asutusesiseseks kasutamiseks mõel-

dud teavet ennast, vaid infosüsteemi ülesehitust ja turvameetmeid. Seadusandja antud volitused ei ole antud juhul sobilikud ning kaitseväel on raske täita talle seadusega püstitatud ülesannet. Asutusesiseseks kasutamiseks mõeldud teabe all peavad autorid silmas avaliku teabe seaduse (edaspidi AvTS) § 35 lg 1 loetelus nimetatud riigikaitselist teavet, eriti lg 1 p 3^1 (Avaliku teabe seadus, 2000).

Riigisaladuse kaitse on vaenuliku luuretegevuse tõkestamise mõttes äärmiselt oluline julgeolekufunktsioon. Ka KKS-ist tuleb selgelt välja riigisaladuse kaitse olulisus seadusandja jaoks ja selle tõttu ongi kaitseväele ette nähtud vastuluureliste ülesannete täitmine. Lähtudes LuK-le antud õiguslikest volitustest tähendab riigisiseses võtmes riigisaladuse ja salastatud välisteabe kaitse sisuliselt turvaala kaitsmist. Kaitseväel võib tekkida probleeme riigisiseste julgeolekuohtude operatiivsel ennetamisel, kuna luurevolitused on piiratud. Ühest küljest on see arusaadav, sest KAPO-l on riigisisese vastuluure üldvolitus, ülesanne kaitsta põhiseaduslikku korda ja tõkestada terrorismi. Hoolimata sellest on siiski autorite hinnangul vaja LuK-le anda salajase kaastöötaja kasutamise õigus kõikide talle seadusega pandud ülesannete täitmiseks, et ennetada vaenulikku luuretegevust ja maandada ka riigisiseseid julgeolekuohte täies mahus. Teine murekoht on see, et LuK on sunnitud KAPO-t informeerima salajase kaastöötaja olemasolust, eirates sellega teabejulgeoleku alusprintsiipe, st teadjate ringi laienemisel suureneb ka võimalus, et luureoperatsioon või kaastöötaja isik paljastub. Analüüsi tulemusel selgus ka, et infosüsteemides olev teave võib jääda osaliselt kaitse alt välja ning kaitseväel on raske tõkestada riigisisest küberohtu.

4. JULGEOLEKUALA KAITSE

4.1. Julgeolekuala ja kaitseväe territooriumi mõiste

Julgeolekuala kaitse laiem eesmärk on tagada nii kaitseväe omandis kui ka valduses olevate asjade julgeolek, st see on otseselt seotud luure- ja vastuluuredistsipliini väekaitselise aspektiga. Edukalt toimiv väekaitse, sh tehnika, inventari ja varude valve, on kaitseväe lahingvõime eelduseks. Lisaks on julgeolekuala kaitse eesmärk takistada kõrvaliste isikute pääsemine väeosadesse ja seeläbi ka juurdepääsupiiranguga andmete juurde.

KKS § 36 lg 1 p 6 kohaselt on kaitseväeluure üks ülesanne julgeolekuala kaitseks teabe kogumine ja töötlemine ning volitused selleks KKS § 37 lg 5 alusel sätestatud sama seaduse § 54^1 lg 1 ja 2 (Kaitseväe korralduse seadus, 2008). Eelmainitud sätete kohaselt võib olulise ohu väljaselgitamiseks ja tõrjumiseks kontrollida isikuandmeid erinevatest andmekogudest, sh ka varjatult. Sama § lg 2 p 1 ja 2 kohaselt võib kaitsevägi

kasutada ohu väljaselgitamiseks ja tõrjumiseks variandmeid, konspiratsioonivõtteid ning varjatud jälgimist. Eelmainitud § lg 3 kohaselt otsustab isiku varjatult jälgimise üle, kas kaitseväe juhataja või volitatud struktuuriüksuse ülem, ning varjatud jälgimist võib teostada kuni 24 tundi. Lisaks tuleb kaitseväel eelmainitud sätte alusel teavitada ka KAPO-t (Kaitseväe korralduse seadus, 2008, RT I, 18.06.2021, 7).

KKS § 36 lg 1 p 6 võtmes kasutatavate volituste hindamiseks tuleb kõigepealt lahti mõtestada julgeolekuala mõiste KKS-i raames. KKS § 50 p 1, 2 ja 3 kohaselt on julgeolekualaks:

1) kaitseväe territoorium;
2) kaitseväe laevad, lennuvahendid ja sõidukid;
3) territoorium, mis on määratletud ajutiselt julgeolekualana.

Veel üks oluline moment julgeolekuala mõiste määratlemisel tekib KKS § 52 lg 3 alusel (Kaitseväe korralduse seadus, 2008). Eelmainitud sätte alusel loetakse julgeolekualal viibimiseks ka seda, kui kaitseväe territooriumil, selle kohal või riigikaitselise ülesandega sadamas kasutatakse mehitamata sõidukit.

