ChatGPT

1.1.1. Probleemi püstitus ja mõistmine

Nortal on hästi lahti kirjeldanud drooniohu alamprobleemid (nt droonide tuvastamine eri tingimustes, ohu määratlemine, lennutaja tuvastamine, võimaliku kahju hindamine, sobivate vastumeetmete valik jne) [1] [2]. Siiski tasuks **alamprobleemide loetelus** sõnaselgelt välja tuua ka *mitme drooni samaaegse ründe* ehk drooniparvede käsitlemine eraldi probleemina. Praegu mainitakse drooniparvede teemat küll hiljem kontekstis (nõue kiiremaks otsustusprotsessiks) [3] [4], ent juba probleemipüstituses rõhutamine aitaks fokuseerida lahenduse otsimist ka sellele keerulisele stsenaariumile. *(Infoks: drooniparved esitavad kordades suurema väljakutse – nõudes sensorvõrgult ja otsustustoe süsteemilt oluliselt kiiremat ja koordineeritumat reageerimist.)*

1.4. Andmeallikad ja tehniline lähteinfo

Nortal loetleb põhjalikult erinevaid standardeid ja andmeformaate (ASTERIX kategooriad, MOSA põhimõtted, U-space/UTM sõnumid, NATO STANAGid, NOTAM-formaadid jms) [5] [6], mis on **hea lähtekoht**. Siiski on oluline juba eelanalüüsis mõelda, **millise konkreetse andmemudeli ja protokolli** kasuks võiks lõplik süsteem otsustada ühise infovahetusformaadina. **Soovitus:** määratleda, millist ühtset formaati kasutatakse eri sensorite jälgimisinfo koondamiseks (näiteks ASTERIX CAT240 vs. STANAG 4676 vms). See tagab, et erinevatest allikatest pärit lennu- ja ohuteave on ühilduv ning integreeritav ühtses süsteemis. Samuti võiks rõhutada **droonide Remote ID** standardite arvestamist – EU regulatsioonide kohaselt peavad paljud droonid edastama kaugidentifitseerimisinfot (nt ASTM F3411-22a protokoll), mis tulevikus võiks olla oluline andmeallikas süsteemile. Praegu U-space standardite all see teema ilmselt kaudselt sisaldub, kuid otsesõnu lahtikirjutamine suurendaks selgust. Lisaks tasub täpsustada, **kuidas plaanitakse mitme sensori andmeid omavahel siduda (fuseerida)** – kas kasutatakse tsentraalset track'i fuseerimisalgoritmi või toimub esmane koondamine regionaalsete keskuste tasemel. See on oluline, et üks droon ei ilmuks süsteemis dubleeritult mitme eraldi objektina ning et eri sensorite info liituks üheks terviklikuks olukorrapildiks. *(Infoks: Standardivalik (ühine andmeformaat) ning multi-sensori andmete fuseerimise põhimõtted on strateegilised valikukohad, mis mõjutavad järgnevate etappide arhitektuurilahendust.)*

1.6. Arhitektuurilised lähtekohad ja tehnilised kitsaskohad

- **X-tee laadne lahendus sensorvõrgus:** Nortal toob välja, et eelistab sensorvõrgus *x-tee laadset lahendust*, kus kõik EDGE-seadmed käituvad nagu X-tee turvaserverid ja töötavad ka keskserveri puudumisel [7]. **Kommentaar:** Reaalajas sensorite andmevoogude puhul võib X-tee analoogia osutuda ebaefektiivseks, kuna X-tee on mõeldud pigem päringupõhiseks andmevahetuseks, mitte pidevaks voogedastuseks. Tasub kaaluda *publish-subscribe* stiilis arhitektuuri või *multicast*-põhiseid lahendusi, mis on loodud reaalajas andmete ja sündmuste jagamiseks. Näiteks hajus sõnumivahenduse kiht (message broker) või otse sensorite võrgus sündmuste jagamine võib olla otstarbekam kui päringute teel andmete küsitlemine. *(Infoks: Reaalajas suure hulga andmepunktide edastamine nõuab optimeeritud lahendust – X-tee pakub turvalisust, ent võib lisada viivitust; spetsiaalsed voogedastuslahendused tagavad kiirema reaktsiooniaja droonide tuvastamisel.)*

