

ASUTUSESISESEKS KASUTAMISEKS

Tallinna Ülikool
Matemaatika-Loodusteaduskond
Informaatika osakond

Info- ja kommunikatsioonitehnoloogia tsentraalse juhtimise ning
haldamise võimalused Eesti Kaitsejõududes

Magistritöö

Magistrant: Joel Puulmann

Juhendaja: Ants Põldsam

Osakonna juhataja: Peeter Normak

TALLINN

2007

ASUTUSESISESEKS KASUTAMISEKS

Sisukord

SISUKORD	2
SISSEJUHATUS	4
1. KAITSEJÕUDUDE INFO- JA KOMMUNIKATSIOONITEHNOLOOGIA TEENISTUSE TEKE NING ARENG KUNI AASTANI 2001	5
1.1. EESTI KAITSEJÕUDUDE ÜLESEHITUS	5
1.2. EESTI KAITSEVÄE TELEKOMMUNIKATSIOONI SÜSTEEMIDE ÜLESEHITUS KUNI AASTANI 1998	5
1.2.1. Raadioside.....	5
1.2.2. Telefoniside.....	7
1.2.3. Infotehnoloogia.....	7
1.3. EESTI KAITSEVÄE TELEKOMMUNIKATSIOONI SÜSTEEMIDE ÜLESEHITUS ALATES AASTAST 1998 KUNI AASTANI 2001	7
1.3.1. Raadioside.....	8
1.3.2. Telefoniside.....	8
1.3.3. Infotehnoloogia.....	10
2. KAITSEJÕUDUDE TRANSMISSIOONIVÕRK	11
2.1. <i>BALNET</i>	11
2.2. <i>Kaitsejõudude transmissioonivõrk</i>	12
2.3. <i>Võrgusõlm</i>	14
2.4. <i>Väeosa/asutuse transmissioonivõrk</i>	15
2.4.1. <i>Keskne sideseadmete ruum</i>	16
2.4.2. <i>Keskne valveseadmete ruum</i>	17
2.4.3. <i>Side- ja valveseadmete ruum</i>	17
3. INFO- JA KOMMUNIKATSIOONI TEHNOLOOGIA JUHTIMINE JA HALDUS KAITSEJÕUDUDES	19
3.1. <i>Kaitsejõudude Peastaabi J6</i>	19
3.2. <i>Väeosa</i>	21
3.3. <i>Side- ja Infosüsteemide Väljaõppe ja arenduskeskus</i>	23
4. TSENTRAALSE JUHTIMISE JA HALDUSE MUDEL	26
4.1. <i>Juhtimine</i>	26
4.2. <i>Kaitsejõudude IKT juhtimise ja halduse mudel</i>	28
4.2.1. <i>Side- ja Infosüsteemide jaoskond – J6</i>	29
4.2.2. <i>Side- ja Infosüsteemide Väljaõppe- ja Arenduskeskus – SIVAK</i>	30
4.2.3. <i>Regionaalne halduskeskus</i>	31
4.2.4. <i>Regioonideks jaotamise alused</i>	32
4.2.4.1. <i>Kaitsevägi</i>	33
4.2.4.2. <i>Kaitseliit</i>	33
4.2.5. <i>Väeosa</i>	34
4.3. <i>Juhtimise- ja haldusprotsessi kirjeldus Kirde regiooni näite varal</i>	35
4.4. <i>Süsteemi rakendumise mudel ja etapid</i>	41
4.4.1. <i>Seadusandlus ja alluvusvahekorrad</i>	41
4.4.2. <i>Standartsete raamistike väljatöötamine</i>	42
4.4.3. <i>Tsentraliseeritult vahendite soetamine uuele süsteemile</i>	51
4.5. <i>Uue süsteemi positiivsed ja negatiivsed küljed</i>	53

ASUTUSESISESEKS KASUTAMISEKS

5. KOKKUVÕTE.....	55
SUMMARY	56
LISA 1	57
LISA 2	60
VIITED:	63
KASUTATUD KIRJANDUS.	64

Sissejuhatus.

Eesti Vabariigi taas iseseisvumisega 20.augustil 1991. aastal muutus aktuaalseks ka riigi kaitsevõime arendamine. Kaheksakümnendate aastate lõpu ja üheksakümnendate algul oli loodud või taastatud erinevates alluvus- ja struktuurilistes vormides piirivalve, kodukaitse ja kaitseliit. 3. septembril 1991.aastal võttis Ülemnõukogu vastu otsuse „Üldisest kaitseväeteenistuse kohustusest“ ja 31. oktoobril algas kaitseväge loomine Peastaabi, kui operatiivjuhtimise organi formeerimisest toonase koloneli, nüüdse kindralmajor Ants Laaneotsa juhtimisel.

Alustada tuli siiski suhteliselt tühjalt kohalt. Kõigepealt tuli selekteerida, kellega hakata kaitseväge taaslooma - Eestis õitses rahvuslus ning kõik idapärane oli võõras ja taunitav. Ohvitserkond, kellest kogu kaitsevägi välja pidi hakkama kasvama, oli suhteliselt kirju – alates Nõukogude Liidu armee reameestest - kolonelidest kuni Ameerika Ühendriikide kolonelideni.

Organisatsiooni edukaks toimimiseks on seda vaja juhtida, eriti oluline on juhtimine hajutatud üksuste puhul, nagu seda on kaitsejõud. Kaitsejõudude juhtimine ei seisne mitte ainult kirjalikes direktiivides ja määrustes, vaid ka otseses verbaalses juhtimises. Sellises segases maailmas hakati looma ja arendama kaitseväge omi info-ja telekommunikatsiooni (edaspidi IKT) süsteeme. Kuni aastani 2000 võib väita, et toimus mingil määral kaitseväge sees tsentraalne IKT juhtimine ja haldus, mis erinevate ülemate tahtel on tänaseks päevaks praktiliselt kadunud või eksisteerib vägagi minimaalsel kujul.

Oma töös tahan tõestada, et tsentraalne IKT haldus on kaitsejõududele lõpp- kokkuvõttes kasulikum nii organisatoorselt kui ka finantsiliselt, kui antud hetkel toimiv „süsteemitus“ süsteemis. Selleks kirjeldan kaitsejõudude IKT arengut alates aastast 1991 kuni aastani 2001, kaitsejõudude transmissioonivõrku ja selle funktsionaalsust, valitsevat olukorda kaitsejõudude IKT valdkonnas ning tsentraalse halduse ning juhtimise mudelit, kasutades viimati nimetatud puhul autori visiooni. Kirjelduse loomisel kasutan erinevate kaitseväge väeosade/asutuste (edaspidi väeosa) side- ja infotehnoloogia teenistuste (edaspidi S6) töötajatega tehtud intervjuude ja küsimustiku analüüsi tulemusi.

1. Kaitsejõudude Info- ja kommunikatsioonitehnoloogia teenistuse teke ning areng kuni aastani 2001.

1.1. Eesti kaitsejõudude ülesehitus.

Kaitsejõud on riigi sõjaväeliselt korraldatud relvastatud struktuurid. Kaitsejõudude ülesanne on tagada pidev sõjaline valmisolek ja kaitse. Kaitsejõud koosnevad kaitseväest, Kaitseliidust ning sõjaajal kaitseväe ülemjuhataja alluvusse antavatest Siseministeeriumi valitsemisalas olevatest sõjaväeliselt korraldatud asutustest ja üksustest¹.

Kaitsevägi jaguneb omakorda Maavägi, Õhuvägi, Merevägi ja keskalluvusega väeosad ja asutused.

1.2. Eesti kaitseväe telekommunikatsiooni süsteemide ülesehitus kuni aastani 1998.

Eesti kaitseväe taastamise järgselt alustati ka kaitseväele erinevate telekommunikatsiooni süsteemide loomisega, mis tagaksid kaitseväe juhtimise nii rahu- kui ka sõjaaegsetes tingimustes. Eriti suurt rõhku pöörati militaarside tagamisele ning treenimisele väeosades, peamiselt just raadioside valdkonnas.

1.2.1. Raadioside

Esimeste raadiosidevahenditena olid kasutuses erinevad Nõukogude Liidu päritoluga raadiojaamad - peamiselt R-108M², R-130 ja R-142³. Vastavalt siis R-108M VHF (Very High Frequency – ultralühilaine) sagedusalas, R-130 HF (High Frequency – lühilaine) sagedusalas ja R-142 HF/VHF sagedusalas⁴. Raadiojaamade kasutamine vastavalt nende võimekustele oli järgnev:

- R-108M kompanii/pataljoni taseme taktikaline raadiojaam;
- R-130 garnisonide vaheline HF raadiosides kasutatav raadiojaam;
- R-142 või R-142N pataljon/brigaadi taseme taktikaline raadiojaamade komplekt. R - 142 komplekti kuulusid järgnevad raadiojaamad R-111 2 tk, R-123 1 tk ja R130 1 tk.

ASUTUSESISESEKS KASUTAMISEKS

R-142N komplekti kuulusid järgnevad raadiojaamad R-171 2 tk, R-163 1 tk, R134 1 tk;

R-142N komplekti kuuluvad raadiojaamad omasid NL armees esmast andmeside ja krüptograafia võimekust, mis Eestisse müüdnud seadmetelt olid kas eemaldatud või polnud üldse paigaldatudki.

Antud tehnika oli peaaesjalikult kasutuses aastatel 1992-1994, mil saabusid esimesed Iisraeli relvatehinguga soetatud kaasaegsed raadiojaamad firmast „Tadiran”. Soetatud raadiojaamad olid Nõukogude Liidu raadiojaamadest kergemad, kompaksemad, mobiilsemad, suuremate sagedusvahemikega. Raadiokanalid olid kaasaskantavatel raadiojaamadel krüpteeritavad (käsijaamadest puudus see võimekus) ning püsisid etteantud sagedustel stabiilsemalt.

Lühiajaliselt kasutati Prantsusmaalt abina saadud raadiojaamu, mis oma tehniliste parameetrite poolest olid analoogsed Nõukogude Liidu raadiojaamadest, kuid nende kasutusaeg jäi ühe aasta piiresse – raadiojaamade toiteelementideks olid patareid ja uute patareide soetamiseks puudusid finantsressursid.

Raadiojaamu, eelkõige HF raadiojaamu kasutati garnisonidevaheliseks ning garnisonisiseseks sidepidamiseks. Raadiosidet pidasid radistid, kellede töökohad asusid garnisonide/väeosade sidekeskustes. Raadiosidet peeti eelkõige kõneedastus meetodiga, kus kasutati eelnevalt kindlaks- määratud koode ja märksõnu, mida nimetati ka „signaalideks“. Raadioside korraldamiseks oli kasutusel radisti kõnetabel ja operatiivinfo jaoks oma kõnetabel, kood sõnade komplektid, oluliste asukohapunktide koodid ja ohvitseri kaardivõrgustiku kodeerimise võtmed. Eelpool loetletud vahendid olid peaaesjalikult kasutuses kuni 1997. aastani.

1993.aastal alustati üle-eestilise operatiivteenistuste sidevõrgu (tänapäeval tuntud kui ametkondadevahelise operatiivraadioside – edaspidi ORS) projekteerimist, kasutades EDACS⁵ (Enhanced Digital Access Communications System) süsteemi. Valmis jõuti ehitati kolm tugijaama: Tallinn, Narva ja Narva-Jõesuu. Finantsressursside puudumise tõttu projekt seiskus, kuid valmishitatud kolm tugijaama on töös veel ka aastal 2007 politsei poolt.

1.2.2. Telefoniside

Telefoni kõneside teenust pakkus igas väeosas sidekeskus, kus oli Nõukogude Liidu päritolu käsikommutaator P-198M, P-194M. või P-193M. Käsikommutaatorisse oli ühendatud üks kuni viis analoogtelefoni ühendust AS Eesti Telefoni (edaspidi ET) televõrku, mille kaudu toimus kõnede edastamine erinevate väeosade vahel. Otse ET televõrku ühendatud lauatelefonid olid väeosa ülemal, staabiülemal, sektsioonide/jaoskondade ülematel, korrapidamisteenistusel. Eelpoolloetletud ülematel oli laual kaks telefoni, millega ta siis helistas – ühe telefoniga majasisesesse televõrku läbi sidekeskuse, teise telefoniga otse ET televõrgu kaudu, kuhu iganes soovis.

1.2.3. Infotehnoloogia

Esimesed arvutid saadi välisabi korras 1993. aastal ning esmane kasutuskoht oli arvutitel raamatupidamises. Nii näiteks soetati esimene arvuti Üksik-sidepataljonile aastal 1994 ning seda jagas pataljoni raamatupidamine Kaitsejõudude Peastaabi sideosakonnaga (edaspidi J6, tolle aegne nimi). Arvutiks oli 486DX2 protsessoriga, tarkvarana kasutati algselt operatsioonisüsteemina Microsoft (edaspidi MS) DOS 6.2 ja MS Windows 3.1. Kontoritarkvarast oli kasutusel MS Word, MS Excel, Coreldraw 5, mille jaoks jäi arvuti jõudlusest siiski vajaka. Üksikud arvutid, mis olid väeosades ei olnud omavahel kohtvõrku (edaspidi LAN) ühendatud. Praktiliselt samalaadne olukord valitses ka teistes väeosades, kus terve väeosa peale oli üks kuni kaks arvutit, mille peamiseks kasutajaks oli raamatupidamine.

Enne ja koos esimeste arvutite kasutuselevõtmisega kasutati dokumentide koostamiseks kas mehhanilisi, elektromehhaanilisi ja üksikuid kuni mõne leheküljelise mäluga kirjutusmasinaid. Arvutite massilist kasutuselevõtmist piirasid eelkõige arvuti hind ja inimeste arvutikasutamise oskused.

1.3. Eesti kaitsevää telekommunikatsiooni süsteemide ülesehitus alates aastast 1998 kuni aastani 2001.

Kogu maailma üha suurenev IKT teenuste kasutamine ei läinud mööda ka Eesti riigist ja selle asutustest – olgu see siis erafirma või riigiasutus.

1.3.1. Raadioside

Raadiojaamadena olid peamiselt kasutusel Iisraeli relvatehinguga soetatud PRC tüüpi raadiojaamad, kuid soetatud PRC tüüpi jaamade kogus ei vastanud enam vajadustele, sest seoses Interneti Protokoli (edaspidi IP) lisamisega taktikalistesse raadiojaamadesse ja kasutusele võtmisega suurriikide poolt tekkis ka Eesti kaitsejõududel vajadus kaasajastada raadiojaamu. Nii asutigi hankima uusi raadiojaamu ja väljavalituks osutus Ameerika Ühendriikide poolt pakutav SINCGARS (Single Channel Ground and Airborne Radio System)⁶ tüüpi raadiojaam PRC-119/E. Paraku lõppes tootjafirma ühinemisel Harris Corporation`iga jaamade tarne Eestisse. Raadiojaamu jõuti Eestisse tarnida väikeses koguses, suurusjärgus sada ühikut koos erinevate lisadega.