Kaitseväe territoorium on sätestatud KKS § 53 lg 1 (Kaitseväe korralduse seadus, 2008, RT I, 18.06.2021, 7). Eelmainitud sätte kohaselt on kaitseväe territoorium KKS-i tähenduses kaitseväe alalises valduses olev territoorium. Seaduses toodud mõistest on võimalik välja lugeda, et tegemist on kaitseväe alalises valduses oleva maa-alaga, ent autorite hinnangul on tegemist ringloogikat kasutava definitsiooniga, mis jääb õiguslikus mõttes lõpuks selgusetuseks. Grammatiliselt tõlgendades KKS § 50 p 1, 2 ja 3 ja lähtudes KKS § 53 lg 1 olevast kitsendusest ei hõlma julgeolekuala kaitseväe omandis või valduses olevaid asju ega esemeid. Tavatähenduses on territoorium siiski maa-ala koos seal asuvate esemetega, ent KKS-i raames on tehtud selge kitsendus. Eesti õigusruumis on võrreldav mõiste riigikaitseobjekt, mis on lahti seletatud riigikaitseseaduses (edaspidi RiKS). RiKS § 83 lg 1 kohaselt võib riigikaitseobjekt olla maa-ala, ehitis või seade, mille kahjustamise või hävitamisega kaasneks oht riigi julgeolekule (Riigikaitseseadus, 2015).

Ainukesed erandid on laevad, lennuvahendid ja sõidukid. Julgeolekuala mõiste on konkreetselt seostatud territooriumi või maa-alaga ning mitte asjadega või esemetega. KKS-i seaduse eelnõus seletuskirjas nr 783 on avardatud julgeolekuala definitsiooni ning selles nähakse kaitseväe territooriumi, mille ulatuses peab kaitsevägi tagama seal viibivate isikute, vara ja teabe julgeoleku, kuna eelmainitu vastu tunnevad huvi kuritegelike kavatsustega ja potentsiaalselt vaenulike võõrriikide ülesandel tegutsevad isikud (Riigikogu, 2019, p. 4). Seletuskiri kinnitab eeltoodud lähenemist.

KKS § 50 lähtudes laieneb kaitseväe omandis või valduses olevatele asjadele kaitse ainult juhul, kui need on kaitseväe julgeolekualal, st ajutiselt või alaliselt valduses oleval territooriumil ning liiklusvahendis, laeval või lennukil. See tähendab, et kui asi viiakse julgeolekualalt välja, siis ei ole võimalik enam kasutada KKS-st tulenevaid julgeolekuala kaitseks mõeldud õigusi.

Kaitseväe kasutatavad IT-teenused on otseselt sõltuvad asjadest ehk füüsilistest seadmetest, kus asuvad andmed. Kuivõrd julgeolekuala mõiste on seotud maa-alaga, siis see tähendab, et ka kaitseväe kasutuses olevatele IT-teenustele, sidevõrkudele ja ka serverites olevatele andmetele ei saa julgeolekuala laieneda. Julgeolekuala kaitse saab laieneda eelmainitud teenuseid majutavatele füüsilistele seadmetele, kui need asuvad samuti kaitseväe territooriumil või laevas, lennuvahendis või sõidukis. Riigisaladuse ja salastatud välisteabe kaitse peatükis leidsid autorid, et ka KKS § 36 lg 1 p 3 koosmõjus riigisaladuse ja salastatud välisteabe kaitse korra § 8 lg 1 p 16 ja 18 ei ole võimalik lõpuni kaitsta kaitseväe sidevõrkudes või töötlussüsteemides olevat infot (Vabariigi Valitsus, 2021).

Autorid peavad vajalikuks rõhutada uuesti, et julgeolekuala ei laiene IT-teenustele või muule IT-seotud vahenditele, sh andmetele. Ainuke vahe võib tuleneda sellest, et kas asi, nt töötajale antud sülearvuti, asub füüsiliselt julgeolekualal ning isegi sel puhul ei pruugi kaitse laieneda IT-teenustele. Arvestades tehnika arengut ja kaugtöö populaarsust, siis on autorite hinnangul tekkinud õiguslik lünk. Kaitseväe IT-seadmetele ei laiene julgeolekuala mõiste, kui teenistuja või töötaja teeb sellega tööd oma elukohas ning kaitseväel ei ole seadusest tulenevat õigust kaitsta oma seadet ega selles asuvat infot. Kaitseväe sisemised reeglid sätestavad teenistuja õigused ja kohustused, ent see siiski ei garanteeri ega võimalda täpselt kontrollida, kas kõrvaline isik pääseb seadmele või selles olevale juurdepääsupiiranguga infole ligi. Asümmeetrilise ohu jaoks pakub see võimaluse pääseda tundlikule infole ligi. LuK-l on eeltoodu tõttu keeruline tagada teabejulgeolekut ning välistada kõrvaliste isikute juurdepääs infole. KKS § 53 lg 1 sätestatud territooriumi mõiste on ajale jalgu jäänud ning ei arvesta tänase päeva IT-lahendustega.

Taustakontrolli õiguslikus analüüsis tõid autorid välja, et kaitseväel on keeruline kui mitte võimatu teha taustakontrolli IT-teenuse pakkujatele, kes ei tule oma teenust füüsiliselt julgeolekualale osutama. Sama õiguslik lünk ja sellest tulenev oht realiseeruks juhul, kui kaitseväe sisevõrgu või muude infosüsteemidega ühendatud seadmed asuksid väljaspool julgeolekuala. LuK-l ei ole võimalik lõpuni kontrollida ettevõtja ega sellega seotud isikute tausta ning seeläbi maandada riske. Lisaks oleks äärmiselt keeruline tagada seadmete füüsiline julgeolek, kui need oleksid ajutiselt lepingupartneri valduses. Analoogne olukord on ülekantav muudele kaitseväe omandis või valduses

olevatele asjadele, nt relvastus, sidevahendid ja muud varud. Varude all peab autor silmas olukorda, kus kaitsevägi hoiustab asju lepingupartneri laopinnal, nt ravimid.

