Kasutusvajadused ja huviosalised

- **Milliseid drooniohu stsenaariume teie valdkonnas peamiseks peetakse?** Näiteks kas Lennuameti ja Lennuliiklusteeninduse ASi jaoks on esmatähtis tagada lennuohutus lennuväljade ümbruses või reguleerida droonilubasid; infrastruktuurioperaatoritele (Elering, Elektrilevi, Tallinna Vesi, raudtee, sadamad, lennujaamad) tähendab drooniseire pigem oluliste varade kaitset. Kuidas teie organisatsioon tutvustab enda vajalikke funktsioone ja töövooge üldises CUAS süsteemis?
- **Kuidas näete oma rolli ühise drooniseireplatvormi arhitektuuris?** Kas teie rakendus vajab reaalajas juurdepääsu droonituvastuse andmetele või sobib hilisem ülevaade? Näiteks tööstusrajatis võidakse huvitada vaid droonidest oma objekti kohal, mitte laiemast õhuruumist[1] – kuidas tagada, et ta näeb üksnes relevantset infot?
- **Kas teie organisatsioon on valmis oma olemasolevaid seireallikaid (radarid, RF-tu vastajad, akustilised ja optilised sensorid vms) jagama või integreerima üleüldisesse süsteemi?** PPA eelanalüüsi käigus toodi välja ettepanek suunata kõik eri allikatelt kogutav drooninfovoo ühtsesse keskmasinasse[1]. Kas te näeksite sellist koondamist sobivana, ja millised oleksid teie eelistatud andmejagamise ja ligipääsu tingimused?
- **Uute ja ärilistel eesmärkidel kasutatavate droonide (nt kaubalennud) kontekstis: millised on teie ootused koostööle U-Space'iga?** Samas kui lähitulevikus on plaanis teostada droonikaubavedusid ja moodustada U-Space'i teenused, peab politseiõigus ja seire integreeruma sellesse keskkonda[2]. Kuidas võiks e-politsei (digitaalse järelevalve) toetada seaduslike droonioperatsioonide korraldust ning ebaseadusliku tegevuse avastamist?
- **Kuidas teie arvates peaks kujunema koostöö rahvusvaheliste partneritega (naaberriigid, NATO, EL-i agentuurid) ülapiiriüleste sündmuste korral?** Kas ja kuidas tuleks juhtida korduvaid andmevahetusi näiteks Läti või Soomega planeeritava „Baltic drone wall" kontseptsiooni raames[3][4]?
- **Kuidas saaks teadusuuringute ja innovatsiooni kogukond (ülikoolid, uurimislaborid) kasutada drooniseire andmeid?** Milliseid piiranguid andmekaitse või turvalisus võib seada teadlastele (nt droonide lendude trajektooride või salvestatud piltide kasutamine)? Kuidas sätestada tingimused, et näiteks neutralseid metoodikaid arendav teadlane saaks anonüümseid seireandmeid analüüsida ilma julgeolekuhuve kompromiteerimata?

Sensorivõrgustik ja tehnilised eeldused

- **Milliseid sensoritehnoloogiaid teie valdkond eelistab droonituvastuseks?** Kas tarvitate või plaanite kasutada radareid, raadiosidetuvastust, akustilisi andureid, kaameraid või mobiile võrgusensorivõimalusi (nt 5G võrgusignaalide analüüs)? Kui

jah, siis milliseid täiendavaid nõudeid või sertifikaate (nt SAPIENT-standard) te ootate selliste seadmete puhul? Briti SAPIENT-raamistiku järgi peaks sensorid olema „nutikad" ja AI-ga varustatud ning saates kesksele juhtimissüsteemile eelkõige oluliselt tõlgendatud infot[5][6] – kas see põhimõte kõnetab ka teid?