1998. aastal alustas kaitsevägi katsetega HF andmesidevõrgu rajamiseks. Selleks paigaldati iga väeosa territooriumile lisaks üks raadiojaam PRC-2200 ja lisati PC tüüpi lauaarvuti, mis oli ühendatud läbi (KAM+) modemi raadiojaamaga. Sellises andmeside võrgus edastati sõnumeid sarnaselt e-kirjadele - oli aadressiväli, päis ja sisu. Antud lahendus töötas kuni 2003. aastani suhteliselt edutult – kaitsejõududes oli ainult kaks inimest, kes teadsid, kuidas süsteem peab töötama ja oskasid seda ka vastavalt seadistada.

Sarnaselt Kaitsejõududele alustas Kaitseliit 1998. aastal oma andmeside võrgu rajamisega VHF sagedusalas. Kasutati Mobira tüüpi raadiojaamu, mis olid läbi modemi ühendatud PC tüüpi lauaarvutiga.

1.3.2. Telefoniside

Kuna punktis [1.2.2](#) toodud televõrgu lahendus oli oma ülalpidamis kulude poolest liiga kallis ja samaaegselt ka aegunud, asusid kaitsejõud 1998. aastal muutma oma lähenemist telekommunikatsiooni võrgu osas

Kalliks muutisid vana lahenduse alljärgnevad tegurid:

- Personalikulud;
- Seadmete suurest vanusest tulenevad hoolduskulud;
- Varuosade nappus telefonikeskjaamadele;

ASUTUSESISESEKS KASUTAMISEKS

- Sõltuvus teisest firmast (ET) – puudus varulahendus, televõrku ei olnud võimalik ühendada HF raadiojaamadega kuna puudusid raadiojaamadel telefoni liidesed.
- ET telefoniarvete suurused küündisid suurusjärku 250 – 350 000 Eesti krooni kogu kaitseväe peale;

Esimeste sammudena asusid väeosad iseseisvalt soetama analoogtelefoni keskjaamu. Muretseti täiesti erinevaid keskjaamu ja iga väeosa asus oma parima „nägemuse” kaudu süsteemi arendama. Soetatud keskjaamad olid erinevatelt tootjatelt ja isegi erinevatelt kontinentidelt. Siemens (Saksamaa), Panasonic (Jaapani), Ascom (Šveitsi), Harris (Ameerika Ühendriigid) on läbilõige firmadest, kellede toodangut kasutati, kuid sellega ka kogu arendus esialgu piirdus.

Süsteem hakkas koosnema analoogtelefoni keskjaamast mis oli üks eelvest loetelust, ning see oli ühendatud ET televõrku. Sellise lahenduse rakendumisel oli nii plusse kui ka miinuseid.

Plussid:

- Remondi- ja hoolduskulud minimaalsed – kasutati uusi seadmeid;
- Vähenes valeühenduste arv – inimfaktori eksimisvõime on kordades suurem kui automaatikal;
- Suurennes ühenduste loomise kiirus – automaatne ühendamine senise käsitsi ühendamise asemel;
- Kadus vajadus eraldi telefonistide pidamiseks - personalirahade kokkuhoid, vabanenud ametikohtad sai ümber tõsta vajalikematesse kohtadesse näiteks IT spetsialist;

Miinused:

- Süsteemitus üle kaitseväe – Ascom, Panasonic, Siemens, Harris iga jaama jaoks pidi olema oma spetsialist;
- Suurt rahalist kokkuhoidu ei saavutatud – ühendus majast välja toimus läbi ET televõrgu;
- Endiselt sõltuvus ET televõrgust ja puudus endiselt tagavaravariant kohaliku ET keskjaama rikke korral.

1.3.3. Infotehnoloogia

Väeosadesse olid juba tekkinud esimesed arvutid ja ajapikku hakati väeosadesse tööle võtma infotehnoloogia spetsialiste. Väeosades komplekteeriti lisaks raamatupidamisele järgnevalt sekretär-asjaajajate ja personali osakondade töökohad. Arvutitega varustatud töökohtade arvu kasvuga seoses tekkis ka vajadus hakata kasutama andmete vahendamist teisiti, kui optilise meedia vahenditega edasi- tagasi andmete tõstmist.

Arvutid ja nende kasutajad ei olnud sugugi vastavuses teineteisega ja nii oli sagedane olukord, kus targemad ja helgemad pead ajateenijate hulgast sattusid n.ö. „prii leiva” peale staapi. Tänapäeval iseenesest mõistetavana tunduva kontoritarkvara MS Office kasutamine oli kui tuumafüüsika ja kui vähegi võimalik oli, siis püüti kõik kirjatööd ja arvutused ikkagi käsitsi ära teha.

Infotehnoloogia spetsialist on alati olnud lai mõiste ning kõigile lükata-tõmmata - seda tabas ka J6, kelle korraldusel toimus peaaegu kogu IT alane tegevus ainult läbi nende – arvutite ja tarkvara soetamine, välja arvatud IT spetsialistide palkamine. Vastavalt „Avaliku teenistuse seadusele” on ametnike ametisse määramise õigus väeosa ülemaal⁷. Kaitsejõudude siseselt ei olnud IT spetsialistidel aga määratud ühtseid kutsestandardeid ja nii oligi võimalik väeosadel palgata antud kohale vägagi erineva tausta ja oskustega inimesi - alustades arvutitehnikutest ja lõpetades kodukasutajatega, kes oma elus olid korra kõrvalt näinud, kuidas arvutisse tarkvara paigaldati.

Väeosade vajadused olid peamiselt suunatud kasutajatoe järele, kuid esines ka juba väeosi, kuhu olid rajatud esmased algelised kohtvõrgud ja paigaldatud esimesed teenusserverid. Peale eelpool loetletu tuli hallata ka esimesi elektroonseid valvesüsteeme, mis väeosadesse rajati, kuna süsteemis sisaldasid nii arvutid kui ka tarkvara.

2. Kaitsejõudude transmissioonivõrk

Seoses üha kasvavate infosüsteemide hulga, arvutite massilise kasutuselevõtu ja aina kasvavate andmeside ühenduse vajadustega otsustati hakata ehitama Kaitsejõududele ühtset transmissioonivõrku. Transmissioonivõrk pidi katma terve Eesti Vabariigi territooriumi ning selle peal pidid hakkama jooksma erinevad teenused – nii kõne- kui ka andmeside. Süsteemiga pidid liituma kõik Kaitseministeeriumi haldusalas olevad üksused.

Kaitsejõudude transmissioonivõrgu tekkele andis omapoolse tõeke ka kolme Balti riigi ühtse õhuseire süsteemi „BALTNET” i rajamise raamleping 16. aprill 1998.

2.1. BALTNET

BALTNET on kolmes Balti riigis toimiv õhuseireandmete hankimiseks, koordineerimiseks, levitamiseks ja kuvamiseks kavandatud süsteem, mille eesmärgid hõlmavad tsiviil- ja sõjaväevõimude vahelist rahvusvahelist koostööd lennunduse alal ning iga osalejariigi vastavate funktsioonide parandamist.

16. aprillil 1998.a. allkirjastatud BALTNET-i raamleping nägi ette, et Leedu Vabariiki rajatakse regionaalse õhuruumi seireandmete koordinatsioonikeskus (Rear Area Security Control Center - edaspidi RASCC), mis võtab vastu, töötleb ning kuvab primaar- ja sekundaarradarite andmeid kolmes Balti riigis, algatab ja koordineerib kõigi radarite seirelatusse sattunud lennukite jälgimist ja tuvastamist ning koordineerib regionaalse informatsiooni vahetamist kolmandate pooltega. Integreeritud informatsioon võimaldab Balti riikide asjaomastel võimudel jälgida, tuvastada ja kontrollida lennuliiklust kogu regiooni õhuruumis.

Lisaks RASCC-ile rajasid Eesti, Läti ja Leedu igauks ka oma riikliku õhu-seirekeskuse, mis võtavad vastu ja kuvavad RASCC-i üldist integreeritud õhuruumipilti ning on tagavarasüsteemiks RASCC-i avarii korral. Riiklikke radarijaamu kasutatakse ka teiste riigi territooriumil paiknevate radarite vahendusel saadud seireandmete töötlemiseks ja kuvamiseks.

ASUTUSESISESEKS KASUTAMISEKS

BALTNET-ile edastatavad radariandmed jäävad andmeid edastava riigi omandiks, kuid BALTNET-i vahendeid võidakse kasutada õhuruumipiltide vahetamiseks NATO-ga ja/või riikide vahel. BALTNET-i juhitakse ja hallatakse kolme Balti riigi esindajatest moodustatud ning RASCC-i juures asuva ühise struktuuri abil.

Eesti riikliku õhuseiresüsteemi arendamine toimub tsiviil- ja sõjaväeliste organite koostöös. Rajatav süsteem on osa BALTNET-ist, mis võtab vastu, integreerib ja saadab andmeid kõigile riigi asjaomastele ametkondadele (õhuvägi, tsiviil-lennujuhtimiskeskus, piirivalve, veeteede amet).

BALTNET-i süsteemi kuuluv Eesti riiklik jaam rajati 1999. aastal Tallinnast 40 kilomeetri kaugusel asuvalle endisele Nõukogude Liidu armee sõjaväelennuväljale Ämaris.

Transmissioonivõrgu ehitus BALTNET-i süsteemile Eestis algas 2000. aastal. Transmissioonivõrgu alguspunkt asus Lõuna Eestis ja lõpp-punkt oli Ämari sõjaväelennuväli. Süsteem oli oma ülesehituse poolest asukohapõhise Point-to-point ühendusel ja kasutusel olid Norra Kuningriigist soetatud NERA 4x2 Mbit/s raadiorelee seadmed. Transmissioonivõrgu sõlmede vahemaa oli sõltuvalt asukohast ja maastikust 30 kuni 40 kilomeetrit ja mastide kõrgus jäi vahemikku 30 kuni 100 meetrit. BALTNET-i transmissiooni võrgusõlmed on oma ehitusel ja süsteemide funktsionaalsuselt sarnased Kaitsejõudude transmissioonivõrgu võrgusõlmedele. Transmissioonivõrgu ehitust finantseeris vastavalt lepingutele Norra Kuningriik, seadmete ostu ja ruumide ehitust ning sisseseaded finantseerisid Ameerika Ühendriigid.

2.2. Kaitsejõudude transmissioonivõrk

Kolme Balti riigi ühtse õhuseire süsteemiga rajamisega loodi osaliselt baas- infrastruktuur tulevasele kaitsejõudude transmissioonivõrgule – osa transmissioonivõrku sai ehitada juba olemasolevale infrastruktuurile ja selle läbi muutus ka kogu võrgu rajamine soodsamaks.

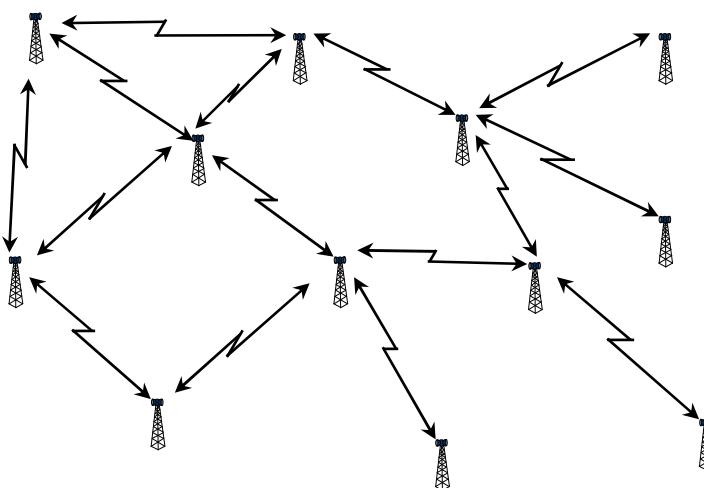
ASUTUSESISESEKS KASUTAMISEKS

Kaitsejõudude transmisionivõrgu ehitamiseks teostati riigihange süsteemi välja- ehitamiseks. Riigihanke võitis Ericsson Eesti As, kes pakkus Ericsson MiniLink 16x2Mbit/s raadiorelee seadmeid. Võrgu ehitust alustati 2001. aastal.

Transmisionivõrgu üle-eestiline väljaehitus oli jagatud ajalistesse etappidesse, mille esimestes etappides ehitati üksikuid jadaliine, millel oli üks ühtne alguspunkt, kuid mis hargnesid erinevates suundades. Liinid olid ehitatud asukohapõhiselt (point-to-point põhimõttel) ning sõlme rikke korral puudus sellest sõlmest ühendus edasi. Esialgne andmemaht lingi kohta oli 2 Mbit/s ning peamise teenusena oli seal telefonikeskjaamade vaheline transmision.

2004. aasta keskpaigas hakati jadaliine omavahel kokku ühendama - selle tulemusena tekkisid esimesed ringid transmisionivõrgus. Ringvõrgustiku tekkimisega võeti kasutusele asünkroonse ülekande viisiga Asynchronous Transfer Mode (edaspidi ATM) seadmed. ATM seadmete rakendumise järgselt muutusid võrgusõlmede läbilaske mahud konfigureeritavateks kuni 34 Mbit/s võrgusõlme kohta. Lisateenusena hakati üle transmisionivõrgu pakkuma kaitseväge interneti ja alates 2006. aastast seoses videotelekonverentsi (VTC) seadmete soetamisega väeosadesse ka VTC teenust.

Transmisionivõrgu põhimõtteline joonis (Joonis 1). Antud joonis on illustratiivne, ning ei kajasta endas võrgusõlmede reaalseid asukohti ega ühenduste arvu⁸.



Joonis 1

2.3. Võrgusõlm

Võrgusõlmed võib põhimõtteliselt jagada kaheks:

- Väeosade liitmine transmissioonivõrku
- Võrgu retransleerimiseks.

Võrgusõlmede vahekaugused on sõltuvalt asustusest ja maapinna iseärasustest 30 kuni 40 kilomeetrit, kuid Tallinnas võib nende vahemaa olla isegi ainult 5 kilomeetri piires.

Kõik võrgusõlmed on varustatud alljärgnevate seadmetega:

- Raadiomast - sõltuvalt asukohast 30 kuni 100 meetrit maapinnast;
- piirdeaed ümber masti ja/või aparatuuri ruumi;
- aparatuuri ruum:
 - konteiner masti all;
 - statsionaarne ehitis – väeosa/asutuse nõrkvooluruum;
- raadiorelee seadmed;
- ATM seadmed;
- Kaughaldus seadmed
 - IP põhised seadmed;
 - GSM Data seadmed;
- valvesüsteemiseadmed;
- kliimaseadmed;
- katkematu toiteallikad;
- elektrigeneraator;
- automaatne tulekustutussüsteem elektrigeneraatori ruumis;
- mehitatud valve;

Kõik võrgusõlmed ja neis olevad seadmed, väljaarvatud väeosade sisene transmissioon, on pideva 24/7 monitoorimise all. Monitoorimist teostatakse monitoorimiskeskuse poolt asukohaga Tallinnas ja süsteemis esinevate rikete korral võetakse ühendust tehnikutegrupiga, asukohaga Tallinnas ning edastatakse töökäsk rikke kõrvaldamiseks.

ASUTUSESISESEKS KASUTAMISEKS

Sellise töökorralduse juures on ainult üks probleem – tehnikute grupp peab olema alati kättesaadav ja võimeline liikuma ükskõik kuhu Eesti Vabariigi otsa vähemalt 12 tunniga. Hetkel on olemas 1 grupp ja seegi koosneb rohkem süsteemi peadministratoritest kui tehnikutest.