- **Lokaalsete lahenduste eelistamine vs parim tehnoloogia:** Arhitektuuripõhimõtetes on kirjas eelistus kasutada süsteemi komponentidena lahendusi, *mis on loodud Eestis või lähiregioonis*, et vähendada kriisiaegseid sõltuvusi [8]. See on arusaadav julgeolekukaalutlus, kuid tasub samas analüüsida, kas mõni kriitiline tehnoloogia (nt sensori- või tõrjesüsteem) on maailmas saadaval, mis märkimisväärselt ületaks kohalikke lahendusi. **Soovitus:** jätta arhitektuuris võimalus

integreerida ka globaalselt parimaid komponente, kui need annavad olulise võimekuse juurde, tagades samas kohaliku toe või varuplaani nende asendamiseks kriisiolukorras. *(Infoks: Liigne piiramine ainult kohalike toodetega võib tähendada mõnest tipptasemel võimekusest loobumist; samas peab olema plaan, kuidas kriisi korral toimib hooldus/toetus – siin on tasakaalukoht "parim tehnoloogia" vs "suveräänne kontroll".)*

- **SPOFi vältimine ja võrgu töökindlus:** Nortali arhitektuuriprintsiip välistab *ükskõik millise üksiku tõrkepunkti* süsteemis [9], mis on õige lähenemine. Selle toetuseks tuleb detailsemalt lahti mõtestada, kuidas tagatakse süsteemi töö ka osalise võrgu või komponendi rikke korral. **Soovitus:** planeerida topeltvõrguühendused ja varundusmehhanismid kriitilistele komponentidele (nt kui üks andmesidekanal katkeb, peab alternatiivne kanal olemas olema; regionaalsed keskused peavad suutma ajutiselt iseseisvalt toimida, kuni ühendus taastub). Samuti tuleb rõhutada *aeg-sünkroniseerimise* (time sync) olulisust – kõik sensorid ja keskused peavad jagama ühtset ajatempot (nt GPS/PTS või võrgu PTP abil), et eri allikate andmed oleksid ajaliselt koherentsed. *(Infoks: Tõrkekindel hajussüsteem eeldab, et igale potentsiaalsele katkestusele on ette nähtud leevendus – olgu see varuühendus, lokaalne andmesalvestus või ajutine autonoomne režiim. Ilma täpsete ajasünkrooni ja redundantsuseta võib "vigu taluv" arhitektuur praktikas ikkagi kogeda andmekadu või ebatäpsusi.)*

- **Riskide loetelu täiendamine:** Nortal on välja toonud esialgse riskide nimekirja arhitektuuri ja komponentide osas (sensori EDGE-võimekus, isetervendav võrk, tuvastusalgoritmide töökindlus, hajus arhitektuuri toimimine katkestuste korral, salastatud vs avaliku võrgu ühendamise küsimus) [10] [11]. **Täiendavalt** soovitame lisada riske, mis võivad mõjutada süsteemi õnnestumist: (1) *vale-positiivsete* ja *vale-negatiivsete* tuvastuste rohkus – droonituvastussüsteemid võivad genereerida hulgaliselt alarme (nt linnud, segajad), mis koormavad operaatoreid; analüüsis tuleks arvestada filtrite ja tehisintellekti vajalikkusega valehäirete vähendamiseks. (2) *Andmejagamise piirangud eri osapoolte vahel* – mitme asutuse koostöösüsteemis võivad tekkida olukorrad, kus mõni osapool ei tohi kogu infot näha (nt salastatud sensorite andmed); riskiks on infolünkade teke operatiivpildis. Tuleks kavandada lahendus, kuidas andmeid klassifitseerida ja õigustega hallata nii, et julgeolekunõuded oleks täidetud, kuid operatiivne pilt ei kannataks. (3) *Side ja andmekogumisvõime katkemine sihilikult* – vastane võib proovida segada sensoreid või sidekanaleid (sh GPS-i) või rünnata süsteemi kübermeetoditega. See risk on osaliselt kaetud CEMA teema all kontekstis, kuid tuleks selgemalt välja tuua vajadus kaitsva *küberturbe* arhitektuuri järele (intrusiooni tuvastus, võrgu segamis- ja ründeoskus testimine jms) juba lahenduse kavandamisel. *(Infoks: Need täiendavad riskitegurid võivad otseselt mõjutada süsteemi tõhusust ja usaldusväärsust – neid arvesse võttes saab järgnevates etappides paremini planeerida leevendusmeetmeid.)*

1.7. Muu vajalik

Nortal planeerib kaasata Ukraina ekspertide kogemust integreeritud õhuseire ja droonitõrje valdkonnas ning isegi võimaliku Ukrainas kohapealse visiidi [12] [13]. See on väga väärtuslik – sõjakogemus annab unikaalseid õppetunde. **Soovitus:** lisaks Ukrainale võiks analüüsis vaadata ka *liitlasriikide* ning rahvusvaheliste organisatsioonide (nt NATO) kogemusi sarnaste süsteemide loomisel. Näiteks NATO C-UAS töörühmad, Balti riikide koostööprojektid või mõne teise riigi (Soome, Iisrael, USA jt) avalikud õppetunnid annaksid võrdlusmomendi. Ukraina õppetunde tuleks vaadelda kontekstis – need on saadud intensiivses konfliktis – ning hinnata, millised neist on ülekantavad rahuaja olukorda Eestis. *(Infoks: Mida laiemalt kogemusi ammutada, seda terviklikum on analüüs. NATO/EU standardid ja praktikad võivad aidata lahendust kujundada nii, et see sobitub rahvusvahelisse raamistikku ja tulevastesse ühishangetesse.)*