- **Kas teie olemasolevad infrastruktuurid (nt raadiosidega tsoonid, radarisüsteemid) on droonide tuvastuseks piisavalt tihedad?** Näiteks läbirääkimistel on toodud välja arvutused, et statsionaarseid ja mobiilseid RF-sensoreid peaks olema sadu[7][8]. Kas teil on teavet, kui palju ja mis tüüpi andureid on praegu paigaldatud teie haldusalas, ning kuidas te uute sensorite lisamist planeeriksite?
- **Kuidas käsitleda seniseid tehnilisi kitsaskohti ja katvuse lünki?** Näiteks kui võrgustikul on ala, kus signaalitugevus on madal või haljendite tõttu radari kokkupuude nõrk, kas süsteem peaks andma hoiatusi katvuseaukude kohta? Kui meelitada ehitada selline süsteem olemasolevate radarite ja uuenduste peale, kuidas te kommenteerite spekulatsioone, et näiteks radari kuulutatud ulatus (900 m) võib reaalsuses olla palju väiksem[9]? Kas tulevase süsteemi puhul peaks selliste sensorispetsiifiliste erinevuste suhtes olema ka teknikute või operaatorite väljaõpe?
- **Kui uus tuvastusseade peaks arendusse tulema (nt noorem arendaja pakub UHF-signaali imetamismoodulit), kuidas te sooviksite selle integreerida?** Arendusprojektides tuleb sageli komponentide nimetus jõudnud enne, kui täpsed tehnilised parameetrid on selged[10][11]. Kuidas kavandada süsteemi arhitektuuri nii, et see oleks modulaarne (plug-and-play), toetaks erinevaid sensoreid ja võimalikke uuendusi (nagu SAPIENT-i nõue[12]) ning oleks jätkusuutlik ka juhul, kui mõni tarnija vahepeal kaoks?

Andmevood ja infosüsteemi arhitektuur

- **Kuidas kujuneb droonide tuvastamise infovool üksikust sensorist avale operaatorile?** Kas teie organisatsioon eelistab, et kõik andmed suunataks tsentraalsesse „paksu" serverisse või saadetaks eelnevalt töödeldud hoiatused otse vastutavale isikule? PPA eelanalüüsi raames soovitati, et kõigi sensorivõrkude info jõuaks ühte keskkoordinaatorisse[1][13]. Kas teil on eelistusi selleteemal?
- **Kes peaks olema ühe püsiteenuse või andmekogumispunkti (näiteks pilveserveri või valitsusasutuse serveri) operaator ja hooldaja?** Kas PPA või Lennuamet peaks haldama keskset süsteemi, või võiksid erinevad osapooled (nt Kaitsevägi, tolli- ja piirivalveasutused) luua andmete ristkasutust läbi partnervõrkude[14]? Näiteks ühes vestluses pakuti, et Kaitsevägi võiks oma sensorid ühendada kinnisesse võrku, kuhu põhiserverilt droonialarmid jooksuksid[15]. Kuidas tagada, et eri operaatorid (tsiviil- ja militaarüksused) saavad vastavalt autoriseerimisele andmeid vaadata?
- **Kuidas defineerida juurdepääsuõigused ja hierarhia erinevate andmeliikide jaoks?** Millisel kujul peaks näiteks üks kiirreageerija või hoolsuskeskus nägema drooni andmeid – kas piisaks hoiatusest või on vaja ka lisainfot (nt drooni

positsioon, suund, tunnused)? Transpordiamet võiks lubada droonil lennata kindlal ajal ja kohal, PPA kontrollib lubasid ning osutab salvestatud kontaktandmed[16]. Kuidas sellised litsentsid ja droonikasutuslubade kontrollid infosüsteemis välja näeksid?

- **Milline peaks olema info salvestus ja andmeturve?** Kui midagi juhtub, tuleb analüüsida drooni püüdmise etappi (nt Lennuliiklusteenindusel tuvastusinfo, turvateenistusel allatulistamisinfo). Kui palju aega tuleks salvestada metatavaid andmeid (nt drooni trajektoori, asukoha infot) ja kes nendele ligi pääseb? Samuti – kuidas tagada, et sõjaväe või liitlaste informatsioon ei lekkiks avalikku operatiivvaatesse? Näiteks on Toomemäe radarid NATOs salajased ja andmed hägustatakse enne tsiviiloperaatoriteni jõudmist[17]. Milliseid krüpteerimis- ja anonüümistamismeetmeid te ootate sellise süsteemi arhitektuuris?