2.4. Väeosa/asutuse transmissioonivõrk

Kaitsejõudude väeosad asukohad on suuresti I Eesti Vabariigi ja Nõukogude Liidu sõjaväeosade paiknemiskohtades. Väga vähesed struktuuriüksused on uusehitistes, kuid sellest hoolimata on kaitseministeeriumi haldusalas olevatel üksustel vägagi kaasaegne nõrkvooluvõrk. Hoonete renoveerimisel on kaasajastatud, ümber ehitatud olemasolevad nõrkvooluvõrgud nii, et need vastavad tänapäevastele standartidele (ISO/IEC 11801, ANSI/TIA/EIA-568).

Nõrkvooluvõrkude renoveerimine/uuendamine ei ole seisnenud mitte ainult füüsilise ühenduse vaid ka võrguseadmete uuendamises. Kaitseministeeriumi hangete alusel on soetatud arvutivõrkudesse erinevaid võrguseadmeid. Peamiste aktiivseadmetena võib välja tuua erinevaid Cisco ja Enterasys`i ruutereid ja võrgulüliteid, samuti serverite ja telefonikesjaamade tärned. Soetatavad seadmed olid suuresti ostetud Foreign Military Financing (FMF) rahadest⁹. FMF raha – Ameerika Ühendriikide poolt liitlasriikidele eraldatav rahaline summa, mille eest siis ostetakse Ameerika Ühendriikide firmadelt peamiselt kaitseotstarbelisi tooteid/teenuseid, või finantseeritakse erialaseid koolitusi Ameerika Ühendriikide sõjaväekoolides¹⁰.

Väeosadesse paigaldatud võrguseadmed olid võimekad Vlan, Tagged ja Untagged paketid, MAC aadressipõhised load, spanning tree on ainult väike osa „tarkusest”. Soetatud seadmed olid küll väga head ja „targad”, kuid inimesed, kellele need kasutada anti ei osanud ega teadnud ka soovida, mida uued seadmet teha oskavad. Seadmed paigaldati väeosadesse, kuid seadmete haldamise kohta ei saadud mitte mingitki koolitust – 20000 kuni 30000.- krooni maksev Enterasys`i või Cisco toodangust pärinev OSI¹¹ mudeli järgselt Layer 2 või koguni Layer 3 oskav võrgulüliti oli kasutuses kui odav 400 kroonine hub oma Layer 1 oskusega.

ASUTUSESISESEKS KASUTAMISEKS

Reeglina on igal väeosal kasutada hooneid ühest kümneteni samal territooriumi ja need kõik on omavahel kokku liidetud üheks ühtseks süsteemiks ja ühte hoonesse, reeglina staabihoonesse, on koondatud enamus teenusservereid ja telefonikeskjaam. Väeosade nõrkvoolu ruumid võib jagada alljärgnevalt:

- Keskne sideseadmete ruum;
- Keskne valvesüsteemi ruum;
- Side- ja valveseadmete ruum;

2.4.1. Keskne sideseadmete ruum

Kesknes sideseadmete ruumis on tavaliselt koos kogu väeoas IKT alane teave. Selles ruumis on nii erinevaid funktsioone täitavaid servereid, varundusseadmeid kui ka reeglina maja sisend väljund magistraal kaablid:

- Valguskaabel – andmeside ühenduste jaoks;
- Vaskaabel – eelkõige telefoniside jaoks, kuid võib kasutada ka valveseadmete ja andmeside ühenduste jaoks ;

Serverite varundamine toimub vastavalt kehtivatele eeskirjadele, mis võivad olla väeosade kaupa erinevad, kuid siiski on dokumendi raam kui selline olemas ja ka rakendatud.

Kesknes sideseadmete ruumis on reeglina alljärgnevad vahendid:

- Telefonikeskjaam – kas digitaalne või siis IP põhinekeskjaam firmalt „Avaya”;
- Server (id) – reeglina rackitavad;
- Kaughaldus seadmed – näiteks IBM Remote Server Adapter (RSA), GSM Data seadmed;
- Võrgulülitid - manageeritavad, peamiselt Enterasys`i või Cisco toodangust ;
- Varunduse seadmed – reeglina LTO¹² või DLT¹³ seadmed, kuid esineb ka eraldi varundusservereid – automaatseid varundus seadmeid ei ole kasutusel;
- DSL ühenduste seadmed – nii ADSL kui ka VDSL¹⁴ ühenduste seadmed;
- Patch`i paneelid – ühenduste kokkuliitmiseks;
- Konditsioneer – sõltuvalt ruumi suurusest 2 kuni 3 tükki;
- Katkematu toite allikas UPS – suudab süsteeme töös hoida 70- protsendilise koormuse juures orienteeruvalt 45 minutit.

ASUTUSESISESEKS KASUTAMISEKS

- 19" Racki kapid erinevates kõrguse ja sügavuse mõõtmetega;
- Hügromeeter koos temperatuuri anduri;
- Tuletõrje/valve signalisatsioon, võimalusel ka automaatne gaaskustutussüsteem;
- Magistraalkaablite sisend ning väljund;
- Valvestatav ala koos videovalve kaameraga;

Lisaks on antud ruum reeglina varustatud ka reservtoitega statsionaarsest elektrigeneraatorist, mille rakendumise ajaks on 1 minut alates elektrivoolu kadumisest hoone peakilbist ja stabiilse, pinge kõikumisteta elektrivooluga (~230 V AC) peakilbi varustamine alates 5ndast minutist.

2.4.2. Keskne valveseadmete ruum

Sarnaselt keskse sideseadmete ruumiga on kesksesse valveseadmete ruumi koondatud antud süsteemi tööks vajalikud seadmed.

Keskses valveseadmete ruumis on reeglina alljärgnevad vahendid:

- Monitorid valvuritele kaamerate jälgimiseks;
- Videosalvesti(d) – kaamerateest saabuva pildi salvestamine;
- Server(id) – läbipääsukaardid, automaatne tulekustutussüsteem,
- Võrgulülitid;
- Patch`i paneelid – ühenduste kokkuliitmiseks;
- 19" Racki kapid erinevates mõõtudes;
- Konditsioneer – sõltuvalt ruumi suuruselt 2 kuni 3 tükki;
- Hügromeeter –
- Tuletõrje/valve signalisatsioon, võimalusel ka gaaskustutussüsteem;
- Valvestatav ala koos videovalve kaameraga

2.4.3. Side- ja valveseadmete ruum

Eelnevates punktides [2.4.1](#) ja [2.4.2](#) mainitud ruume on reeglina ühes väeosas alati üks, väga harva on neid dubleeritud – pole tegu nii missioonikriitilise tööga. Lisaks eelnevalt mainitud ruumidele asub igas hoones oma ruum, kuhu selle hoone/ehitise IKT ja valve- seadmed koonduvad. Kuna seadmete hulk, mida kasutatakse kõrvalhoonetes on tunduvalt väiksem kui

ASUTUSESISESEKS KASUTAMISEKS

peahoones, siis reeglina on enamasti side- ja valveseadmed koondatud ühte ruumi ja sageli võivad nad ka asuda ühes racki kapis, mis on pooleks jaotatud. Suuremate hoonete puhul võib side- ja valveseadmete ruume olla ka hoone igal korrusel.

Side- ja valveseadmete ruumis asuvad

- Võrgulülitid - manageeritavad, peamiselt Enterasys;
- Erinevad patch`i paneelid – ühenduste kokkuliitmiseks;
- Konditsioneer – sõltuvalt ruumi suuruselt 1 kuni 2 tükki;
- Katkematu toite allikas UPS – suudab süsteeme töös hoida 70 protsendilise koormuse juures orienteeruvalt 120 minutit.
- 19” Racki kapp (id), mis on võimalik jagada kaheks eraldi seisvaks osaks ;
- Hügromeeter;
- Tuletõrje/valve signalisatsioon, võimalusel ka gaaskustutussüsteem;
- Magistraalkaablite sisend
- Valvestatav ala koos videovalve kaameraga

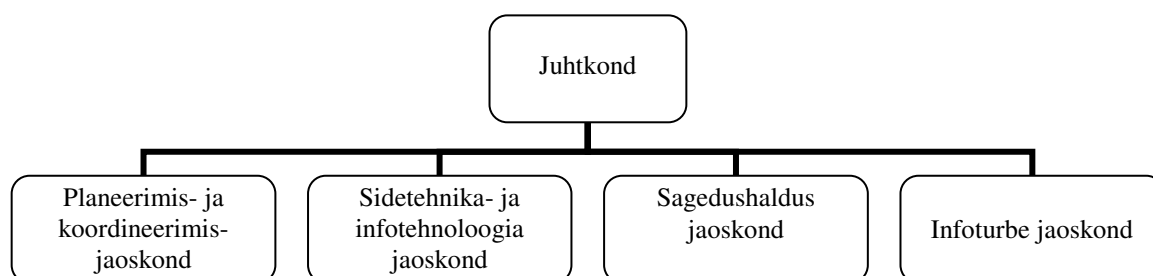
3. Info- ja kommunikatsiooni tehnoloogia juhtimine ja haldus kaitsejõududes.

Kaitsejõududes võib antud hetkel välja tuua kaks eraldi seisvat taset IKT juhtimises ja haldamises:

- Kaitsejõudude Peastaabi J6 – strateegiline tase;
- Väeosad – operatiivne tase;

Sii nimistusse tuleks lisada ka Side- ja Infosüsteemide Väljaõppekeskus ja Arenduskeskus (edaspidi SIVAK), mille peamiseks ülesanneteks on IKT erialased koolitused ja IKT-alane arendustöö kaitsejõudude siseselt kaasates vajadusel selleka ka erafirmasi.

3.1. Kaitsejõudude Peastaabi J6



Joonis 2

Kaitsejõudude IKT-alase arengu koordineerimine ja juhtimine on pandud J6 õlgadele. J6.-e erinevad osakonnad koordineerivad nii administratiiv- kui ka militaar IKT vahendite tsentraalset soetamist, kaitsejõudude IKT teenistuste inimeste väljaõpet ning koostööd teiste riikidega, sagedushaldust kaitsejõududes, infoturvet ja lisaks sellele pakuvad nad ka kasutajatuge Kaitsejõudude Peastaabile ja teistele staapidele (Maaväe staap. Õhuväe staap. Mereväe staap), kes asuvad samas hoones peastaabiga.

Vastavalt eelpool loetletud ülesannetele on ka J6 struktuur suunatud rohkem strateegilisele planeerimisele ja koordineerimisele, aga mitte operatiivsele juhtimisele ning arendustööle.

ASUTUSESISESEKS KASUTAMISEKS

Side- ja infosüsteemide alase arendustööga kaitsejõudude siseselt peab tegelema SIVAK, vastavalt J6`st saadavatele arengusuundadele.

Sidetehnika- ja infotehnoloogiajaoskonna peamised ülesanded on:

- Raadio- ja traatside vahendite hanked – nii missiooni, kui ka ajateenijatest koosnevad allüksused;
- Transmissioonivõrgu arenduskava koostamine ja finantsvahendite planeerimine;
- Tarkvara haldus ja hanked – NATO annab oma liikmesriikidele igal aastal Microsofti toodete litsentse, mida saab kasutada asukohamaades. Lisaks on kasutusel mitmete tarkvara tootjate korporatiivsed litsentsid – antiviiirus, Windows, jne.

Samas on hetkel olukord, kus väeosad peavad ise soetama endale enamuse tarkvarast ja seda mitte riigiasutuse (government) ega ka korporatsiooni (corporate) litsentsiga vaid tavatingimustel. Eriti puudutab see olukordi, kus väeosa vajadus piirneb viie kuue litsentsiga, kuid sedasi soetavad sama tarkvara mitu väeosa ongi juba litsentside arv kasvanud kolme- neljakümne piirile ja saavutatud mingigi soodustus tarkvara hankel. Kaitsejõududes kehtiv finantspoliitika ja litsenseerimise tingimused ei luba ka rakendada sellist skeemi, et üks väeosa ostab mingi tarkvara paketi ja annab/müüb teistele väeosadele kasutada.

- Kõik väeosad on eraldi seisvad juriidilised isikud, kes on kantud äriregistrisse – litsenseerimistingimused;
- Väeosa ei tohi teenida tulu – seega soetatud tarkvara eest ei ole võimalik teistelt väeosadelt saada finants ega ka muid materjaalseid vahendeid.

Kui soetataks tarkvara tsentraalselt ja selle üle peetaks ka arvestust senisest paremal kujul, saavutataks kindlasti finantsvahendite kokkuhoid. Kaitsejõudude peastaap, kui antud organisatsiooni pea, omab õigust jagada alluvatele tarkvara, ise selle pealt tulu mitte teenides;

- Infotehnoloogia vahendite tsentraalsed hanked;
- Osalemine erinevates NATO töögruppides – igal NATO riigil on võimalus, kui mitte öelda lausa kohustus osaleda mõningastes töögruppides ja anda omapoolne panus antud eriala arengusse kõigile NATO liikmesriikidele ;

ASUTUSESISESEKS KASUTAMISEKS

J6`e sidetehnika- ja infotehnoloogia jaoskond on, arvestades neile püstitatud eesmärke, liiga väiksekoosseisuline – nende koosseisu suurus jääb alla isegi suuremate väeosade IKT teenistusele. Koosseisu suurendamist takistavad tegurid on:

- Kaitsejõudude suurus – Igale NATO riigile on antud ette piirarv, kui suur võib olla tema palgaline koosseis. See puudutab nii kaitseväelasi kui ka avaliku teenistuse seaduse alusel töötajaid. Koha juurde saamiseks antud osakonda, peab keegi teine selle koha loovutama.
- Tasustamise tingimused – avaliku sektori teenistujate tasustamise tingimused (palk, lisahüved) ei ole konkurentsivõimelised erafirmadega konkureerimiseks;

3.2. Väeosa

Väeosadesise IKT teenistuse eest on vastutav väeosa IKT teenistuse ülem. Juhised väeosa IKT arengu planeerimiseks ja kavandamiseks peaks ta saama oma väeosa ülemalt ja J6`st. Väeosa ülemalt peab ta saama informatsiooni järgnevatel aastatel toimuvatest või planeeritavatest organisastiooni ümberkorraldamistest – IKT vahendite hange läbi J6 või planeerida oma väeosa eelarvesse. J6`st peab ta saama raamistiku ja juhised, kuhu poole on kavas järgneva viie aasta jooksul liikuda ning millised vahendid tulevad tsentraliseeritud korras ja millised tuleb väeosa eelarvesse planeerida. Kahjuks peab tõdema, et antud ajahetkel ei saada informatsiooni ei väeosaulemalt ega ka juhiseid J6`st.

Sõltuvalt väeosa suurusest on kogu IKT teenistuse suurus 2 -3 kuni 8 inimeseni, siin- hulgas ei kajastu väeosade sidesõlmed personal. Antud inimestest on reeglina 1 kuni 3 sideohvitseri ja/või allohvitseri ning 1 kuni 3 infotehnoloogia spetsialisti.