Üks võimalik lahendus probleemile on see, et kaitsevägi määrab ajutiselt lepingupartneri territooriumi ajutiseks julgeolekualaks lähtuvalt KKS § 54 lg 1 (Kaitseväe korralduse seadus, 2008). Tegemist ei ole hea lahendusega, kuna see on mõeldud üksikjuhtumite tarbeks. Esiteks oleks see nii ettevõtjale kui ka kaitseväele koormav. Teenuse osutaja peaks oma igapäevases töös arvestama, et kaitsevägi kontrollib kõikide isikute liikumist ettevõtja territooriumil. See tähendab, et viimasele tuleb edastada teave kõikidest isikutest, kes tulevad ajutisele julgeolekualale.

Käsitletud probleeme oleks võimalik lahendada, kui laiendada taustakontrolli õigusi juriidilise isiku suhtes ning täpsustada territooriumi mõistet, st julgeolekuala oleks kaitseväe valduses olev territoorium koos seal asuvate esemetega. Seetõttu pakuvad autorid välja KKS-i raames uue võimaliku definitsiooni: *kaitseväe territoorium on käesoleva seaduse tähenduses alaliselt kaitseväe valduses olev maa-ala koos selle juurde kuuluvate esemetega*. Eelnev mõiste siiski ei hõlma infosüsteeme või selles liikuvat teavet; need saaks lisada julgeolekuala nimistusse. Selline lähenemine looks täiendava võimaluse kaitsta juurdepääsupiiranguga teavet. Omaette küsimus on siiski, kuidas praktikas kontrollida ja kaitsta töötlussüsteemides olevat infot, kui IKT[1]-seade on väljaspool julgeolekuala, nt tegevväelase või töötaja kodus. Sellisel juhul peab kaitsevägi arvestama perekonna ja eraelu puutumatuse põhimõttega ja rangelt hindama, kas ja kui palju on seda võimalik üldse riivata. Eelmainitud küsimusele vastamine väärib eraldi uurimist, kuid eelpool kirjeldatu kinnitab veel kord, et kaitseväe julgeolekukorraldus on seadusandlikult poolikult lahendatud ning võrreldes KAPO ja VLA-ga sätestatud ebavajaliku detailsusastmega, mis takistab paindlikku lähenemist muutuvale julgeolekuolukorrale ja seab LuK ebavõrdsesse seisu.

4.2. Julgeolekuala kaitseks kasutatavad volitused

Riigisiseste meetmete paremaks võrdluseks on kajastatud ka kaitseväe õigused väljaspool Eesti vabariiki ja rahvusvahelise sõjalise operatsiooni raames. Selline käsitlus aitab paremini mõista riigisiseste volituste piiranguid.

KKS § 52 lg 1 sätestab, et julgeolekualal viibimiseks on vaja kaitseväe luba ning KKS § 55 lg 1 p 1–3 sätestab, et kaitsevägi võib kinni pidada isiku, kelle kohta on põhjendatult alust arvata, et ta:

---

[1] Infokommunikatsioonitehnoloogia

1) viibib julgeolekualal ebaseaduslikult,

2) on julgeolekualale sisenemisel või julgeolekualal toime pannud süüteo või

3) ohustab oma käitumisega ennast või teisi.

Varasemalt toodud KKS § 54[1] lg 1 kohaselt võib olulise ohu väljaselgitamiseks ja tõrjumiseks kontrollida isikuandmeid erinevatest andmekogudest, sh ka varjatult. Olemuselt ei erine see kuidagi taustakontrolli või riigi vastu suunatud luuretegevuse tõkestamisel läbiviidavast isikuandmete registrikontrollist. Sama sätte lg 2 p 1 ja 2 kohaselt võib kaitsevägi ohu väljaselgitamiseks ja tõrjumiseks kasutada variandmeid ja konspiratsioonivõtteid, varjatud jälgimist. Seletuskirja nr 783 kohaselt on sellised volitused vajalikud, et kaitsevägi saaks julgeolekuintsidentidele ise vahetult reageerida, hinnata ohtu adekvaatselt, võimalusel ennetada ja mitte sõltuda teistest asutustest (Riigikogu, 2019). Riigisiseses kontekstis peetakse siin silmas eelkõige KAPO-t JAS § 6 tuleneva riigisisese vastuluure peamise läbiviijana.