Ligipääsud ja jagamispraktika

- **Millised aktuaatorid ja andmevahetusühendused tuleks CUAS-i lõppkasutajatele võimaldada?** Kas eri asutustel (PPA, politseipatrullid, piirivalve, päästeamet, maksuhaldus, toll vm) on vaja otsest juurdepääsu süsteemi veebiportaalile või mobiilirakendusele, kus nad saavad HOIATUSI? Näiteks kui piiril või linnas patrullijuhiks oleva Ljudmilla vahekohtunikule tuleb SMS hoiatusega, kas ta suunatakse seejärel kohe juhtimiskeskusesse[18]? Millised infokihid või -tasemed peavad rakenduses olema (nt lubatud/punktuaalne hoiatus vs täielik droonikinnitus) ja kuidas endine juurdepääsuhierarhia kujuneb?
- **Kes määrab süsteemis rollid ja vastutuse?** Milline on näiteks „peamiseks koordineerijaks" ehk kukesõela (flagship) süsteemi sisselülitamine pärast lubade andmist ning kelle vajadusel süsteemi väljalülitab? Usaldusmudel peaks selge olema: näiteks tööjuht teab, et Kaitseväe taristu tuvastus on ainult seotud kaitseväe vajadustega, samas Sinu huviringe piiravad - mis siis konkreetsetel andmetel kuvatakse[17][16]? Kes peab süsteemi haldama rahuajal ja kes kriisiolukorras (vastavalt riigikaitselistele kohustustele)?
- **Kuidas tagada info rollikeskne varjamine või avalikustamine?** Näiteks, kas radarite piike ja signaalid on alati nähtavad või tuleks kuvada vaid "kaetud ala" abstraktselt, et operatiivkorrapidaja ei näe sensorite täpseid paigutusi[19]. Millised täpsusastmed või metaandmed on lubatud tuvastuse hoiatuses (piloodi teated, piketeave, sobivuse tase)? Kas paigalduse täpsus võiks olla piiratud teabe „üleküllastuse" vältimiseks?
- **Mis juhtub teabelekete või -kuritarvituste korral?** Kes vastutab, kui mõni ametnik või teenusepakkuja kasutab saadud drooniteavet väljaspool ette nähtud eesmärki (nt avaldab saladusi või kuritarvitab piltimaterjali)? Kas süsteem peaks logima kõiki päringuid ning kas uurimise eesmärgil hakkab droonituvastuse info allikale (kas sensorile või ametikohale) tagasijoondamine olema võimalik?

Õiguslikud, eetilised ja privaatsusküsimused

- **Kuidas kajastub eraomandi kaitse drooniseiresüsteemi seadistamisel?** Millised õigusnormid piiravad droonide või kaamerate abil eraomandiga piirkondadesse vaatamist? Näiteks milline on lennutrasside planeerimisel droonidesäte: ega turvamees ei tohi kaudselt salvestada keelualas hoone pealt kaadrit, isegi kui tuvastaks drooni. Kuidas te eristate sõjalis-salajase, elutähtsa ja eravaldusesse jääva teabe kuvamist/kättesaamist?
- **Kuidas reguleerida droonide poolt kogutava video ja isikuandmete kasutust?** Kas näha täpseid koordinaate või ainult "ala, kus droon lendab"? Kuidas tagada näiteks selle, et üks kasutaja ei saaks süstemaatiliselt filmida eraeluasetest ega koguda isikuandmeid (nt näopiirkonnad, numbrimärgid) droonikamera või infrapuna abil? Kas ja kuidas arvestada GDPR-i või muude andmekaitsenõuetega (nt andmete anonüümistamine või keelatud ajaline säilitamine)?
- **Millal loetakse sensorite täpsus liigseks?** Kas on keegi, kes seab ülemise piiri, kui kauguselt või kiirusega droon tuvastatakse? Kui sensorid oskavad eristada inimesi, kirjeautosi või droonitüüpe väga täpselt, kas seda peaks piirama? Millal on oht, et tuvastusseade muutub isikukutsete jälgimisseadmeks? (Näiteks kui ultraheli- või infrapunakaamerad suudavad lugeda relvakoode, kas see on lubatud?)
- **Milliseid turvalisusnõudeid peaks süsteem järgima?** Kas suhtlus drooniseiresüsteemi ja sensorite vahel peab toimuma turvatud VPN-kanalites, spetsiaalsetes sagedusalades või krüpteeritult? Kuidas tehakse järelevalvet, et süsteemi enda turvalisust (küberrünnakute, signaali häkkimiste, infosüsteemi häkkimisohu vastu) pidevalt hinnatakse ja uuendatakse?