Erinevate väeosade IKT teenistused on komplekteeritud erinevatel tasemetel inimestega – võib leida nii IKT vallas kõrgharidust omavaid inimesi kui ka keskharidusega, ilma IKT kallakuta inimesi, kes täidavad mingeid omi kindlaid rolle antud asutuses. Ebahütlase taseme peamiste põhjustena võib välja tuua järgneva:

- Erialased teadmised;
- Kaadripuudus;
- Kaitsejõudude tsentraalse IKT arengukava puudumine/mitteteadmine;
- Kehvad tasustamistingimused võrreldes erasektoriga;

ASUTUSESISESEKS KASUTAMISEKS

Väeosa IKT teenistuse koosseis:

- Kaitseväe ohvitser, kes reeglina juhib antud väeosa IKT teenistust. Saanud sõjaväelise juhtimisalase õppe koos siderühma ülema erialakursusega Kaitseväe Ühendatud Õppeasutustest. Oskab koolitada ajateenijatele kuni pataljoni tasemele kasutusel olevaid militaar sidevahendeid – taktikalised raadiojaamad ning nende seadistamine, välikaabel ja välitelefoni, kuid ei tea ega pole ka õpetatud, kuidas antud vahendid töötavad. Koolis õppides on talle tutvustatud MS Office paketti ja räägitud andmeside üldistest alustest, saab üldjuhul hakkama arvutisse Microsofti toodangu installeerimisega, serveritest ja võrgulülititest ei tea reeglina midagi;
- Allohvitser-instruktor – aitab teostada koolitust ja kontrollib sidevahendite kasutamist. Reaalselt on läbinud jalaväeinstruktori kursuse või sideallohvitseri baaskursuse. Oskab koolitada kuni pataljoni tasemele militaar sidevahendeid. IT alased teadmised on reeglina saadud kas iseõppimise teel või IT spetsialisti poolt õpetatud. Mõnedes väeosades on siia kategooriasse kuulumas ka üksikud IT spetsialistid, kes on kaitsejõududes tegevteenistuses. Nende kohta kehtib järgnev punkt -Infotehnoloogia spetsialist;
- Infotehnoloogia spetsialist – omab baasteadmisi infotehnoloogiast. Need teadmised on omandanud gümnaasiumis õppides, reaalse töö käigus, väeosast koolituste võimaldamisega või omal vabal tahtel manuaalidest õppides. Reeglina puudub läbitud kursuste kohta sertifikaat, kuna ta peab seda ainult paberitükiks, mida on võimalik kõigil raha eest osta. Peab ennast kõige targemaks IKT küsimuste alal antud väeosa territooriumil või isegi terves kaitsejõududes. Võib esineda ülemate teadmatust ära kasutades valetamise episoode. Teab, mis on OSI mudel, kuidas arvutisse tarkvara installeerida, kuid reeglina puuduvad oskused võrguseadmete haldamiseks.

Eesti Vabariigis on antud hetkel, st. aastal 2007 veel majanduskasv ning pidevalt võime lugeda- kuulda ajalehtedest ja televisioonist, et on puudu erinevate erialade spetsialiste. See ongi loonud olukorra, kus kaitsejõududest on lahkunud paljud ohvitserid/allohvitserid ning paljud planeerivad lahkumist. Lahkumise ajendiks on enamasti kehvemad tasustamistingimused kui erasektoris ja vähema pingelisusega töö. Siiani on suurem lahkumiste laine mööda läinud IKT teenistujatest, kuigi nende tasustamine ei ole võrreldav

erasektoriga, on siiski siiani neid suudetud tasustada paremini kui teiste valdkondade teenistujaid.

Tsentraalse IKT arengukava puudumine on viinud hetkeks kaitsejõud olukorda, kus erinevad väeosad osutavad samalaadset teenust, kuigierineval kujul. Eriti raske olukorra ette seab see tavakasutaja, kes pole kuigi tuttav erinevate infotehnoloogiliste rakendustega. Iga kaitseväe ohvitser peaks kolme kuni viie aastase teenistuse järel ühes väeosas vahetama oma teenistuskoha (väeosa) ehk roteeruma.

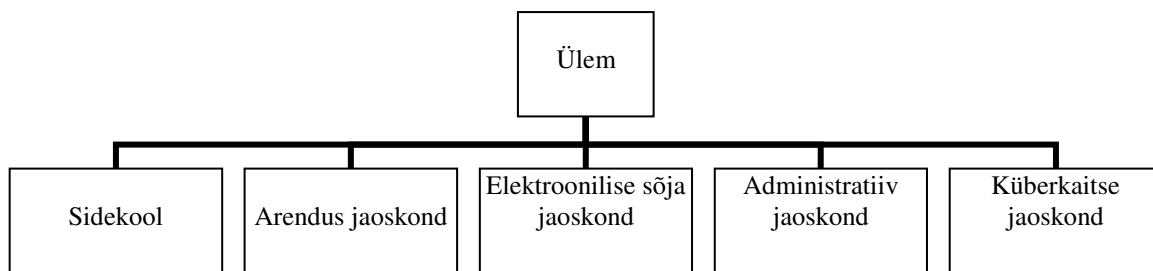
Kuidas see tavakasutajat puudutab? Oma töökohas LtVök Tapa Väljaõppekeskuses oleme me rakendanud näiteks SQL¹⁵ andmebaasil põhineva elektroonilise toidutellimise, maksnud selle kirjutamise eest firmale sümboolse summa raha ja saanud vastu igati toimiva kasutajale suuremat vabadust andva süsteemi endale toitu ettetellimiseks. Samas ülejäänud väeosad kasutavad siiani aastast 1992 pärit paberil tellimist ja heietavad vaikselt mõtet analoogse rakenduse käivitamiseks. Samalaadseid näiteid võib tuua veel teisigi, mis väeositi on erinevad – kas siis kasutaja või süsteemi poolt vaadates.

Märki tsentraalsusest kannab antud hetkel Kaitseministeeriumi ja Kaitsejõudude Peastaabi poolt kord aastas läbiviidav arvutite riigihange. Antud hanke jaoks vajaminevad lähteandmed võetakse enamjaolt õhust. Iga väeosa küll esitab omad vajadused peastaapi, kuid sealt peale hanke lõppu saadav tulem on sageli risti vastupidine soovitul ja sageli eirab see kasutajate poolt esitatud vajadusi. Taotluses märgitakse ära lauaarvutite, sülearvutite ja serverite vajadus ning igas kategoorias lisatakse, millisel otstarbel on planeeritud antud tehnika kasutamine – GIS rakendused, kontoritöö, andmebaasi server jne., kuid taotleja ei pruugi saada endale mitme aasta jooksul mitte ühtegi serverit tsentraalselt.

3.3. Side- ja Infosüsteemide Väljaõppe ja arenduskeskus

Antud struktuuriüksus on moodustatud kaitseväes 2001. aastal ja praegusel ajahetkel on ta üks osa Kaitseväe Ühendatud Õppeasutustest. SIVAKI loomise eesmärgiks oli parandada ja ühtlustada kaitseväelaste ja teenistujate IKT- alaseid teadmisi ning oskusi. Lisaks sellele oli üheks peamiseks eesmärgiks saada üheks NATO IKT kompetentsikeskuseks, andes Eestile oma erialase nishi, millega saadakse ollakse kasulik kõigile NATO liikmesriikidele.

ASUTUSESISESEKS KASUTAMISEKS



Joonis 3

Administratiivjaoskonna peamised funktsioonid on:

- Igapäevaste töövahendite tagamine;
- Juhend- ja õppematerjalide tootmine;

Sidekooli peamised funktsioonid on:

- Sideeriala nooremohvitseride ja vanemallohvitseride koolitus;
- Erialaste juhend- ja õppematerjalide koostamine;
- E-õppekeskkonna „Ilias” haldus ja arendus koostöös Kaitseväe Ühendatud Õppeasutustega;

Arendusjaoskonna peamised funktsioonid on:

- J6 poolt soetada plaanitavate IKT vahendite testimine enne soetamist;
- Tarkvara kirjutamine;
- Transmissioonivõrgu seadmete haldamine koostöös monitooringu keskusega;

Elektroonilise sõja jaoskonna peamised ülesanded on:

- Kaitseväelaste ja teenistujate koolitamine antud erialal;
- Erialaste juhend- ja õppematerjalide koostamine;

Küberkaitse jaoskonna peamised ülesanded on:

- Kaitseväelaste ja teenistujate koolitamine antud erialal;
- Erialaste juhend- ja õppematerjalide koostamine;

ASUTUSESISESEKS KASUTAMISEKS

Antud ajahetkeks on need struktuuriosad komplekteeritud ja on olemas ka juba esimesed valmisproduktid antud väeosast. Sidekooli on lõpetanud neli lendu ohvitsere ja kaks lendu allohvitsere, Elektroonilise sõja jaoskonnal on valmimas erialane film mida kujutab endast elektrooniline sõda ja kuidas end selle mõjude eest kaitsta, Küberkaitse jaoskond on saavutamas erialaselt aksepteeritavat kohta NATO-s – olles antud erialal teerajaja, Arendusjaoskonnas on valminud mobiilse taktikalise transmissioonivõrgu testprojekt.

Lähtudes struktuurist ja ka peamistest funktsioonidest peaks arendusjaoskond tagama kogu kaitsejõududesse tsentraalselt soetatava riist- ja tarkvara testimise ning tarkvara moodulite kirjutamise. Antud hetkel see päris hästi ei toimi ja paljud väeosad tellivad endale tarkvara kirjutamist erafirmadest.

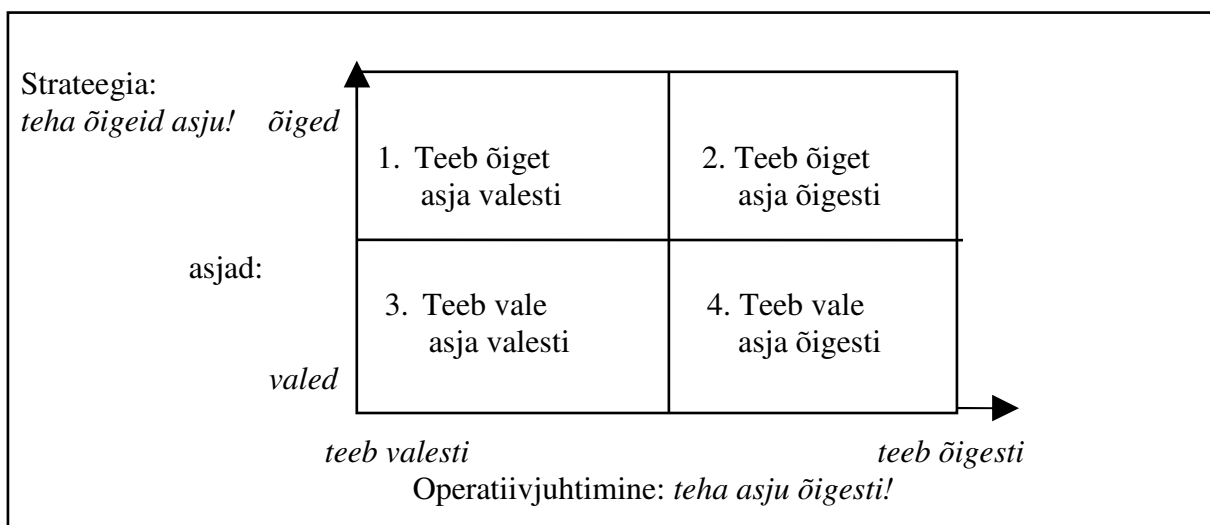
4. Tsentraalse juhtimise ja halduse mudel

Kaitsejõudude Peastaabi J6 üheks peamiseks ülesandeks on tagada kaitsejõudude IKT- alane areng ja seda arengut koordineerida. Milles koordineerimine seisneb - ei ole täpsustatud – kas ainult direktiivide ja määruste kirjutamises või hoopis IKT vahendite tsentraalses haldamises? Antud töö osas toon välja erinevad tasemed, kuidas oleks võimalik kaitseväe IKT teenistust tsentraalselt hallata ja juhtida

4.1. Juhtimine

Juhtimisel on mitu taset - institutsionaalne, strateegiline, operatiivne. Kui operatiivne juhtimine aitab organisatsioonil teha asju õigesti, siis strateegiline juhtimine on vajalik selleks, et teha õigeid asju (vt. joonis 4). Kui strateegiline juhtimine puudub, võib juhtuda, et organisatsioon liigub innukalt vales suunas ja mida rohkem ta pingutab, seda hullemaks olukord läheb. Ehk teisiti öeldes - võib juhtuda, et inimeste kvalifikatsioon on hea, inimeste motivatsioon on hea, aga organisatsiooni orientatsioon on vale.

Strateegiline ja operatiivjuhtimine (B.Karlöf)



Joonis 4

Juhtimise tasandid:

- Institutsionaalne juhtimine - omanikusuhe, poliitiline võim - Kaitseväe juhtkond
- Strateegiline juhtimine - arengusuuna ja ressursside kohta käivad otsused pikemas perspektiivis - Kaitsejõudude Peastaabi J6

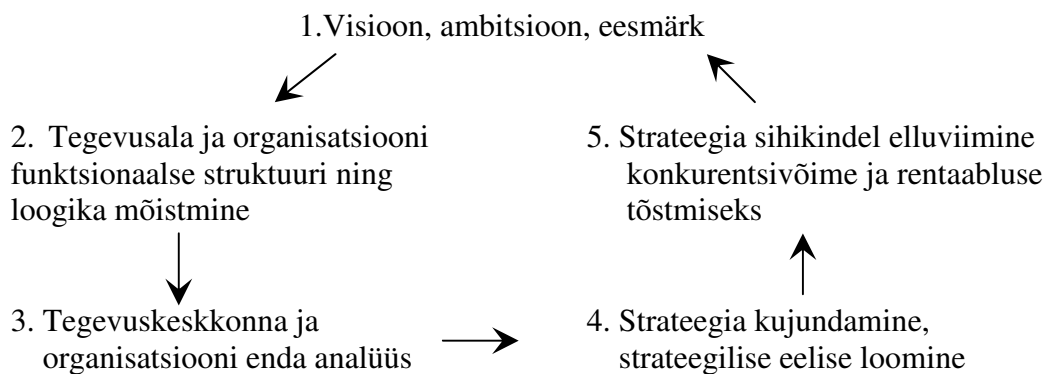
ASUTUSESISESEKS KASUTAMISEKS

- Taktikaline juhtimine - ressursside kasutamine, suunamine ja vajadustele kohandamine
- Regionaalne keskus;
- Operatiivjuhtimine - tööpanuse muutmine tulemuseks. Väeosa.

Strateegia:

- Eesmärk on lõpptulemus, mida püütakse saavutada. Eesmärk tuleb väljendada sellisel kujul, et tema saavutamise taset oleks plaanitava perioodi lõpus võimalik mõõta.
- Strateegia on kokkuvõte sellest, kuidas kavatakse eesmärkideni jõuda. Strateegia kavandamine on strateegilise planeerimise üks osa. Strateegiline planeerimine on strateegilise juhtimise üks osa.
- Poliitika: eelnevalt tehtud püsiv otsus, mis määratleb organisatsiooni seisukoha(d) kõigi olulisemate korduva iseloomuga asjade, nähtuste ja olukordade suhtes.
- Planeerimine: ressursse siduva tegevuskava koostamine eelseisvaks perioodiks. Firmades on strateegilise planeerimise keskpunktis turupositsiooni kindlustamine ja pikaajaliste tegevussuundade arendamine.