Lisaks täpsustakse seletuskirjas, mis on julgeolekuala vahetu lähedus. Seletuskirja kohaselt on see julgeolekuala läheduses asuv ala, millelt on võimalik tekitada vahetu või kõrgendatud oht kaitseväe julgeolekule ning üheks hindamiskriteeriumiks on füüsiline nägemisulatus (Riigikogu, 2019, lk 4). Kõrgendatud oht antud kontekstis on korrakaitseseaduse § 5 lg 4 (edaspidi KorS) tulenev mõiste, mida määratletakse kui ohtu isiku elule, kehalisele puutumatusele, suure väärtusega varalisele hüvele või karistusseadustiku 15. peatükis sätestatud I astme kuriteo või 22. peatükis sätestatud kuriteo toimepanemise ohuna (Korrakaitseseadus, 2011). Vahetu oht on KorS § 5 lg 5 tulenev mõiste, mille kohaselt loetakse vahetuks ohuks olukorda, kus korrarikkumine leiab juba aset või on suure tõenäosus, et see kohe toimub (Korrakaitseseadus, 2011). Riigikohus on ka leidnud, et seletuskirjas toodud vahetu kui ka kõrgendatud ohu mõisteid on võimalik defineerida läbi KorS-i (RKPJKo nr 5-19-38, p 75). Julgeolekuala kaitse võtmes peab kaitseväeluure ennetama võimalikke ohu allikaid, mis ohustaksid:

1) julgeolekualal viibivate isikute elule;

2) julgeolekualal viibivate isikute tervist;

3) kaitseväe omanduses või valduses olevat vara.

Karistusseadustiku (edaspidi KarS) 15. peatükis sätestatakse riigivastased süüteod, nt KarS § 232 lg 1 riigi reetmine füüsilise isiku poolt ning KarS 22. peatükis sätestatakse üldohtlikud süüteod, mille näidetena võib käsitleda KarS § 414 lg 1 lõhkeaine ebaseaduslikku käitlemist või KarS lg 415 lg 1 lõhkeaine, lahingmoona ja nende olulise osa ebaseaduslikku käitlemist (Karistusseadustik, 2001). Eelmainitud süüteod on riigisisese julgeoleku meetmete kontekstis relevantsed, kuna käsitlevad süütegusid,

mida asümmeetrilist ohtu kujutavad isikud või organisatsioonid võivad toime panna kaitseväelaste või kaitseväe vara suhtes. Asümmeetrilist ohtu kujutav isik võib üritada mõjutada kaitseväe personali toime panema KarS 15. peatükis või 22. peatükis sätestatud süütegusid.

Julgeolekuala turvalisuse tagamise võti peitub ennetavas riskide maandamises ning mitte mõjutamise fikseerimises või tagajärgede uurimises. Eeltoodu võtmes peab LuK-l olema võimekus ise koguda ja jagada kaitseväele infot kõikvõimalike ohtude kohta. Kindlasti jagavad ka teised julgeolekuasutused infot kaitseväega KKS § 41 lg 1 ja 2 sätestatud alustel, ent teiste abile ei ole võimalik lootma jääda, kuna peavastutaja nimetatud ohtude tõrjumisel on kaitsevägi ise.

Seletuskirjast tulenevalt on julgeolekuala kaitse seotud ikkagi kaitseväe valduses oleva territooriumi lähiümbrusega, st võimalikud luureoperatsioonid ei tohi toimuda sellest väga kaugel. Ainuke erisus, mis eksisteerib, tuleneb KKS § 52 lg 3, mille kohaselt mehitamata sõiduki käitleja viibib julgeolekuolekualal, kui tema kontrollitav sõiduk on samuti julgeolekualal. Kaitse ulatus sõltub seega otseselt käitleja füüsilisest asukohast.

Esimene meede, mida saab kasutada julgeolekuala kaitsel, on KKS § 37 lg 1 p 5 avalikest allikatest kättesaadav info, ent selle kasutegur on väike, kuna asümmeetrilist ohtu kujutav isik pigem ei levita avalikult oma plaani julgeolekuala mõjutada (Kaitseväe korralduse seadus, 2008). Järgmine meede on KKS § 54^1 lg 1 sätestatud isikuandmete registrikontroll, ent normi sõnastuses on üks piirang, st isikuandmeid võib kontrollida olulise ohu väljaselgitamiseks ja tõrjumiseks. Oluline oht viitab käesolevas kontekstis sellele, et isiku tegevus peab mingil moel olema ohtlikkuse poolest silmatorkav. Käesolevat meedet ei ole võimalik rakendada isiku suhtes, kelle käitumine ei tekita esialgsel hinnangul olulist ohtu või kelle osas ei ole kaitseväel eelinfot. Igapäevasest elust on hea näide loodushuvilised inimesed, kes käivad tihti väeosade või õppustel osalevate üksuste ligidal vaba aega veetmas. Samuti võib kaitseväe julgeolekualal toimuva vastu huvi tundev isik tulla väeosa pääsla juurde ning vaadelda julgeolekuala, ent kaitseväel on KKS-i alusel raske reageerida sellise tegevuse peale, kui antud isiku tegevus ei kujuta sätte mõistes olulist ohtu. Kaitsevägi saab käesoleval juhul ära fikseerida olukorra ja PPVS-ist ja KorS-ist tulenevalt paluda politsei- ja piirivalveametil isik tuvastada. Oluline oht eeldaks juba vähemalt julgeolekuala jäädvustamist, ent isegi siis on keeruline tõestada inimese tahtlust jäädvustada kaitseväele kuuluvat territooriumi või seal toimuvat, sest see eeldaks salvestamisvahendi füüsilist kontrolli. Pääsla või territooriumi ligiduses viibimine ei ole iseenesest keelatud ja asustatud alal on keeruline silmas pidada kõiki territooriumist möödujaid.