Eraomandi kaitse vs avalik seire

- **Kui droonseiresüsteem kasutab maapealseid sensoreid (radarid, kaamerad, RF-vastuvõtjad) eravaldustel (nt sideoperaatorite tornid, tööstusrajatised), kuidas säästa maaomanikku?** Kas sensorid saavad seada piirangu, et näha ainult lennurajooni või üllatuslikku droonilendu, ilma et salvestaksid muu tausta? Milline seadistus kõrvaldab pildilt majad/hooned või teeb kindlaks, et sensorid on ainult vaatlusalustel vabadustsoonides (nt propellerite tsoon)?
- **Mis saab eraomaniku poolt drooniotsingus osalemata jätmise järel kui droon on kriminaalse taustaga?** Kas kaitse- või kohtuasutustel on õigus kasutada seadmeid eraomandil kriminaalmenetluses (nt salajased kaameravõrgud)? Kuidas tagada, et avalik seire (nt politsei droonipatrull) ei rikuks eraomaniku õigusi ilma hädavajalikku uurimisotsust?
- **Kas süsteem peaks lubama eraisikutel/droonihuvilistel enda sensorid (nt väikese raadioiseloomustaja või kaugseirekaamera) infrastruktuuri infosüsteemi liidestada?** Kui jah, siis mis tingimustel ja kontrollimehhanismide all? Näiteks PPA esindaja tõi näite, et Viljandi tehase seadmed võiksid potentsiaalselt integreerida (mis tähendab, et ta maksab RFI-süsteemi eest ja näeb

oma territooriumi, aga ei näe piiriandmeid)[20]. Millised tingimused peaks kehtima sellisele anonüümsele või piirangutega andmesideliidesele?

- **Kas teile tundub kohane erainvestorite kaasamine drooniseiresse?** Mõned elutähtsad teenusepakkujad (nt Eesti Energia) võivad nõustuda seadmete ostmisega, kuid soovivad seejärel juurdepääsu ainult „oma objekti" lähedal oleva õhu kohta[21]. Kas see on vastuvõetav? Mis tingimustel andmed jagatakse ja kas nendest võiks tekkida era- ja avaliku huvi konflikt?

U-Space koostöö ja lennujohtimine

- **Kuidas tagada valitsuste, lennuameti ning hädaabiteenistuste informeeritus U-Space'i (droonijuhtimise digitaalse keskkonna) sündmuste kohta?** Kui droonidel lastakse lennata reaalajas planeeritud marsruudil (nt linnatransport, kaubavedu), peab süsteem kuvama, et tegemist on lubatud lennuga. Milline oleks lennujuhtimise (Lennuamet/ANS) ja drooniohutuse andmevahetusprotokoll – kas need sidemed tuleks luua reaalajas või esialgu ainult planeerimisetapil?
- **Kui tuvastatakse draon ohualas U-Space'i huvist lähtuvalt (nt lennujaama lähivaate raadiuses), kuidas infosüsteem reageerib?** Kes teavitab lennuliiklusteenindust? Kas tuvastuskaamera või radaridel peab olema integreeritud liides, mis annab automaatselt üle hoiatuse ATC-le, nagu see toimub mõnes provintsis aeroportide reaalajas droonihäire korral? Milline on ANS/ATC roll juhised droonitalituste korral ja kuidas tagada, et drooniseire sünkroniseerib lennujuhtimisega?
- **Kas U-Space'i juhtimisega seotud andmed (nt drooni plaanitud lennutugevus, registreeritud piloodi ID) on jagatud seire platvormiga?** Näiteks kas CUAS-süsteem saab vastavalt lennuplaanile distsiplineerida drooni (sõnum X märku tohib/ei tohi edasi lennata), või ainult tuvastada selle olemasolu? Kuidas oleks tagatud, et näiteks juhendamissüsteem kuvab drooni ainult õhuõigust omaval kasutajal, mitte juurdepääsu kontrollimata kolmandale isikule?