Strateegiline protsess



Joonis 5

Strateegiline planeerimine on organisatsiooni juhtkonna ülesanne, kes organiseerib õiged inimesed otstarbekohase ajakava alusel koguma süstemaatilist teavet eesmärgiga teha pikaajalist perspektiivi puudutavaid otsuseid inimeste ja finantside jaotuse kohta organisatsiooni erinevate tegevussuundade vahel.

ASUTUSESISESEKS KASUTAMISEKS

Strateegiatöö on eriti oluline, kui tegutsetakse ebakindlas, kiiresti muutuv, turbulentse keskkonnas. Turbulentsele keskkonnale on iseloomulik alljärgnev:

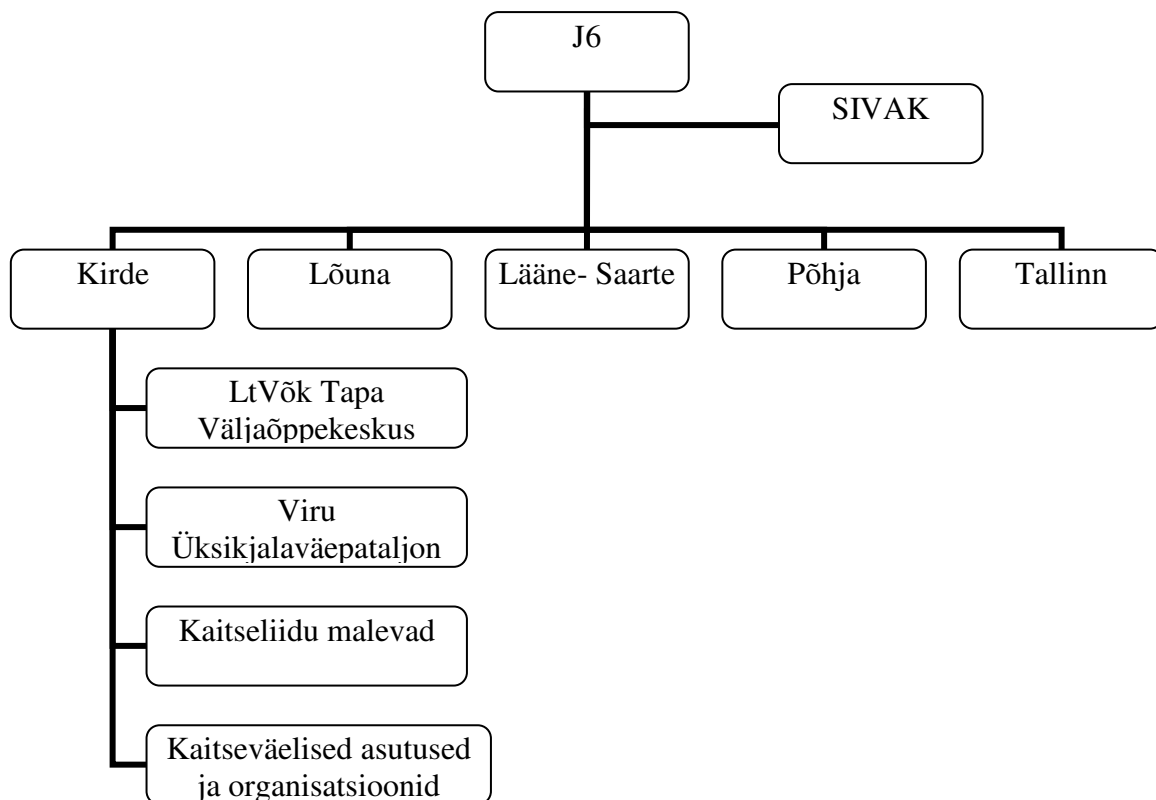
- kasvab sündmuste uudsuse aste - varasemast kogemusest on järjest vähem kasu;
- tugevneb tegevuskeskkonna mõju - järjest rohkem ressursse nõuavad sellised tegevused nagu suhtekorraldus, monitooring, nähtuste jälgimine ja analüüs;
- suureneb keskkonna muutumise kiirus - kiireneb infotöötlus ja -kasutus;
- kasvab keskkonna keerukuse aste - võimalikud hälbepildid levivad kiiremini, kergemini ja laiemalt kui varem, nõrgeneb sündmuste, protsesside, tendentside kontrollitavus.

IKT maailm on oma olemuselt turbulentne - paljud tehnoloogiad mida veel paari aasta eest peeti uuenduslikeks on asendunud veelgi parematega.

4.2. Kaitsejõudude IKT juhtimise ja halduse mudel

Kas kaitsejõudude IKT teenistust saab võrrelda suurfirmade, korporatsioonide analoogsete teenistustega? Kindlasti, sest oma arvutipargi suurusega kuuluvad kaitsejõud kindlasti Eestis ühtede suurimate asutuste hulka. Võib väita, et arvutit kasutab töö juures pea 75% teenistujatest eelkõige oma tööülesannete tõttu, olgu selleks siis raamatupidamine või allüksuse veebel – neil kõigil on oma tööpäev as arvuutil oma kindel koht. Sama võib ka väita kaitsejõudude telefonide koha – pea 75% teenistujatest on oma ametikohaga kaasnev lauatelefoni number.

ASUTUSESISESEKS KASUTAMISEKS



Joonis 6

Antud joonis on põhimõtteline nägemus sellest, kuidas võiks kaitsejõududesiseselt välja näha tsentraalne IKT juhtimine koos kõigi oma erinevate tasemetega.

Joonisel on erinevad tasemed oma vahel ühendatud ja eristub 3 taset.

1. Strateegiline juhtimine – J6
2. Taktikaline juhtimine - Regionaalne keskus – Põhja, Kirde, Lõuna, Lääne-Saarte ja Tallinn
3. Operatiivne juhtimine - Väeosa – antud joonisel LtVõk Tapa Väljaõppekeskus, Viru Üksikjalaväepataljon, Kaitseliidu malevad ja kaitsevälised asutused ja organisatsioonid

4.2.1. Side- ja Infosüsteemide jaoskond – J6

Hetkel olemas oleva struktuuriga üksus, mille peamiseks rolliks on strateegiline juhtimine ja planeerimine. Uue struktuuri kohaselt oleks Sidetehnika- ja infotehnoloogia jaoskonna hallata alljärgnevad osad.

ASUTUSESISESEKS KASUTAMISEKS

- Riist- ja tarkvara hanked, ning nende lähteülesannete täpsustamine;
- Kaitsejõudude transmissioonivõrgu arengu ja finants vahendite planeerimine;
- Tarkvara haldus;
- Militaar sidevahendite hankimine;
- Uus ehitiste side- ja valveseadmete lähteülesannete koostamine koostöös väeosaga;

Hangete läbiviimine on pikk ja keeruline protsess, eriti arvestades too koostamise hetkel kehtivat seadusandlust, kus üle kolmasaja tuhande (300 000) eesti krooni suurune ost läheb riigi hankesse. Alates 01.05.2007 tõuseb riigihanke piirsumma viiesaja tuhande (500 000) eesti kroonini. Senine praktika erimenetluseta riigihangete osas näitab, et hanke lähte ülesanded päevad olema vägagi detailselt lahti kirjutatud, et vältida hilisemaid kohtus käimisi hanke kaotanud osapoole(te)ga. Hangete teostamiseks tuleks Sidetehnika- ja infotehnoloogia osakonda luua juurde ametikohad hangetega tegeleva personali jaoks, ning see personal peab olema IKT alaste teadmistega. Antud hetkel viib kaitsejõududes tsentraalseid hankeid läbi Kaitsejõudude Peastaabi Logistika osakond (edaspidi J4) vastavalt hangete lähteülesannetele, kuid J4`jas puuduvad IKT alaste spetsialistis tasemel teadmistega teenistujad.

4.2.2. Side- ja Infosüsteemide Väljaõppe- ja Arenduskeskus – SIVAK

Antud struktuuri rakendumisel oleks SIVAK peamine organisatsioon, mille kaudu hakkaks toimuma vastavalt J6 arengukavadele ja vastavalt tekkinud vajadustele tsentraalselt koordineeritud IKT alane arendustöö ja erialaste koolituste läbiviimine. See peab hõlmama endas alljärgnevaid osi, mis võivad olla omavahel seotud:

- Riistvara testimine;
- Tarkvara testimine;
- Tarkvara loomine;
- Riist- ja tarkvara alased koolitused

Kogu selle võimekuse saavutamiseks ei pea SIVAK`i koosseisu suurendama drastiliselt. Osa eelpool loetletud teenustest saab sisse osta ka tsiviilfirmadest, osaledes antud projektis eelkõige kas projektijuhina või siis LIAISON (koostöö) isikuna kahe organisatsiooni vahel ning saades endale kogu dokumentatsiooni testimisest või tarkvara loomisel tarkvara koodi.

ASUTUSESISESEKS KASUTAMISEKS

Antud LIAISON süsteem töötab mitmetes NATO riikides edukalt. Siin kohas võib ära mainida Hollandi Kuningriigi armee ja nende taktikalise mobiilse transmissioonivõrgu süsteemi „TITAN”. Hollandi analoogne arenduskeskus osaleb eelkõige sõjalise ja tehnilise poole pealt ja tsiviilfirmadest tuleb eelkõige seadmete ja tarkvara arenduse pool.

Antud hetkel on Eestis samalaadne kooslus märgata oma taktikalise mobiilse transmissioonisüsteemi hankimisel. SIVAK teeb läbi J6 ja Kaitseministeeriumi koostööd hanke võitnud Eesti IKT firmaga. See koostöö hõlmab endas nii süsteemi funktsionaaluse kirjeldamist, testimist, süsteemi väljaehitust, koolitust kui ka testsüsteemi käikuandmist 2007. aasta teisel poolel.

4.2.3. Regionaalne halduskeskus

Hetkel regionaalse juhtimise ning halduse struktuuriüksused puuduvad. Üksused tuleks moodustada soovituslikult mingi väeosa juurde, kuid J6 otsealluvusesse nii erialaselt kui ka finantsiliselt.

Regiooni halduskeskus koosneks

- Keskuse ülem;
- Serverite administraatorid;
- Võrguseadmete administraator;
- IT spetsialist;

Keskuste ülesanneteks on alljärgnev:

- Kaitsejõudude transmissioonivõrgu seadmete esmane hooldus;
 - Valvekeskusest saadud veateadetele reageerimine;
- Regiooni serverite haldamine;
 - Installeerimine;
 - Varundamine;
 - Kasutaja kontode haldus;
- Regiooni telefonikeskjaamade haldamine;
 - Telefoninumbrite haldamine;
 - Kasutajaõigused;

ASUTUSESISESEKS KASUTAMISEKS

- Numbrite lisamine ja eemaldamine;
 - Krosseeringute tegemine;
- Võrguseadmete haldamine:
 - Seadmete konfigureerimine;
 - Seadmete uuendamine;
 - Patchimine;
- Regiooni arvutite haldus:
 - Arvutite üle arvestuse pidamine,
 - Arvutihangete lähteülesannete koostamine J6`de;
 - Arvutite remont;
- Regiooni tarkvara haldus:
 - Millised ja palju tarkvara litsentse meil on?
 - Milliseid ja palju tarkvara litsentse on meil juurde vaja?
- Regiooni VTC seadmete haldus;
- Regiooni IKT eelarve haldamine (väljaarvatud kõneside teenused Elioni ja EMT`i)
- Suhtlemine IKT firmadega:
 - Elion – kõne- ja andmeside teenused. Reserv transmissioonivõrgu rikke korral
 - EMT – mobiilside teenused;
 - Elisa – mobiilside teenused;
 -
- Rajatava ametkondadevahelise Operatiivraadioside (ORS) võrguhaldus regioonis:
 - Tetra terminalide haldus;
 - Õigused;
 - Numeratsioon;
 - Koostöö teiste ametkondadega;

4.2.4. Regioonideks jaotamise alused

Eesti Vabariigis läbiviidud haldusreformide tulemusena võib väita, et Eesti on jagatud 5 regiooni: Tallinn, Põhja, Kirde, Lõuna ja Lääne-Saarte. Oma töös kasutan praktiliselt samu termineid, kuid kuna regioonidesse jaotamisel võib olla erinevusi, siis toon alljärgnevalt regioonide kaupa välja suuremad asutused antud alal.

4.2.4.1. Kaitsevägi

Kaitsevägi jaguneb Maa-, Mere- ja Õhuväeks ning keskalluvusega üksusteks. Eesti territoorium on kaetud erinevate kaitsejõudude väeosadega, milledest mõningad asuvad ka hajutatult üle Eesti Vabariigi. Regioonidesse saaks kaitseväge väeosad jagada alljärgnevalt:

- Tallinn – Tallinnas paiknevad väeosad, kaasaarvatud ka Kaitsejõudude Peastaap;
- Põhja – Harjumaal paiknevad väeosad;
- Kirde – Järvemaal, Lääne- ja Ida-Virumaal ning Jõgevamaal paiknevad väeosad;
- Lõuna – Viljandimaal, Tartumaal, Põlvamaal, Valgamaal ja Võrumaal paiknevad väeosad;
- Lääne-Saarte – Pärnumaal, Saaremaal, Hiiumaal, Läänemaal ja Raplemaal paiknevad väeosad.

4.2.4.2. Kaitseliit

Kaitseliit jaguneb 15 malevaks, mille vastutusala kattub välja arvatud mõne erandiga Eesti maakondade piiridega.

1. jaanuarist 2004.a. moodustati Kaitseliidus juhtmalevad. Juhtmaleva staabi põhiülesandeks on Kaitseliidu malevate tegevuse planeerimine ja koordineerimine omal vastutusosal.

Juhtmalevate vastutusalad ja staapide paiknemine on järgmine:

- Alutaguse juhtmaleva vastutusala on Alutaguse Maleva, Jõgeva Maleva, Viru Maleva ja Järva Maleva territoorium. Juhtmaleva staap paikneb Jõhvis
- Harju juhtmaleva vastutusala on Harju Maleva, Rapla Maleva ja Tallinna Maleva territoorium. Juhtmaleva staap paikneb Tallinnas;
- Pärnumaa juhtmaleva vastutusala on Pärnumaa Maleva, Lääne Maleva ja Saaremaa Maleva territoorium. Juhtmaleva staap paikneb Pärnus;
- Tartu juhtmaleva vastutusala on Tartu Maleva, Sakala Maleva, Valgamaa Maleva, Võrumaa Maleva ja Põlva Maleva territoorium. Juhtmaleva staap paikneb Tartus.

Nagu eelpool loetletust näha, saab regionaalsete keskuste arvu sõltuvalt töökorraldusest lugeda suurusjärku 4 kuni 5. Arvestades asjaolu, et Tallinnas asub vägagi palju kaitsejõudude

väeosi, on otstarbekas lähtuda halduskeskuste moodustamisel 5 keskuse põhimõttest, kusjuures kõik keskused töötavad samadel alustel.