2. Tegevusplaan

- **Ajakava ja vahe-eesmärgid:** Plaan näeb ette ~10-nädalast tööperioodi [14], mis on üsna tihe ajakava kogu eelnõu läbiviimiseks. Soovitame Tellijal ja teostajal koos planeerida *riskivaru* juhuks, kui mõni töövoog (nt sidusrühmade intervjuud või õigusanalüüsi sisend) viibib planeeritust. Nortal on küll planeerinud töövoogude osalise paralleelsuse ja iganädalased sünkroniseerimised [15], kuid reaalsuses võivad kohtumiste ajad ja andmekogumine nihkuda. **Soovitus:** leppida kokku selged *vahe-eesmärgid* ja regulaarsed ülevaated – näiteks vahekokkuvõte 5. nädala paiku, mil esitletakse esialgseid järeldusi või arhitektuuri visiooni mustandit, et Tellija saaks varakult tagasisidet anda. See aitaks vältida olukorda, kus lõpparuandes ilmneb ootamatusi. *(Infoks: Tihe ajaraam nõuab paindlikkust – varajased kontrollpunktid ja riskivarud tagavad, et ajasurve ei vähenda analüüsi kvaliteeti ning Tellija saab protsessi käigus suunata fokuseerimist.)*

- **Prototüüpimise kaalumine:** Tegevusplaani lõpus on ette nähtud *"Prototüüpimise vajaduse määratlemine"* [16], s.t. hinnatakse, kas ja milliseid prototüüpe järgmises faasis vaja on. Meie hinnangul võiks juba eelanalüüsi käigus – võimaluste piires – läbi viia mõne *väikesema ulatusega tehnilise katse* või demonstratsiooni olemasolevate sensoritega. Näiteks integreerida pilootprojektina üks radar või droonituvastusseade testkeskkonda ning kuvada selle andmed lihtsas kaardirakenduses. See annaks praktilist infot integratsiooniprobleemidest ja andme kvaliteedist. Kui see siiski ei mahu eelarvesse/ajakavva, siis tuleks **järgmises etapis** kindlasti planeerida piisav aeg ja eelarve prototüübi(te) loomiseks. Analüüsis võiks rõhutada, et prototüüpimine on *kriitiline järgmine samm* riski maandamiseks enne täismahus arendust. *(Infoks: Varajane "proof-of-concept" demonstratsioon kinnitab kontseptsiooni toimivust ning paljastab võimalikud kitsaskohad – see on väärtuslik sisend enne suurema ressursi kulutamist. Ilma prototüübita jäävad mõned praktilised küsimused õhku; seega on prototüüpimine järgmises faasis peaaegu vältimatu.)*

2.1. Projekti meeskond ja rollid

Nortal on kokku pannud interdistsiplinaarse tiimi: ärianalüütik, süsteemiarhitekt, julgeoleku- ja droonieksperdid, õigusekspert ning projektijuht [17]. See katab põhilised rollid. **Siiski** tasub Tellijal üle vaadata, kas tiimis on esindatud *piisav spetsiifiline droonitõrje kompetents*. Ehk, kas nimetatud "droonieksperdid" omavad praktilist kogemust droonide tuvastussüsteemidega (radarid, RF-sensorid, optilised vahendid) ning vastumeetmetega. Vajadusel võiks teostaja kaasata kitsama ala spetsialiste – näiteks side- ja andmesidetehnoloogia ekspert (et kavandada keerukate sensorvõrkude integratsiooni) või keegi, kel on *operatiivkogemus* reaalsest drooniintsidentide haldamisest. Samuti on kasulik planeerida koostöö olemasolevate sensoritootjate või -operaatoritega: näiteks mõne radarit või droonidetektorit haldava asutuse spetsialistid saavad anda sisendi, kuidas nende andmeid kõige paremini integreerida. *(Infoks: Droonide seire ja tõrje on kiiresti arenev ning väga spetsiifiline valdkond – meeskonna laiapõhjaline kogemus on küll tugev alus, kuid konkreetsete tehniliste niššide (nt sagedusvahemikud, radarite signaalitöötlus, elektroonilised vastumeetmed) tundmine aitab tagada, et analüüsis tehtavad järeldused ja ettepanekud on realistlikud ning kõige ajakohasemad.)*

---

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 NORTAL.docx
file://file_000000002d8872469df12443bd9b05a5