Andmete anonymiseerimine ja väärkasutus

- **Kuidas vähendada droonisensorite kogutavate isikuandmete sattumist identifitseerijate kujul analüüsiks?** Kas peaks vastu võtma põhimõtte, et enamasti tuvastab süsteem ainult „ala, kus droon asub" ega salvesta täpseid GPS-koordinaate ega lennutrajektoori, välistades isiklike lennuväljade kaardistamise? Kuidas tagada, et pildid ja heliandmed (nt patrullautolt salvestatud häälinteraktsioon drooni kohal) anonümiseeritakse?
- **Milliseid stsenaariume näete andmete kuritarvitamiseks?** Näiteks kurjategija võib kasutada süsteemi infot planeerimiseks (nt jälgides politsei drooniresursse või lüngata sensorite ülesehituses). Kuidas seda kaitsta? Samuti, kas teavet saaks kasutada näiteks rahvastiku / ühiskonna suundumuste analüüsiks väljaspool drooniohutuse konteksti? Kui näiteks kogu kesklinna drooniaktiivsus muutub, kas see võiks mingil moel pääseda statistikasse, mille abil kontrollida linlasi?

- **Kui teabe juurdepääs on lahti (n-ö „open data"), kuidas tagada selle eetiline kasutamine?** Teadusuuringud ja arendajad võivad soovida droonide liikumist ennustada või ehitada uusi avastusseadmeid. Kuidas sätestada, et inimtegevuse mõttes ei kuritarvitataks drooniliikumise analüüsi (nt sihtimistel reeglid, et jälgitakse ainult drooni, mitte selle valdav roll)?

Piiriülene info jagamine ja koostöö

- **Millisel kujul oleks kasulik üleilmne või piiriülene droonituvastusinfo vahetus?** Näiteks Läti ja Eesti jagavad signaalituvastust audiosensorite kaudu[22], kuid piiriüleselt võiks luua „droonimüüri" kogu Balti regiooni kaitseks[3][4]. Kas leiate, et Eesti peaks liituma laiemate initsiatiividega, millega jagataks reaalajas hoiatusi liitlastega? Millised tehnilised või juriidilised piirangud takistaksid piiriülest andmevahetust?
- **Kuidas käsitleda välisriigi droone Eestisse sisenemisel?** Kas reaalajas hoiatus peaks andma märku ka rahvusvaheliste juhtumite korral – näiteks kui drone maandub Eesti lennuväljal, mis on rahvusvaheliselt avatud, või lendab piiri suunas? Kas NATO/National Security perspektiivist võiks vaja minna ühiseid ohuhinnanguid ja käitumisreegleid? Milliseid rahvusvahelisi standardeid (EASA uue regulatsiooni kujul, ICAO suunised) võiks CI-süsteem toetada?
- **Milline on oodatav koostöö rahvusvaheliste droonitehnikafirmadega (näiteks DJI) või rahvusvaheliste turvatarnijatega?** Kas te näete Eesti süsteemi standardeid (nt SAPIENT, NATO) võimalike eksportimiseks või piiriülesteks koostoimeteks? Kuidas tagada, et ka kaugelt kontrollitavad, välisriigi päritolu droonid edastaksid meile vajalikku metaandmet, olles regulatsiooniga kooskõlas?

Teaduslik ja haridusalane andmekasutus

- **Milline juurdepääs peaks olema akadeemilistel ja teadusasutustel drooniseire andmetele?** Kas eeldatakse näiteks ERASETA sektoriga toetust läbi teadusuuringute – kas pilootprojektid võiksid lubada ülikoolidel analüüsida reaalajas infot (muidut ka salastatud/maskitud kujul) näiteks droonide trajektooride mudeldamiseks? Kui jah, siis millist liiki andmeid (metaandmed, visualiseeritud kaart, anonüümse andmemeetrika) see peaks olema?
- **Kuidas juriidiliselt lubada teadustööks andmete kasutamist, säilitades turvalisust?** Kas peaks eraldi juhtimiskeskus või uuringupartnerilt nõutakse täiendavaid turvagarantiite või sertifikaate, et imenduda süsteemi arendusse? Näiteks kas on võimalik anda teadlasele juurdepääs andmetele ainult laborikeskkonnas või krüpteeritud testivõrgus? Millised andmekaitse- või salastatusklassid tuleks aruannetes säilitada (nt tüpograafilise detaili vähendamine; andmete avaldamine ainult anonüümsetena)?
- **Kas tegutsevad programmifondid või kogukonnad (EU rahastus teadusprojekti kaudu) võiksid pakkuda süsteemi arendamiseks kaasinvesteeringut?** Kas, kui arendatakse uusi droonituvastussensoritüüpe või -algoritme, on võimalik neid

reaalajas CUAS-infrastruktuuri testida? Mis tüüpi katseandmed (nt pilootuurimised) oleks huvipakkuvad, et drooniseire platvormi täiendada?