4.2.5. Väeosa

Väeosades kaoks IKT teenistused oma senisel kujul – osa nende funktsionaalsusest läheks üle regiooni (haldus) ja arendus läheks üle SIVAK`isse. Väeosas IKT teenistujate peamised ülesanded oleksid alljärgnevad:

- Kaitseväelased:
 - Militaarsidevahendite alane koolitus;
 - Militaarsidevahendite hooldus;
 - Militaarsidevahendite üle arvestusepidamine;
- Infotehnoloogia spetsialist:
 - Kasutajatoe pakkumine;
 - Kasutajate vajaduste edastamine regiooni:
 - Arvutid;
 - Kasutaja õigused;
 - Tarkvara;
 - Esitlustel tehniline tugi;
 - IT- alaste koolituste vajadus

Väeosadelt kaoks kogu IKT eelarve, kuid sellest hoolimata peavad nad esitama regiooni oma orienteeruvad vajadused järgneva eelarveaastaks – Kõnelimiidid, orienteeruv arv uusi seadmeid ehk teiste sõnadega hakkaks toimuma ressursipõhine planeerimine.

4.3. Juhtimise- ja haldusprotsessi kirjeldus Kirde regiooni näite varal

Joonisel 6 on põhimõtteliselt toodud alluvusskeem ja lahti kirjutatud ka suurem osa Kirde regiooni kuuluvatest väeosadest.

Kirde regiooni kuuluvad alljärgnevad kaitsejõudude väeosad:

- LtVÕK Tapa Väljaõppekeskus;
- Viru Üksik-jalaväepataljon;
- Põhja Kaitseringkonna staap;
- Kaitseväe Logistika keskuse erinevad laod;
- Alutaguse Malev;
- Viru Malev;
- Jõgeva Malev;
- Järva Malev.

Sõjaseisukorra väljakuulutamisel peab antud piirkonda tegevust juhtima ja koordineerima Põhja Kaitseringkonna staap asukohaga Rakvere, Lääne-Virumaa. Kaitseringkonna staabi hoone oleks ka kõige mõistlikum koht antud regioonis, kuhu rajada regionaalne halduskeskus.

- Pole vaja soetada ruume juurde;
- Elektrooniline ja mehitatud valve on olemas;
- Asub praktiliselt regiooni keskpunktis nii geograafiliselt kui ka IKT seadmete hulga poolest.

Väeosadel jäävad alles kõik nõrkvooluruumid. IKT vahendite auditi tulemusena (vaata punkti [4.4.3](#)) võib olulisel määral muutuda kõikide sideseadmete ruumi sisustus. Väeossa jäävad alles teenusserverid, telefonikeskjaam ning varundusseadmed, kuid nende arv võib kas suurendea või väheneda sõltuvalt punktide [4.4.2](#) ja [4.4.3](#) tulemusena.

ASUTUSESISESEKS KASUTAMISEKS

Struktuur

Väeosa	Kehtiv struktuur			Uus struktuur			Muutus			Märkused
	Ohvitserid	All-ohvitserid	IT spetsialist	Ohvitserid	All-ohvitserid	IT spetsialist	Ohvitserid	All-ohvitserid	IT spetsialist	
Põhja kaitseringkond	0	0	1	1	1	0	+1	+1	-1	1 IT spetsialist regiooni
LtVÕK Tapa Väljaõppekeskus	5	2	4	3	3	2	-2	+1	-2	1 ohvitser ja 2 IT spetsialisti regiooni, 1 ohvitser kaitseringkonda
Viru Üksik-Jalaväepataljon	1	1	2	1	1	1	0	0	-1	1 IT spetsialisti regiooni
Kaitseväge logistikakeskuse laod	0	0	0	0	0	0	0	0	0	Puudub reaalne vajadus personali järele
Alutaguse malev	0	1	0	0	1		0	0	0	
Viru malev	0	0	0	0	1		0	+1	0	
Järva malev	0	1	0	0	1		0	0	0	
Jõgeva malev	0	0	0	0	1		0	+1	0	
Regioon	0	0	0	1	0	4	+1	0	+4	
Kokku	6	5	7	6	9	7	0	+4	0	

Tabel 1

ASUTUSESISESEKS KASUTAMISEKS

Kehtiv struktuur

Hetkel on Kirde regioonis IKT teenistujate arv väeosade kaupa alljärgnev:

- LtVÕK Tapa Väljaõppekeskus – 5 sideeriala ohvitseri, 2 sideeriala allohvitseri ja 4 IT spetsialisti;
- Viru Üksik-jalaväepataljon – 0 sideeriala ohvitseri (ametikoht täidetakse 2007 suvel), 1 sideeriala allohvitser ja 2 IT spetsialisti;
- Põhja kaitseringkonna staap – 1 IT spetsialist;
- Kaitseväe Logistika keskuse erinevad laod – 0 inimest;
- Alutaguse Malev – 1 sideeriala allohvitser;
- Viru Malev – 0 inimest;
- Jõgeva Malev – 0 inimest;
- Järva Malev – 1 sideeriala allohvitser.

Kokku – 6 sideeriala ohvitseri, 5 allohvitseri ja 7 IT spetsialisti

Eelpool toodud loetelu peegeldab endas ainult olemasolevat palgalist koosseisu. Kindlasti on mõnes Kaitseliidu malevas tööl erineva arv IKT spetsialiste, kuid neid pole määratud oma maleva sidepealikeks.

Kaitseliidu malevate ja Kaitseväe Logistikakeskuse IKT alane tugi asuvad Tallinnas – vastavalt Kaitseliidu Peastaabis ja Kaitseväe Logistikakeskuse staabis. Seni toimiva mudeli puhul on küllaltki sagedane olukord, kus IKT süsteemi rikke korral tuleb oodata kuni viis (5) tööpäeva, enne kui rike kõrvaldatakse ja taastub süsteemi normaalne töö.

LtVÕK Tapa Väljaõppekeskuse ja Kaitseväe Logistikakeskuse IKT teenistuste juhtide vahel on sõlmitud suuline kokkulepe, et Tapa piirkonnas toetab LtVõk Tapa Väljaõppekeskus Kaitseväe Logistikakeskuse ladusid nii IKT vahendite haldamisel, kui ka rikete kõrvaldamisel. Antud hetkel on toetus alljärgnev:

- Telefonikeskjaama haldus;
- Võrgulülitite haldus;
- Väeosa transmissioonivõrgu haldus;
- Kasutajatugi;

ASUTUSESISESEKS KASUTAMISEKS

- IKT vahendite esmane hooldus;

Eelpool toodud loetelu on näide, kuidas ja millist rolli peab regionaalne halduskeskus hakkama täitma. LtVÕK Tapa Väljaõppekeskus ei saa antud teenuste osutamise eest mitte mingisugustki materiaalselt kasu ega pole ka palgatud eraldi inimest antud töid tegema – seda tehakse ühe osana tööst.

Uus struktuur.

Regionaalse halduskeskuse loomisel võiks IKT personali kogus regioonis olla järgnev:

- Regionaalne halduskeskus – 1 sideeriala ohvitser, 4 IT spetsialisti
 - Keskuse ülem – 1 inimene;
 - Serverite administraator – 1 inimene;
 - Võrguseadmete administraator – 1 inimene;
 - IT spetsialist – 2 inimest;
- LtVÕK Tapa Väljaõppekeskus – 3 sideeriala ohvitseri ning 3 allohvitseri ja 2 IT spetsialisti;
 - Igal väeosal oma sideeriala ohvitser ja allohvitser, arvestades asutuse suurust 2 kasutajatuge pakkuvat IT spetsialisti
- Viru Üksik-jalaväepataljon – 1 sideeriala ohvitser, 1 allohvitser ja 1 IT spetsialist;
 - väeosal oma sideeriala ohvitser ja allohvitser, arvestades asutuse suurust 1 kasutajatuge pakkuvat IT spetsialist;
- Põhja Kaitseringkonna staap – 1 sideeriala ohvitser ja 1 allohvitser;
 - Sideeriala ohvitseri ja allohvitseri peamisteks ülesanneteks on kontrollida antud regiooni väeosade sideerialast väljaõpet, pidada arvestust militaarsidevahendite üle.
- Kaitseväe Logistika keskuse erinevad laod – 0 inimest;
 - Eraldi IT spetsialisti järele vajadus puudub – pole piisavalt tööülesandeid;
- Alutaguse Malev – 1 sideeriala allohvitser;
 - Maleva militaar- sidealase tegevuse juhtimine ja koordineerimine;
- Viru Malev – 1 sideeriala allohvitser;
 - Maleva militaar- sidealase tegevuse juhtimine ja koordineerimine;
- Jõgeva Malev – 1 sideeriala allohvitser;
 - Maleva militaar- sidealase tegevuse juhtimine ja koordineerimine;

ASUTUSESISESEKS KASUTAMISEKS

- Järva Malev – 1 sideeriala allohvitser.
 - Maleva militaar- sidealase tegevuse juhtimine ja koordineerimine;

Kokku – 6 sideeriala ohvitseri, 9 sideeriala allohvitseri ja 7 IT spetsialisti.

Kui võrrelda vana ja uue struktuuri isikkoosseisu suurusi tabelis 1, siis võime tõdeda, et uues struktuuris on sideeriala ohvitseride arv jäänud samaks, kuid nende tööülesanded on muutunud. Sideeriala allohvitseride struktuuriline arv kasvab 4 inimese võrra, eelkõige tänu Kaitseliidu ja väeosadesse uute kohtade lisandumisega. IT spetsialistide arv kogu regioonis ei kasva, kuid nende hulk väeosades muutub.

Keskuse ülem

Keskuse ülema ametikoht oleks sõjaväelase oma ja seda eelkõige 2 põhjusel:

1. sõjaväelasel on olemas juhtimiskogemus
2. väeosadel on valmidus koostöö tegemiseks militaarsfääri kuluva inimesega suurem kui tsiviilisikuga;
3. .

Keskuse ülema ametikoht oleks vanemohvitseri oma – ametikoha auaste major. Ametikohal töötav isik peab omama riigisaladuse töötlemiseks juurdepääsuluba tasemega „Täiesti salajane” ning peaks omama IKT- alast kõrgharidust, soovituslikult IT juhtimise erialal või telekommunikatsiooni erialal.

Keskuse ülema peamisteks töö ülesanneteks oleks:

- Tarkvara litsentside haldus;
- Telefonikeskjaamade haldus;
- Eelarve koostamine ja haldamine;
- Jõude vajaduste edastamine;
 - Tarkvara;
 - Riistvara;
 - Koolitus;

Serverite administraator

Ametikoht oleks kõrgemametniku ametikoht. Ametikohal töötav isik peab omama riigisaladuse töötlemiseks juurdepääsuluba tasemega „Täiesti salajane” ning peaks omama IKT alast kõrgharidust, näiteks Informaatika.

Peamisteks töö ülesanneteks oleks:

- Teenus serverite haldamine
 - Kasutajagrupid, õigused
 - Andmete varundamine;
 - Tulemüüride haldamine ja monitoorimine;

Võrguseadmete administraator

Ametikoht oleks vanemametniku ametikoht. Ametikohal töötav isik peab omama riigisaladuse töötlemiseks juurdepääsuluba tasemega „Täiesti salajane” ning võiks omada IKT alast kõrgharidust, näiteks „Arvuti- ja süsteemitehnika”. Peale selle oleks soovituslik omada Cisco võrguakadeemia CCNA programmi sertifikaati.

Peamisteks tööülesanneteks oleks nii väeosade, kui ka kaitsejõudude transmissioonivõrgus:

- Võrgulülite haldamine;
- Ruuterite haldamine
- Võrguseadmete monitoorimine;
- ATM seadmete haldamine;
- Võrguliikluse analüüs;

IT spetsialist

Ametikoht oleks vanemametniku ametikoht. Ametikohal töötav isik peab omama riigisaladuse töötlemiseks juurdepääsuluba tasemega „Täiesti salajane” ning võiks omada IKT alast kõrgharidust, näiteks „Informaatika”.

Peamisteks töö ülesanneteks oleks:

- IKT vahendite üle arvestuse pidamine;
- IKT vahendite installeerimine;

ASUTUSESISESEKS KASUTAMISEKS

- Kasutajatoe pakkumine jagatud hoone puhul;
- IKT vahendite remont ja hooldus;
- Väeosadesse IKT vahendite transport ja paigaldamine;
- Vajadusel väeosa IT spetsialisti asendamine puhkuse ajal

4.4. Süsteemi rakendamise mudel ja etapid.

Eelpool kirjeldatud süsteemi rakendamine peab toimuma läbi mitme etapi ja iga etapi lõppedes peavad tulemused olema reaalselt mõõdetavad.

4.4.1. Seadusandlus ja alluvusvahekorrad

Esimese punktina tooksin ma välja eelkõige seadusandluse ja alluvussuhete muutmise vajaduse. Nimelt Kaitsevägi ja Kaitseliit on kaks eraldiseisvat struktuuri ja hoolimata igapäevasest koostööst esineb sellest hoolimata probleeme just juhtimisahelas. J6, kes justkui peaks koordineerima Kaitsejõudude Peastaabist nii Kaitseväge kui ka Kaitseliidu IKT erialast arengut, on oma peamise panuse teinud Kaitseväele. See puudutab nii militaar kui ka tsiviil IKT tehnikat ja selle kasutamist igapäevasest töös. Alluvussuhted, nagu sai eelpool töös punktis [4.2](#) kirjeldatud, hakkaksid olema järgmised:

- J6 – juhib ja koordineerib tervet IKT süsteemi kaitsejõududes, tagab arenduse ja koolitused koostöös SIVAK`iga;
- Regionaalne halduskeskus – allub otse J6`le;
 - Palgad tulevad kas Kaitsejõudude Peastaabi eelarvest või Staabi- ja Sideüksuste Väljaõppekeskuse Üksik-Sidepataljoni eelarvest;
 - Logistiline toetus läbi kaitsejõudude Peastaabi – igale regionaalsele keskusele on eraldatud 1 sõiduauto;
- Väeosa – IKT teenistus allub füüsiliselt väeosale, kuid
 - Palgad tulevad väeosa eelarvest;
 - IKT alane koolitus ja arendus läbi regiooni J6`st

Lisaks tuleb muuta Kaitsejõududes kasutusel olevat finantskorda. Antud hetkel on kõik väeosad iseseisvad juriidilised isikud ja maksavad oma IKT teenuste eest ise. Eesti mobiiltelefoniga (edaspidi EMT) on küll Kaitseministeeriumil sõlmitud eraldi leping ja loodud

ASUTUSESISESEKS KASUTAMISEKS

läbi selle kõneside teenustel eraldi sooduspakett, kuid samalaadset lepingut pole suudetud saavutada teiste kasutuselolevate telekommunikatsiooni teenusepakkujatega. Regionaalse halduskeskuse käivitamise puhul hakkaks aga rahalise poolega tegelema halduskeskus. Siia kuuluksid kõik sideteenuste kulud (Elion, Elisa, EMT, kaitsejõudude transmissioonivõrgus väljuvad kõned), mobiil- ja fikstelefonide soetus- ja hoolduskulud, IT vahendite remondikulud (arvutid, serverid, võrguseadmed). Arvutite, serverite ja võrguseadmete soetamine peaks toimuma tsentraalselt läbi J6.