KKS § 55 lg 1 p 1 kohaselt saab kaitsevägi kinni pidada julgeolekualal ilma kooskõlastuseta mehitamata sõidukit käitleva isiku tulenevalt KKS § 52 lg 3. Käesoleval juhul ei oma tähtsust see, kui kaugel on sõiduki käitleja julgeolekualast, vaid loeb asjaolu, et mehitamata sõiduk on kaitseväe territooriumil või selle kohal. Tekib kummaline olukord, kus ohtu kujutav isik võib luurata julgeolekuala territooriumi ümber jalutades, ent kui ta kasutab julgeolekuala kohal mehitamata õhusõidukit, siis on võimalik ta kinni pidada selles kohas, kust ta drooni lennutab. Sättest tuleneb justkui volitus kinni pidada drooni kooskõlastuseta käitlev isik ükskõik kus, ent muud julgeolekuala kaitseks toimuvad operatsioonid peavad toimuma territooriumi vahetus ümbruses. Praktikas tähendab see siiski seda, et kinnipidamine toimuks julgeolekuala ligidal, sest kaugel asuva ohuallikale reageerimine võtab aega ning suure tõenäosusega õnnestub mehitamata sõiduki käitlejal enne lahkuda. Autorite hinnangul on ka seadusandja tahe pigem see, et mehitamata sõidukit käitleva füüsilise isiku kinni pidamine toimuks siiski julgeolekuala vahetus ümbruses.

KKS § 54^1 lg 2 p 1 ja 2 annavad võimaluse kasutada variandmeid, konspiratsioonivõtteid ning varjatud jälgimist. Eeltoodud meetme rakendamine on sõltuv kahest asjaolust, st edasilükkamatu vajadus ning kõrgendatud oht. Autorid on varasemalt toonud välja, mida need mõisted tähendavad ning alati ei pruugi asümmeetrilist ohtu kujutava isiku tegevus vastata eeltoodud asjaoludele. Variandmete ja konspiratsioonivõtete volituse olemasolu on mõistlik, sest võimaldab kaitseväe teenistujatel varjata seda, et nad on tuvastanud kõrgendatud ohu allika ning asunud rakendama vastumeetmeid. Varjatud jälgimise teostamise volitus on samuti positiivne, ent praktika käigus võib selle rakendamine olla keeruline, kuna õnnestunud operatsiooni jaoks on vaja eelinfot ja planeerimisvõimalust. Lisaks on varjatud jälgimise operatsiooni korraldamine ressurssi ja aega nõudev tegevus. Täiendava takistuse seab KKS § 54^1 lg 3 tulenev ajapiirang, mis ei võimalda ette planeerida pikemaid operatsioone ohtude täpsemaks tuvastamiseks. Olukorras, kus on tõsisem oht või tuleb täiendavalt teavet koguda, tekib ajapiirangu tõttu lisaprobleeme. Sellises olukorras peaks KAPO üle võtma teise luureasutuse poolelioleva operatsiooni, mis eeldab täiendava ressurssi eraldamist ja sündmuse asjaoludega kurssi viimist.

Sellise juhtumi korral oleks kaitseväel abi hoopis salajase kaastöötaja rakendamise volitusest. Julgeolekualad on üldiselt staatilise iseloomuga ja asuvad asustatud alade juures, erand on KKS § 50 p 2 sätestatud sõidukid, laevad, lennuvahendid. Julgeolekuala ligidal elavate kohalike inimeste kasutamine kaastöötajatena aitaks tegelikult kaitseväel tuvastada võimalikke hübriidohte, kes üritavad kohalikku keskkonda sulanduda. Samuti aitaks see kokku hoida varjatud jälgimise kuluvat ressurssi.

Kaitseväel on võimalik julgeolekuala kaitset KKS § 54[1] lg 1 ja 2 alusel läbi viia ning on võimalik ebaseaduslikult julgeolekualal viibivad isikud kinni pidada lähtudes KKS § 55 lg 1 p 1–3. Muret tekitab siiski asjaolu, et julgeolekuala kaitsmisel õiguslike volituste rakendamist mõjutab vananenud ja ebaselge kaitseväe territooriumi mõiste, mis tuleneb KKS § 53 lg 1.

KOKKUVÕTE

Artikli eesmärk oli tutvustada lugejale kaitseväeluure riigisiseseid julgeoleku tagamise meetmeid ning võimalikke lünkasid kaitseväeluuret puudutavas seadusandluses. Õigusnormide lünkade tuvastamiseks ja ilmestamiseks toodi erinevaid näiteid riigisisestest julgeolekuohtudest.

Autorite hinnangul tekib ebakõla kaitseväeluurele püstitatud ülesannete ja nende täitmiseks antud õiguste vahel. Eelmainitud ebakõla tuleneb sellest, et seadusandja poolt seatud ülesanded eeldavad tegelikult suuremaid õiguseid võrreldes kehtivate volitustega. KKS ei võimalda kehtival kujul kaitseväeluuret vajalikul tasemel läbi viia, et tegeleda riigisiseste julgeolekuohtudega. Õigusselguse vaatenurgast lähtudes on probleem, et LuK tööd reguleerivad õigusnormid paiknevad mitmes eriseaduses.