Riskid ja turvalisus

- **Milliseid valehäireid ja vääraid positiivseid tuvastusi saaks süsteemiga vältida?** Näiteks kodukasutaja, spordiüritus või metsloomad võivad põhjustada drooni sarnaseid andmesignatuure. Kuidas operatiivsed üksused peaksid käsitlema tõenäosust, et näiliselt patrullile teatatud „tuvastatud droon" on hoopis õhupalli või muu pardifoto? Milline on sobiv standardne olukord tuvastuste kinnitamiseks ja väärtuste tõrke analüüsimiseks?
- **Kuidas kaitsta süsteemi enda haavatavuste eest (häkkimine, sabotaaž)?** Kas tuleks viia läbi turvaauditeid, häkkimise simulatsioone, et tuvastada nii sideühenduste kui ka infosüsteemi nõrkusi? Kes oleks vastutav süsteemi rünnaku avastamise eest ning milline on varuplaan?
- **Kuidas riskeerida juhtimisahela katkemine erakorralises olukorras (kriis, sõda või looduskatastroof)?** Kas süsteem peab suutma töötada maakera tugivõrkudest sõltumatult, nt lokaalselt piiri- või maakonnakeskustes, kui tugijaamadena kasutatavad ühendused on välja lülitatud[23]? Kas näiteks sõjaseisukorras võidakse süsteem täielikult üle anda kaitseväele, nagu oleks „põhiserv- oli intressiseni" (tsiviil juhtimissüsteemist üle)**[24]? Millised toimingud on vajalikud süsteemi üleandmiseks sõjaolukorras?
- **Kas olete hinnanud, milliseid füüsilisi või tehnilisi võimalusi vastane võiks drooniseiresüsteemi häirimiseks kasutada?** Näiteks kas droonilendude signaali häirimise (jammimine) või võltsinfo esitamise vastu (näiteks valearmide genereerimine) peab süsteem olema immuunne. Kuidas see kajastuks süsteemikava riskijuhtimises?

Tehnoloogiline innovatsioon ja ERA sektor

- **Millist panust on valmis andma telekommunikatsiooni sektor (sideoperaatorid) droonide detekteerimisse?** Näiteks kas 5G võrgud ja mobiilimastid võiksid andmeid edastada droonide positsioonide kohta (nt GSM-i signaalide anomaaliad)? Kuidas kaasata operaatorite olemasolevaid sidevõrke sensorina?
- **Kuidas koosdrooni- ja radaritootjad võiksid integreeruda süsteemi?** Kas droonitootjad on valmis tagama oma toodetele digitaalse „tagasisignaali" (näiteks IteD RPiga infot reaalajas), et neid saaks rakendada CVAS-süsteemi tuvastuselementidena? Kuidas julgustada kohalikke ettevõtteid ja erakäitajaid arendama ühisplatvormi (nt Eesti droonitootjad, turvafirmad)? Kas on oodatud eraettevõtted pakkuma spetsiaalseid lisafunktsioone või laiendusi (nt DJI droonidesse pugevat juriidilist piirangut?)
- **Kas on plaan paigaldada mobiilsed või kaasaskantavad tuvastusseadmed avalikele teenindussõidukitele (politseiautole, päästeautole)?** PPA-vestluses mainiti mobiilsete RF- andurite paigutust patrullautodele (nt Lõuna- ja Põhja-lõike

patrull, kus kokku ~90 andurit auto kohta)[8]. Kas sarnane lähenemine oleks laienev teistelegi (nt tuletõrjetorud, kiirabi)? Milline seire võimaldab anda täiendava hoiatusi ka liikuvatest üksustest?

- **Kuidas käsitleda erasektoriga seotud riske (korruptsiooni, huvide konflikte)?** Näiteks, kui mõni turvafirma või ettevõte osaleb andmete kogumises, kelle huvid esmajärjekorras kaitsta – avalikku hüve või kliendi huve? Kuidas ennetada olukordi, kus süsteemi arendaja või operaatorid kasutavad siseteavet enda eeliste hankimiseks?