Kirde regiooni näite kohaselt saabuksid kõigi 8 väeosa mobiilside-, fiks telefoniside teenuste, interneti ja satelliittelevisiooni arved halduskeskusesse. Eesmärgiks on saavutada võimalikult minimaalsed kulud tsiviilfirmade vahendeid kasutades. IKT vahendite soetamise, remondi ja hoolduskulude vähendamine eelkõige läbi hangete. Hetkel kõik väeosad sooritavad oste iseseisvalt ja näiteks mobiiltelefonide ostu korral saadav soodustus on keskmiselt 100.- krooni telefoni kohta, hoolimata sellest, kas ostetakse 1 või 20 mobiiltelefoni. Regionaalse halduskeskuse käivitamisega saab kindlasti telefonide hinda veelgi allapoole, sest 8 eraldi asutuse käive on ikkagi 8 eraldi asutuse käive hoolimata kuuluvusest samasse süsteemi, kui 1 suure keskuse käive, mis katab praktiliselt eelnud 8 asutuse käibe.

Antud hetkel toimivas süsteemis on esinenud juhtumeid, kus Kaitsejõudude transmissioonivõrgus olevatele telefonikeskjaamadele on jätud planeerimata eelarvesse raha sisevõrgust (tasuta) väljapoole helistamiseks. Selliste vigade kõrvaldamiseks on tulnud siia maani optimeerida teiste väeosade vastavat eelarve artikli rida. Halduskeskuste rakendumise korral oleks antud eelarve rea täitmata „unustamise” tõenäosus kordades väiksem.

Antud etapi mõõdetavateks tulemusteks on alluvusvahetõrgete selge ja konkreetne määratlus, muudetud on Kaitsejõudude siseselt toimivat finantsarvestust nii, et regionaalne halduskeskus saab osutada IKT teenust väeosadele ilma väeosadele arveid esitamata.

4.4.2. Standardsete raamistike väljatöötamine

Ühe suurima puudusena väeosade läbilõikes võib tuua standardiseeritud lahenduste puudumist – see puudutab nii riistvaralisi, tarkvaralisi kui ka organisatoorseid lahendusi.

Teenusserverite platvorm

Sõltuvalt asutusest võivad ühe ja sama teenuse osutamiseks olla kasutusel täiesti erinevad lahendused. Nii on osades väeosades kasutusel Microsofti (edaspidi MS) Exchange serveri teenused ja praktiliselt kogu asjaajamine (nii asutusesisene kui ka väline) toimub selle kaudu. Teistes väeosades, kus pole soetatud MS Exchange serveri tarkvara eelkõige kõrge hinna tõttu ning on kasutusel Linux peab MS Exchange funktsionaalsuse ligilähedaseks tagamiseks kasutama mitmeid erinevaid tarkvaraprogramme.

Alustada tuleks standartse serveriteenusplatvormi ja teenuste määratlemisega – kas MS'i põhine platvorm või Linuxi x distributsioon. Vastavalt sellele saab edasi määratleda, milliseid rakendusi, kuidas ja millise lõpphinna eest suudetakse kasutajatele pakkuda.

Antud hetkel võib välja tuua kaks eraldiseisvat lähenemist. Sõltuvalt väeosast on kasutusel kas MS Windows serverid koos Active Directoryga või hoopiski Linuxi erinevat distributsioonid eelkõige Debian 3.x versiooniga. Mõlemad lahendused iseenesest on head ja antud hetkel täidavad ka oma peamise eesmärgi – toimub kasutajate autoriseerimine ja isikliku ning jagatud võrguketta pinna andmine teenusserverites, siseveebi lehtede hoiustamine. Kasutaja jaoks oleks see justkui kõik, mida ta tahta ja soovida oskaks.

Kasutaja liikumisel MS Exchange süsteemiga väeosast Linuxi baasil toimivasse väeosas saab kohe peamiseks probleemiks kasutajale informatsiooni kättesaadavus infosüsteemist. MS Exchange serveri kasutamisel seadistatakse kasutaja arvutisse MS Office Outlook (edaspidi MSOO) koos kogu oma funktsionaalsusega. MSOO võimaldab kasutajatel kasutada alljärgnevat teenuseid:

- E-kirja klient (e-mail) -. Saab kasutada ka ilma MS Exchange serverita, kuid sellisel juhul toimib ainult e-kirjade lugemine, ei saa kasutada
- Kalender (Calendar)– personaalne ja jagatud kalender. Ajaplaneerimine;
- aadressiraamat (Contacts) – e-mail, telefoninumbrid, postiaadress, isiklikud andmed – täielik pilt inimesest ja tema hobidest;

ASUTUSESISESEKS KASUTAMISEKS

- Ülesanded (Tasks) – saab teha märkmeid käsilolevate ja tulevaste ülesannete kohta. Algus, lõpp, osalejad, tähtsus, progress, jne;
- Märkmed (Notes) – asendab märkmepaberit laual. Pole kunagi kadunud, kui pole ise ära kustutanud – seal, kus on su arvuti on ka su märkmed.
- Journal – ajahaldusena kasutamiseks;
- Uudiste voog (RSS Feed) – veebist veebilehtedele tehtud uue materjali pealkirjade arvtisse RSS lugejasse salvestamine. Peamine RSS`i kasutamise koht on ajalehed ja uudistekanalid.
- Postiloend (Newsgroup) – postiloendite kasutamine nii lugemise kui ka kirjutamise jaoks. Loendi uuendamine toimub kas automaatselt (ajaline intervall) või kasutajapoolse sekkumisega (allalaadimine).

Kasutaja peab harjumuspärase ühe programmi asemel hakkama kasutama hoopis mitut erinevat programmi ja sageli pole antud programmid ka omavahel liidestatud ning informatsiooni ülekandmine tuleb teha manuaalselt.

Peale eelpool toodud võimaluste on enamus maailma suuremaid mobiiltelefonide tootjaid loonud oma telefonide haldustarkvara just peamiselt MSOO`i baasil, kuigi toetavad ka MS Outlook Express ja Lotus toodangut. Nokia PC Suite võimaldab sünkroniseerida telefoni ja arvuti vahel olenevalt telefoni tüübist nii inimeste kontakt andmeid (Contacts), e-kirju (e-mail), kalendrit (Calendar) kui ka ülesandeid (Tasks). Selline lahendus on vägagi kasulik mobiilsele inimesele ja juhile. Elektrooniline märkmik kas siis arvutis, GSM telefonis või pihuarvutis hakkab järgneva viie kuni kümne aasta pärast ka Eestis muutuma sama tavapäraseks, kui see on juba Ameerika Ühendriikides.

Linuxis sellise võimekuse tagamine on suhteliselt raske. Antud hetkel on enam levinud e-kirja klientideks MS Outlook Express või Mozilla Thunderbird. Mõlemad rakendused töötavad tavakasutajal MS Windowsi keskkonnas ja on arvutisse installeeritud lokaalse seadme profiiliga, kasutades e-kirjade lugemiseks kas POP3 või IMAP ühendust.

Mozilla Thunderbird`ile on võimalik installeerida juurde eraldi pakulina Mozilla Calendar/Sunbird/Lightning, mis oma funktsionaaluselt on suhteliselt sarnane MSOO kalendri, kuid ka lisapaketiga Thunderbird ei taga päris kõiki MSOO võimalusi.

ASUTUSESISESEKS KASUTAMISEKS

Täiendatud Mozilla Thunderbird koos Mozilla Lightning`uga võimaldab:

- koostada sarnaselt MSOO-le personaalset kalendrit;
- koostada sarnaselt MSOO-le jagatud kalendrit, kui teenusserverisse on loodud kalendri fail;
- kasutada e-kirja klienti;
- ülesanded (todo) – märkmete tegemine käsilolevate ja tulevaste ülesannete kohta.
- (agenda) – vastavalt seadistustele kuvatakse tänased ja homsed Lightningusse tehtud kanded.
- Uudiste voog (RSS Feed) – veebist veebilehtedele tehtud uue materjali pealkirjade arvtilisse RSS lugejasse salvestamine. Peamine RSS`i kasutamise koht on ajalehed ja uudistekanalid.
- Postiloend (Newsgroup) - postiloendite kasutamine nii lugemise kui ka kirjutamise jaoks. Loendi uuendamine toimub kas automaatselt (ajaline intervall) või kasutajapoolse sekkumisega (download).

Vabavaraline Mozilla Thunderbird koos Lightningu lisapaketiiga on võimeline asendama MSOO`i oma peamiste funktsionaalsuste poolest – Journali kasutamine MSOO kasutajate juures on minimaalne, kui isegi mitte oelda olematu. Lõpptarbijale ei ole erilist vahet, kas kasutatakse tasuta vabavaralist lahendust või kallist tarkvara - peamine on see, et töö saaks tehtud ja oleks võimalikult lihtne antud tarkvara kasutada.

Arvutivõrkude liigid vastavalt neis sisalduva informatsiooni järgselt.

Antud hetkel on väeosades kasutusel hulk erinevaid arvutivõrke, mis oma funktsionaalselt on sarnased, kuid nimetused, mis on võrkudele omistatud võivad erineda suuresti. Standardiseerida tuleks arvutivõrkude nn töödeldava informatsiooni liigi järgsed nimed ning tehniline ülesehitus.

Administratiiv arvutivõrk (edaspidi „must” arvutivõrk). Väeosas peamine arvutivõrk, kus toodetakse enamus andmeid – peamiselt MS Word`is, MS Powerpoint`is ning rahandusüsteem. „Musta” arvutivõrku saavad kasutada kõik väeosa teenistujad, kellele on väljastatud võrgu kasutaja tunnused. Võrk on ehitatud domaini serveri peale ja vajadusel segmenteeritud

ASUTUSESISESEKS KASUTAMISEKS

VLAN`ide abil erinevatesse kasutajagruppidesse. „Mustas” arvutivõrgus on võimalik kasutada interneti, kuid enamus porte on kinni pandud. Avatud portidena on kasutusel eelkõige IMAP, POP3, SSL, HTTP, HTTPS, SMTP, ning VPN`i port (hetkel on kasutusel väeosades erinevad pordid ja erinevad VPN tarkvarad).

Ametkondlik arvutivõrk (edaspidi „punane”arvutivõrk)– teisi sõnutsi riigisaladuse Automatiseeritud InfoTöötlus Süsteem (edaspidi AITS). „Punases” arvutivõrgus töödeldakse ja toodetakse elektrooniliselt vastavalt „Riigi saladuseeadusele” klassifitseeruv teave. „Punane” arvutivõrk kasutab sarnaseid tehnoloogilisi lahendusi nagu „must” arvutivõrk, kuid kõik seadmed ja võrguosad (võrgulülitid, serverid, kaabeldus) peavad vastama kaitseministri määrusele 29.01.2007 nr. 14 „Elektroonilise teabeturbe ning eriside korraldamiseks ja kontrollimiseks kasutatavad meetodid ja vahendid”. Samas igas väeosas on kasutusel omamoodi lahendus – terminal serveril ja terminalidel põhinev arvutivõrk, üksik PC ilma arvutivõrgu ühenduseta ja ilma optilise meedia seadmeteta. Arvutivõrk on ülesehitatud kas Cat5E kaablitele või fiiberoptilistele kaablitele – võrgulüliti ja seadmevaheline kaabel peab olema ilma jätkudeta otsekaabel lõpptarbija seadmesse.

Avatud interneti (edaspidi „roheline” arvutivõrk). Kasutamise eesmärk on järgnev:

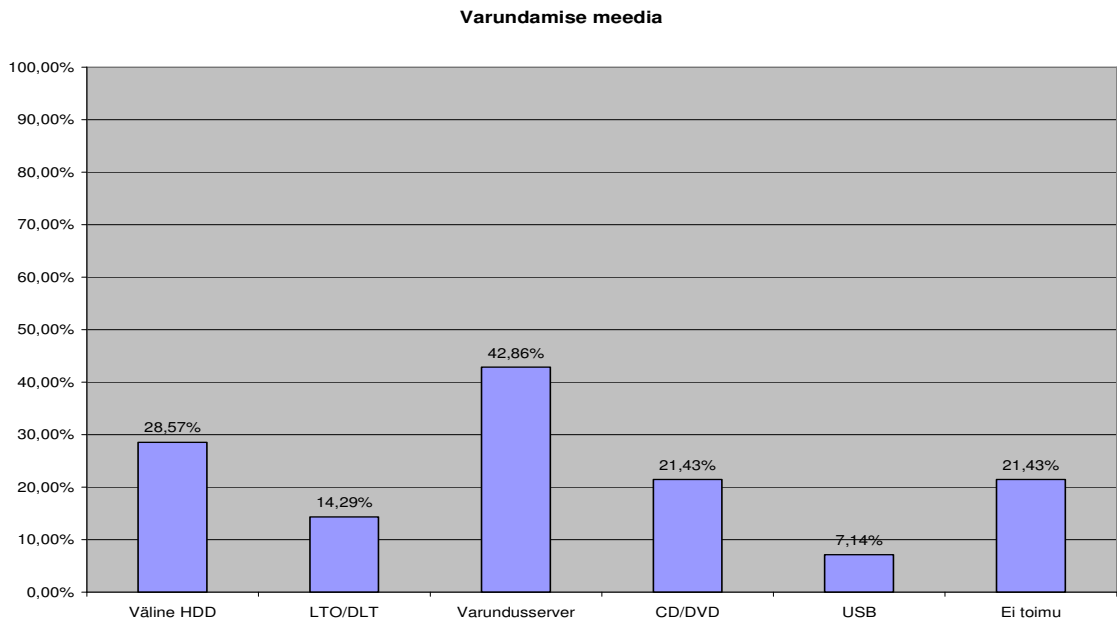
- Ajateenijate internetipunktid;
- Külalistele interneti võimaldamine;
- Ühiselamutes interneti võimaldamine;

„Roheline” arvutivõrk on internetiteenuse pakkujalt saadav ühendus, mida on natukene ümber seadistatud eelkõige arvutivõrgu portide sulgemise näol. Kasutajale on avatud reeglina IMAP, POP3, SSL, HTTP, HTTPS, SMTP ja neti pankade ID kaardi pordid. „Rohelist” arvutivõrku edastatakse nii kaabli-(Cat5E), kui ka traadita (IEE 802.11 a/b/g standartses) arvutivõrgus. „Roheline” arvutivõrk asub välismaailma eest tule müüri taga, kasutab eraldi teenusserverit, kuid on füüsiliselt ühendatud „musta” võrgulülitisse ja seal omakorda loogiliselt eraldatud (VLAN`iga) „mustast” arvutivõrgust.