Kehtiva seadusandluse kohaselt tähendab LuK-le riigisaladuse ja salastatud välisteabe kaitse st luuretegevuse tõkestamine praktikas turvaala kaitsmist. Lisaks ei ole kaitseväeluurel võimalik rakendada täies mahus salajase kaastöötaja luurevolitust luuretegevuse tõkestamisel. Teine julgeolekuasutus kontrollib LuK salajast kaastöötajat ning riigisiseselt ei ole võimalik luuretegevuse tõkestamisel eelmainitud kaastöötajat kasutada. Täiendavalt on töötlussüsteemides oleva info kaitses lüngad, kuna potentsiaalseid riigisiseseid ohte ei ole võimalik avastada ning kogu juurdepääsupiiranguga info ei ole tegelikult kaitstud.

Julgeolekuala kaitset raskendab aegunud kaitseväe territooriumi mõiste, mistõttu jäävad kaitse alt välja infosüsteemid ja nendes olev juurdepääsupiiranguga teave. Julgeolekuala kaitseks varjatud jälgimise teostamine nõuab ressurssi, on piiratud ajalise kestusega ning nõuab edukaks läbiviimiseks eelinfot ohu kohta. Lisaks ei ole võimalik kasutada riigisiseselt salajase kaastöötaja volitust. Ülaltoodu tõttu on käesoleval hetkel võimalik tegeleda ainult osa riigisiseste ohtudega.

Siiski on KKS-ist võimalik välja lugeda seadusandja tahe, et LuK funktsioon oleks sarnane teiste julgeolekuasutustega, st täidaks määratud luure- ja vastuluure ülesandeid. Õiguslikust vaatenurgast oleks kaks võimalikku lahendust:

1) kaitseväeluure volituste laiendamine KKS-is;

2) kaitseväeluure valdkonna reguleerimine JAS-is.

Kaitseväeluure volituste laiendamine KKS-is

LuK volituste laiendamine KKS-is esmalt tähendaks seda, et LuK tegevust reguleeriks edaspidigi KKS ning sellisel puhul säilib senine luure- ja julgeolekuasutuste õigusliku regulatsiooni killustatus. Autorite hinnangul tuleks täiendada kaitseväeluure valdkonda alljärgnevate volitustega.

KKS § 36 lg 1 p 3 sätestatud riigisaladuse kaitsel tuleks lubada salajase kaastöötaja luurevolituse kasutamine riigisiseselt vaenuliku luuretegevuse tõkestamiseks. KKS § 37^1 lg 4^2 p 3 ja lg 4^4 koosmõjul peab kaitsevägi teavitama KAPO-t salajase kaastöötaja varjatud jälgimise otsusest ning seetõttu tekib vastuolu KKS § 37^1 lg 2. Eeltoodud sätte kohaselt on salajase kaastöötaja seotus kaitseväega varjatud kolmandate osapoolte eest ning selle tagamiseks peaks salajase kaastöötaja sobivuse kontroll jääma kaitseväe teada. Täiendavalt tuleks kaaluda varjatud jälgimise õiguse andmist kaitseväele, et tõkestada vaenulikku luuretegevust. Töötlussüsteemide vastaste rünnete ennetamiseks aitaksid eelmainitud volituste kasutamise riigisisesed võimalused.

Julgeolekuala kaitse läbiviimise lihtsustamiseks oleks vajalik uuesti sõnastada kehtiv KKS § 53 lg 1 sätestatud kaitseväe territooriumi mõiste, mis kahjuks on segane ja vananenud. Uus territooriumi mõiste oleks: *kaitseväe territoorium on käesoleva seaduse tähenduses alaliselt kaitseväe valduses olev maa-ala koos selle juurde kuuluvate esemetega*. Laiema teabejulgeoleku tagamise nimel tuleks lisada infosüsteemides olev juurdepääsupiiranguga teave KKS § 50 toodud julgeolekuala nimistusse. KKS § 36 lg 1 p 3 ei hõlma kogu juurdepääsupiiranguga teavet ja selle kaitset. § 54^1 2 toodud õigustele tuleks lisada salajase kaastöötaja rakendamise volitus, kuna see annaks võimaluse kasutada varjatud jälgimise peale kuluvat ressurssi otstarbekamalt. KKS § 54^1 lg 3 sätestatud ajapiirangut tuleks pikendada, et LuK saaks tuvastada ohu ning tekkinud olukord ei tarbiks asjatult teise julgeolekuasutuse ressurssi.

Kaitseväeluure valdkonna reguleerimine JAS-is

Kaitseväeluure valdkonna õiguslikul reguleerimisel JAS-is on võrreldes jätkuva KKS-i täiendamise ja parendamisega võrreldes tugevad pooltargumendid. KKS § 36 lg 1 p 3, 5 ja 6 sätestatud teabe kogumise ja töötlemise ülesannetest nähtub seadusandja ootus, et kaitseväeluure funktsioon ja vastutus oleks võrdne julgeolekuasutuse ülesannetega. Õigusnormides sätestatud ülesannete edukas täitmine eeldab paratama-

tult vastuluureliste ja laiendatud julgeolekuluureliste tegevuste läbi viimist. Praegu eksisteeriva õigusliku killustatuse tõttu reguleerib kaitseväeluure valdkonda samaaegselt kaks eriseadust KKS-i ja JAS-i kujul. Selle tõttu on samasisulised luurevolituste mõisted defineeritud kahes erinevas seaduses, seejuures erinevat ja mõneti vastuolulist lähenemist rakendades.