Juhtimine, rollimudel ja eriolukorrad

- **Kes on vastutav süsteemi üldjuhtimise eest rahuajal?** Kas välja peaks mõtlema üleriigilise juhtimiskeskuse? (PPA sekku siis ainult praktikas, või peaks ka teised (nt Kaitsevägi) liituma olemasolevas tsiviil-juhtimiskeskuses[14].) Kuidas tagada, et eriüksused (kapo, lasketiirus töötav VLA, päästeamet) annavad oma sisendid ning kes haldab lõplikku infot?
- **Kuidas süsteemi juhtimine muutub erakorralises olukorras (sõda, eriolukord)?** Kuidas on tagatud, et kriisiolukorras jätkub side, informatsiooni voog ja kelle valitsemise alla süsteem langeb (nt PPA vs Kaitsevägi)? Näiteks on diskuteeritud vajadust sõjaseisukorras andmesüsteem Kaitseväele üle anda, et neil oleks „tsiviilsüsteem" kasutada[24]. Mis toimingud on kriisirežiimi jaoks ette valmistatud ja mis rollid eriolukorra aegses muutuses on?
- **Kas olete planeerinud sidevõrkude dubleerimist või alternatiivseid ühendusmeetodeid?** Kui süsteem põhineb kekserveril Tallinnas, siis kas Läti või Soomega suhtlevad ühendused on piisavad? Mida teha, kui pealinn on ühenduseta – kas maakondlikud tsentraalsed serverid (nt Tartus, Narvas) võtaksid iseseisvalt ohjad üle[25]? Kas planeeritav drooniseire on „tsiviil-" või pigem „militaarsüsteemi" tüüpi infrastruktuur (mis eeldab näiteks kiiret edasiarendust ja sidevarukooslusi)[26]?
- **Kuidas tagatakse süsteemi jätkusuutlikkus ja sõltumatud uuendused?** Kas on strateegia, et kui konkreetne tarnija enam olemas pole (pankrot või müük), saab juhtkond süsteemi teistele arendajatele usaldada? Näiteks PPA vestluses märkisid, et praegused kaupmehed on pigem startup-laadsed ja et me peaksime suutma potentsiaalse turu-välja arenduse edasi arendada ka ilma konkreetsest ettevõttest sõltuvuseta[27].

Kokkuvõtlikud küsimused

- **Kuidas teie hinnangul eristub CUAS-süsteemi roll igapäevases patrulltöös versus kriisiolukorras?** Kuidas hoida tasakaalu, et sõidukiirlusest lähtuvad valvejuhid ei suurendaks drooniseiresüsteemi automatismi nii, et see üle koormaks (nt iga „droonisignaal" põhjustab koheselt tormi)?
- **Kui te saaksite süsteemi kavandamisel esitada valitsusele peamist soovitust, mis võiks täiustada julgeolekuteenust, mis see oleks?** Kas rõhutaksite

tehnoloogilist investeeringut, juristi panust seaduskujutusse, andmeturbepoliitika kujundamist või haridust ja teaduse kaasamist?

Allikad: Ülalpool loetud intervjuude ja analüüside põhjal on välja toodud mitmeid arutelukohti CUAS-süsteemi infojaotuse, sensoreid puudutavate kitsaskohtade ning privaatsus- ja julgeolemisküsimuste kohta[1][3][5][4][28]. Esitatud küsimused peaksid aitama kaardistada erinevate osapoolte ootusi ja muresid.

---

[1] [21] [27] Ppa_resampled_mono_PRE180_vadlight_20251214_013058.txt

file://file-CrQk6RF2WRAA1KUPpjkW2F

[2] [3] [9] [10] [11] [13] [14] [15] [16] [17] [18] [19] [20] [22] [23] [24] [25] [26] [28] Tannar 121225 Recording 355_resampled_mono_PRE180_vadlight_20251214_015542.txt

file://file-L6MRorT9HExT4opTwiRfbn

[4] Estonian Organization Proposes ‘Wall’ to Keep Drones Out

https://www.nationaldefensemagazine.org/articles/2025/5/5/estonian-organization-proposes-wall-to-keep-drones-out

[5] [6] [12] SAPIENT autonomous sensor system - GOV.UK

https://www.gov.uk/guidance/sapient-autonomous-sensor-system

[7] [8] Sys Recording 354_resampled_mono_PRE180_vadlight_20251214_014137.txt

file://file-DwKW8TMtUKGQZxScK5CWyN