Eeltoodu tõttu näevad autorid ühe variandina reguleerida kaitseväeluure valdkond JAS-is sarnaselt teiste julgeolekuasutuste õiguslike alustega. Üks lahendusviis oleks täiendada JAS § 5 toodud julgeolekuasutuste loetelu järgmiselt: *julgeolekuasutused on kaitsepolitseiamet, välisluureamet ja kaitseväe põhimääruses määratud struktuuriüksus*. LuK oleks sellisel juhul VLA ja KAPO-ga võrdses seisus, kuid ei peaks olema eraldi juriidilise isikuna kolmas julgeolekuasutus. Sarnast lahendust rakendatakse kaitseväe suhtes ka praegu; nimelt on kriminaalmenetluse seadustikus selgelt sätestatud sõjaväepolitsei kui uurimis- ja jälitusasutuse roll. Samas on sõjaväepolitsei jätkuvalt kaitseväe struktuuriüksus, mille funktsioonid väljaspool kriminaalmenetlust reguleerib jätkuvalt KKS. Sellise lähenemise tugevus peitub õigusselguses, sest valdkond ja luurevolitused oleksid ühes seaduses ära sätestatud ning eksisteeriv killustatus ja kaoks tervikpildi hoomamatus. Raske on üheselt väita, mis on seni õigusloomeliselt takistanud valida üheselt mõistetav lahendus, võib-olla on selleks olnud soov vältida kolmanda julgeolekuasutuse tekkimist. Autorid ei ole uurimistöö käigus üheselt mõistetavaid põhjuseid tuvastanud. Praktikas ei ole kaitseväeluurele pandud ülesannete täies mahus täitmine senise lähenemisega võimalik. Tagamaks Eesti valmisolek riigi sõjaliseks kaitseks ka ennetavas faasis tuleb astuda julge samm ja nimetada asju oma õigete nimedega: Eesti vajab spetsialiseeritud ja tugeva julgeolekuluure komponendiga kaitseväeluuret, mida käsitletakse võrdselt kahe teise julgeolekuasutuse, KAPO ja VLA-ga.

SIIM ARTUR JUHT

Kaitseväe teenistuja

E-post: siim.artur.juht@eesti.ee

Siim Artur Juht on lõpetanud Kaitseväe Akadeemia 2021. aastal maaväe õppesuunal. Hetkel omandab Tartu Ülikoolis juriidilist kõrgharidust.

EERIK HELDNA

Maksu- ja Tolliameti tolliosakonna juhataja

E-post: eerik.heldna@eesti.ee.

Eerik Heldna on pikaajalise politseistaažiga julgeolekuekspert ning mh teeninud kaitseväe luurekeskuse ülema asetäitjana julgeolekualal. Alates 2020. aasta maikuust juhib ta Eesti tolli. Ta on lõpetanud Sisekaitseakadeemia kohtueelse uurimise eriala, Föderaalse Juurdlusbüroo (FBI) Akadeemia ning omandanud magistrikraadid nii Tallinna Tehnikaülikooli haldusjuhtimise erialal kui ka Tartu Ülikooli õigusteaduskonnas. Eerik on osalenud mitme seaduse väljatöötamisel ning tegutsenud Ukraina julgeolekuvaldkonna koolitajana.

KASUTATUD ALLIKAD

Avaliku teabe seadus (2000) RT I, 10.03.2022, 4.

Darchiashvili, D., 2018. Russo-Georgian War of August 2008: Clash of Ideologies and National Projects in the Era of Hybrid Warfare. *Sõjateadlane (Estonian Journal of Military Studies),* 8, pp. 12–37.

Development, Concepts and Doctrine Center, 2011. JDP 2-00 = Joint Doctrine Publication 2-00: Understanding and Intelligence Support to Joint Operations. UK Ministry of Defence. [Võrgumaterjal] Leitav: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/311572/20110830_jdp2_00_ed3_with_change1.pdf [Kasutatud 26.08.2022].

Eaton, J. G., 2002. The beauty of asymmetry: An examination of the context and practice of asymmetric and unconventional warfare from a western centrist perspective. *Defence Studies*, 2(1), pp. 51–82.

Gentry, J. A., & Spencer, D. E., 2010. Colombia's FARC: A Portrait of Insurgent Intelligence. *Intelligence and National Security*, 25(4), pp. 453–478.

Harber, J. R. 2009. Unconventional Spies: The Counterintelligence Threat From Non-State Actors. *International Journal of Intelligence and CounterIntelligence*, 22(2), pp. 221–236.

Ilardi, G. J., 2010. Irish Republican Army Counterintelligence. *International Journal of Intelligence and CounterIntellingece*, 23(1), pp. 1–26.

Jaagant, U., 2017. Ebaseadusliku relvaäri kohtuasjas mindi kokkuleppele, süüdistatavaid ootab vangla ja tsiviilhagi. *Delfi*. [Võrgumaterjal] Leitav: https://www.delfi.ee/news/paevauudised/krimi/ebaseadusliku-relvaari-kohtuasjas-mindi-kokkuleppele-suudistatavaid-ootab-vangla-ja-tsiviilhagi?id=78397322 [Kasutatud 26.08.2022].

Julgeolekuasutuste seadus (2000) RT I, 27.05.2022, 30.

Kaitseministeerium, 2017. *Eesti julgeolekupoliitika alused.* [Võrgumaterjal] Leitav: https://www.kaitseministeerium.ee/sites/default/files/sisulehed/eesmargid_tegevused/395xiii_rk_o_lisa.pdf [Kasutatud 26.08.2022].

Kaitseminister, 2022. *Kaitseväe põhimäärus*. RT I, 04.05.2022, 3.

Kaitsepolitseiamet, 2020. *Kaitsepolitseiameti aastaraamat 2019–2020.* [Võrgumaterjal] Leitav: https://kapo.ee/sites/default/files/content_page_attachments/Aastaraamat_2019_2020.pdf [Kasutatud 26.08.2022].

Kaitseväe korralduse seadus (2008) RT I, 18.06.2021, 7.

Karistusseadustik (2001) RT I, 28.04.2022, 27.

Karmon, E., 2005. *Coalitions between Terrorist Organizations: Revolutionaries, Nationalists and Islamists.* Leiden: Martinus Nijhoff Publishers.

Kilcullen, D., 2013. *Mägedest alla: Linnapartisanide ajastu saabumine.* Tallinn: Postimees & Grenader Grupp OÜ.

Korrakaitseseadus (2011) RT I, 06.08.2022, 16.

NATO Standardization Office, 2020. AAP-6 = Allied Administrative Publication (NATO Standardization Office, 2020). [Võrgumaterjal] Leitav: https://nso.nato.int/nso/nsdd/main/standards/ap-details/3154 [Kasutatud 26.08.2022].

Phelan, P., 2011. Fourth Generation Warfare and its Challenges for the Military and Society. *Defence Studies*, 11(1), pp. 96–119.

Rekkedal, N. M., 2006. *Insurgency and Counter-Insurgency: A presentation of Concepts and Problems.* Stockholm: National Defence College.

Riigikaitseseadus (2015) RT I, 10.03.2022, 26.

Riigisaladuse ja salastatud välisteabe seadus (2007) RT I, 06.05.2020, 36.

Riigikogu, 2019. *Kaitseväe korralduse seaduse muutmise seaduse seletuskiri nr 783.* [Võrgumaterjal] Leitav: Riigikogu: https://www.riigikogu.ee/download/13ceb49f-1f09-4640-9042-a286ffbd7ed8 [Kasutatud 26.08.2022]

RKPJKo 19.12.2019, nr 5-19-38, 5.

Ryabikhin, L., & Viktorova, J., 2004. Weapons Transfers as a Soft Security Issue in Eastern Europe: Legal and Illicit Aspects. *European Security*, 13(1), pp. 73–93.

Secret Intelligence Service Act, (1994) [Võrgumaterjal] Leitav: https://www.legislation.gov.uk/ukpga/1994/13/section/7 [Kasutatud 26.08.2022].

Shulsky, A., & Schmitt, G. J., 2013. *Varjatud sõda: sissevaade luureteenistuse maailma.* Tallinn: AS Eesti Ajalehed.

Sildam, T., 2018. Sõjaväeluurele voli juurde – öökull saaks pikemad tiivad. *ERR*, 04.11.2018. [Võrgumaterjal] Leitav: https://www.err.ee/874380/sojavaeluurele-voli-juurde-ookull-saaks-pikemad-tiivad [Kasutatud 26.08.2022].

Szafranski, R., 2002. Centers of Gravity and Asymmetrical Warfare. rmt: *Asymmetric Warfare*. The Royal Norwegian Airforce Academy, pp. 239–265.

United States Army, 2019. ADP 2-0 = *Army Doctrine Publication 2-0 Intelligence*. (2019). Washington, DC: Department of the Army Headquarters. [Võrgumaterjal] Leitav: https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN18344_ADP%202-0%20FINAL%20WEB.pdf [Kasutatud 26.08.2022].

United States Army Intelligence Center and School, 2004. FM 2-0 (2004) = *Field Manual 2-0: Intelligence*. (2004). Washington, DC: Department of the Army. [Võrgumaterjal] Leitav: https://fas.org/irp/doddir/army/fm2-0.pdf [Kasutatud 26.08.2022].

Vabariigi valitsus, 2021. *Riigisaladuse ja salastatud välisteabe kaitse kord.* RT I, 31.12.2021, 22.

Veljovski, G., Taneski, N., & Dojchinovski, M, 2017. The danger of „hybrid warfare" from a sophisticated adversary: the Russian „hybridity" in the Ukrainian conflict. *Defense & Security Analysis*, 33(4), pp. 292–307.

Westerlund, F., & Norberg, J., 2016. Military Means for Non-Military Measures: Russian Approach to the Use of Armed Forces as Seen in Ukraine. *The Journal of Slavic Military Studies*, 29(4), pp. 576–601.