ASUTUSESISESEKS KASUTAMISEKS

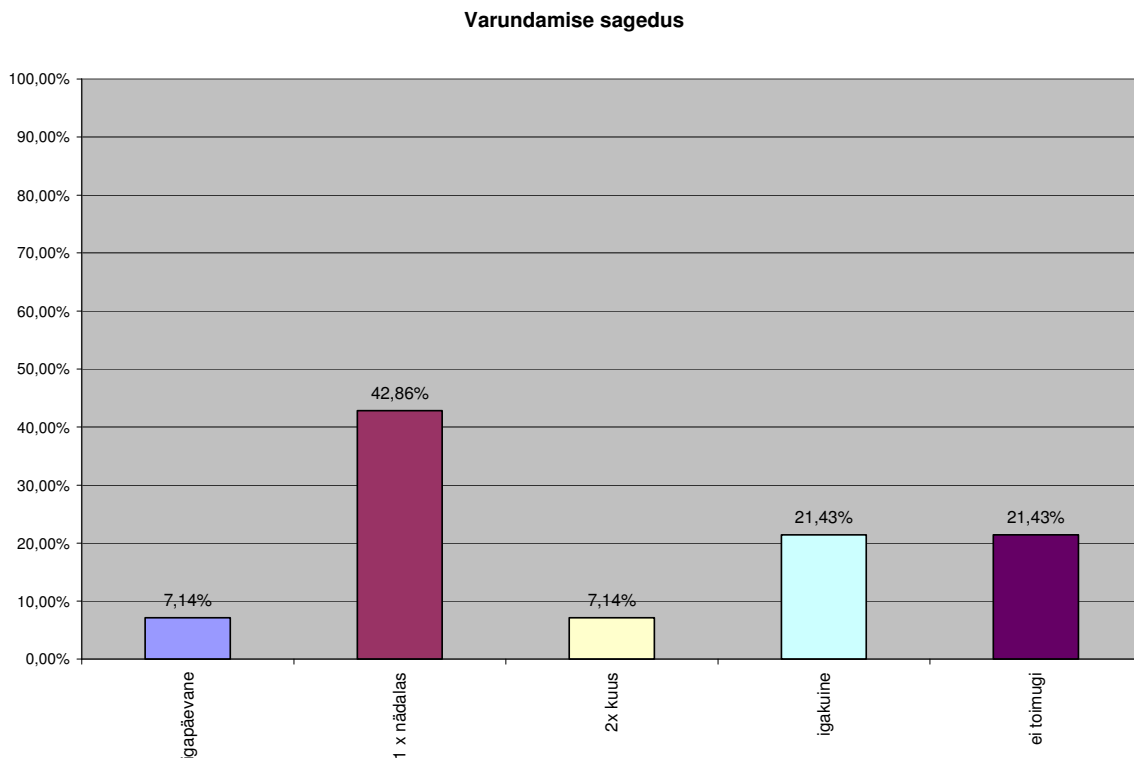
Andmete varundamine

Andmete varundamisel tuleb üle minna ühtsele standartile ja seadmetele. Antud hetkel varundab iga väeosa omi teenusserveried vastavalt olemasolevale võimekusele – kes kasutab varunduseks eraldi serverit, kes snapshot¹⁶ tehnoloogiat ja varundab saadud info välisele kõvaketta seadmele või teistele meediatele (graafik 1).



Graafik 1

ASUTUSESISESEKS KASUTAMISEKS



Graafik 2

Võib väita graafiku 2 alusel, et saadud tulemuste järgi pole ükski väeosa missiooni kriitiline ja andmete kaotamiseks varundatud koopiade puudumise tõttu ei ole eriti suur kaotus. Vastavalt serveris olevale informatsioonile tüübile tuleks varundamine jagada vastavalt andme mahtudele erinevatesse kategooriatesse ning igale kategooriale määrata ka siis vastav salvestus tehnoloogia. Lisaks selgus küsitluse tulemusena, et üks väeosa võib varudada erinevaid teenusservereid erinevatele meediatele – kas siis varundusserver ja DVD ketas või magnetlindid ja väline kõvaketas.

„Must” arvutivõrk, Domaini server, võiks olla varundatud koos kõigi kasutaja- profiilidega vähemalt iganädalaselt, kui isegi mitte igapäevaselt. – sõltub asutuses toodetava informatsiooni kaotamiseks kriitilisusest. Varundamiseks peaks kasutama eraldi varundusservereid, mis iganädalaselt/päevaselt teatud kellaajal teostavad snapshoti teenusserverist. Varundusserver peab asuma eraldi hoones, varundusserveri ruum peab vastama samadele nõuetele nagu serveriruum – loetletud eelnevalt töö punktis [2.4.1](#).

ASUTUSESISESEKS KASUTAMISEKS

Raamatupidamine koos laomajandusega on kõige missiooni kriitilisemate andmetega kogu Kaitsejõududes. Enamasti on raamatupidamisel kasutusel eraldi server, kust käitatakse teenusprogramme ja kuhu salvestatakse kõik kanded. Raamatupidamine tuleb varundada igapäevaselt, varundamine peaks toimuma automaatselt kindlal ajahetkel ja varundatud andmeid saab hoida samas varundusserveris, kus ka domain serveri varundust, kuid eraldi kettamassiivil.

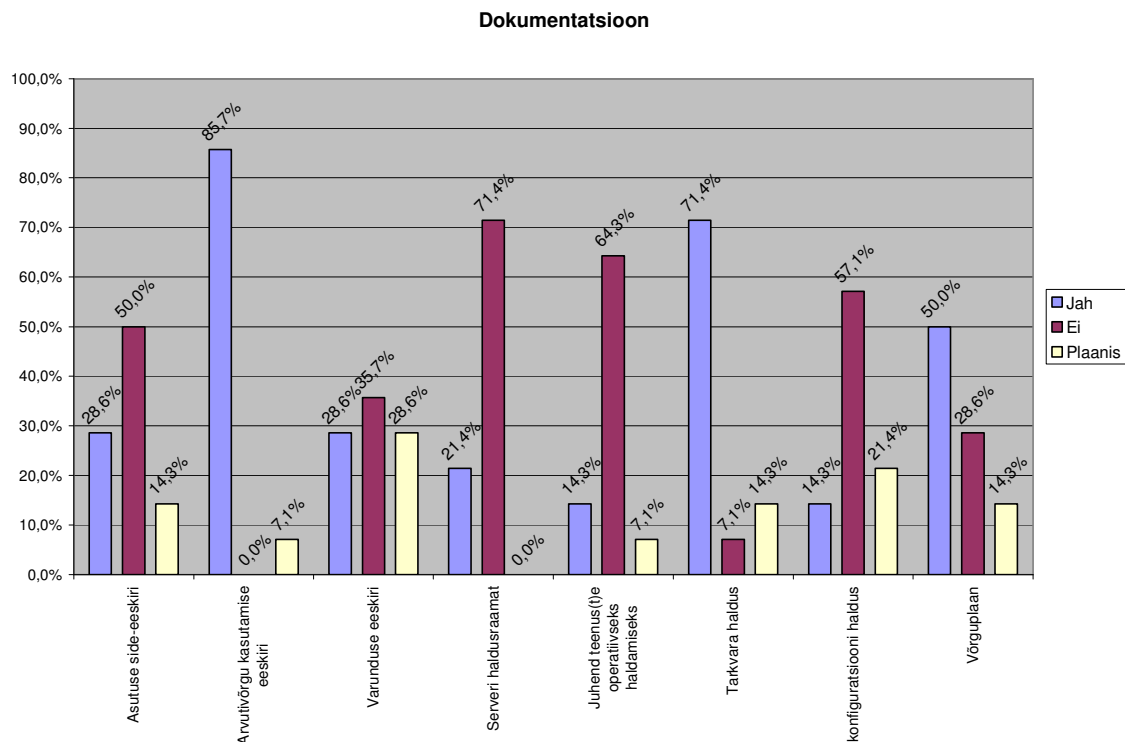
„Punases” arvutivõrgus on andmete varundamine tähtis, kuid andmemahtude suurusest lähtudes ei ole optimaalne kasutada selleks eraldi varundusserverit, vaid hoopis kas LTO või DLT tehnoloogial põhinevatle magnetlintidele snapshoti salvestamist. Varundamiseks ei saa kasutada „musta” arvutivõrgu varundusserverit – „must” ja „punane” arvutivõrk ei tohi omavahel füüsiliselt kokku puutuda.

„Rohelise” arvutivõrgu andmete varundamine ei ole vajalik, kui ei kasutata veebiserverit oma väeosa välise võrgulehe ülalhoidmiseks. Väeosa veebiserveri varundamiseks võiks kasutada kas andmete DVD-le kirjutamist või välisele kõvakettale (HDD) andmete salvestamist.

Dokumentatsioon

Lähtudes väeosadele läbiviidud küsitluse tulemustest ja tutvudes väeosades kasutusel- oleva IKT- alase dokumentatsiooniga saab väita, et väeosades on kasutusel ainult osaline loetelu küsimustikus olevatest dokumentidest, mida näitab ka allolev graafik 3

ASUTUSESISESEKS KASUTAMISEKS



Graafik 3

Küsimustik näitas, et enamus väeosasi on aluseks võtnud „Kaitsejõudude IT eeskirja”, mis on väljaantud aastal 2000, seda pole uuendatud alates selle väljatöötamise ajast ja nii ongi tekkinud olukord, kus tuleb kasutada juba aegunud tehnoloogiaid. kui soovitakse järgida eeskirja.

Dokumentatsioon tuleb ühtlustada ja kaasajastada. Dokumentatsiooni koostamiseks tuleb moodustada töögrupp, kuhu on kaasatud nii J6, SIVAKI kui ka väeosade IKT teenistused. Esmaselt tuleb luua ja sisse seada alljärgnevad dokumendid:

- Tsentraalne IKT eeskiri, mis peab endas sisaldama alljärgnevat:
 - Administratiivse arvutivõrgu kasutamise eeskiri;
 - Ametkondliku arvutivõrgu kasutamise eeskiri;
 - Interneti kasutamise eeskiri;
 - Wifi võrkude kasutamise eeskiri;
 - Varunduse eeskiri;
 - GSM ja PBX teenuste kasutamise eeskiri

ASUTUSESISESEKS KASUTAMISEKS

- Serverite, võrgulülite ja arvutite konfiguratsiooni ja halduse raamatud:
 - Konfiguratsiooni haldus (riistvara);
 - Muudatuste haldus (eelkõige tarkvara);Ettepanek oleks - üle võtta ITIL¹⁷ist Service Support`i pakett.
- Tarkvara haldus – kuidas ja millistel alustel hakkab toimima tarkvara haldus kaitsejõududes:
 - Litsentside haldus;
 - Tarkvara hankimine;
 - Tarkvara mahakandmine;Samuti oleks ettepanek ITIL`ist üle võtta Software Asset Managment pakett.
- IKT vahendite kasutamise eeskiri:
 - Arvutite kasutuse eeskiri;
 - Rüperaalide kasutamise eeskiri;
 - Telefonide kasutamise eeskiri;
- IKT vahendite soetamise, arvestamise ja mahakandmise kord;
 - Kuidas toimub IKT vahendite soetamine;
 - Kuidas peetakse arvestust IKT vahendite üle;
 - Kuidas amortiseerunud IKT vahendid maha kantakse;

Standartsete raamistike väljatöötamise etapp on mõõdetav ja etapi lõppemiseks peavad olema väljatöötatud ja kasutuselevõtmiseks valmis eelpool loetletud punktid

4.4.3. Tsentraliseeritult vahendite soetamine uuele süsteemile

Standartsete raamistike väljatöötamise etapi algfaasis tuleb juba hakata planeerima finantsvahendeid punkti [4.4.2](#) täitmiseks, vältimaks olukorda, kus uued juhendid ja määrused töötatakse välja ning määratakse aeg, mis ajast peab neid rakendama, kuid sageli ei kaasne nende rakendamiseks finantsressursse.

Läbi tuleb viia põhjalik riist- ja tarkvara audit eesmärgiga saada täielik ülevaade väeosade IKT vahendite seisust – millised vahendid on olemas ning kuidas saab neid rakendada uues süsteemis, milliseid vahendid ja millises järjekorras on vaja juurde soetada.

ASUTUSESISESEKS KASUTAMISEKS

Riistvara

Teenusserverite tarkvara platvormi määratlemisel saab edasiliikuda teenusserverite arvuga – MS Exchange puhul on vaja rohkem arvutusjõudlust, kui Linuxi puhul. Seega peab iga väeosa jaoks vajaminevate serverite arvu eraldi arvestama – kõik sõltub väeosa arvutipargi ja kasutajate suurusest. Kõik teenusserverid peavad omama RSA kaardi abil kaughaldus funktsiooni, et vältida olukorda, kus taaskäivituse jaoks peaks serveri administraator sõitma mitukümmend kilomeetrit. Lisaks peab tagavaravariandina olema võimalik kasutada GSM Data ühendust seadmete kaughalduseks.

„Punase” arvutivõrgu serveri ja võrgulülite kaughalduseks tuleb kasutusele võtta ametkondadevaheline turvalise andmesidevõrgu (edaspidi ATA) krüpteerimise seadmed. Krüpteerimise seadmed tuleb soetada hiljemalt esimese regionaalse keskuse käivitamiseks.

Varundamise protseduuride ja -seadmete standardiseerimise käigus määratletakse, kuidas ja milliste seadmetega mis tüüpi andmeid varundatakse. Hetkeolukorrast lähtudes on varundusseadmete seis suhteliselt hea, kuigi erinev. Auditi käigus saadud informatsiooni kohaselt tuleb varundusseadmed ümber jaotada nii, et saaks tagatud punktis 4.4.2 kehtestatud nõuded varundamisele

Võrgulülid peaksid olema Kaitseväes suhteliselt standartsed (Enterasys või Cisco firmade toodangust) ning nende väljavahetamiseks tehtavad kulutused on eeldatavasti kõige väiksemad Kaitseväe siseselt. Kaitseliidus seevastu tuleb praktiliselt kõik võrgulülid ümber vahetada - vägagi palju on kasutusel Layer1 võimekusega lüliteid ja seda eelkõige kaitseliidu erinevates malevates.

Tarkvara.

Tarkvara auditi tulemusena saadakse terviklik pilt kaitsejõududes kasutuselolevast tarkvarast. Paljud väeosad on ise soetanud endale erinevat tarkvara ning antud hetkel J6 puudub ülevaade just isesoetatud tarkvarade üle. Auditiga koos peaks toimuma ka väeosade tarkvara vajaduste väljaselgitamine, mille tulemusena peab teostuma kas suuremahulise tarkvara hanke või

tarkvara litsentside ümberjaotamise väeosade vahel. Auditi tulemina saadud informatsioon jääb kuni halduskeskuste käivitumiseni J6 hallata.

Esmase tarkvara hankena tuleb teostada kas MS Exchange soetamine või ühe ühtse raamatupidamise tarkvara soetamine (soovituslikult mingi ERP süsteem) - sõltuvalt teenusserverite platvormi valikust.

Koolitused

Kaitsejõududes on väga erineva tasemega IT spetsialiste, kellede baasil hakkavad seisma suured vastutused uue süsteemi käivitamisel. Vastavalt teenusserverite platvormi valikule ning lähtudes personalist, keda on planeeritud regionaalsetesse keskustesse tuleb viia läbi vägagi erinevaid koolitusi. Võttes aluseks teabe, et IT spetsialiste on Eestis puudu

4.5. Uue süsteemi positiivsed ja negatiivsed küljed.

Igal süsteemil on omad head ja halvad küljed. Alljärgnevalt katsun välja tuua peamised positiivsed ja negatiivsed küljed.

Positiivsed küljed uue süsteemi puhul

Peamiste positiivsete külgedena näen ma alljärgnevaid aspekte:

- Standartiseeritud IKT süsteem kaitsejõudude siseselt, loomulikult esineb üksikuid kõrvalekaldeid vastavalt eriala spetsiifikale – näiteks Õhuvägi ja nende poolt kasutatavad vahendid õhuseire pildi saamiseks ja töötlemiseks;
- IKT alaste kulude kokkuhoid pikemas perspektiivis – täpsete summade kohta tuleb teostada eraldi analüüs, mis hõlmaks endas kulude võrdluse tsentraliseeritud süsteemi ja hetke olukorra vahel:
 - Riistvaralised kulud;
 - Tarkvaralised kulud;
 - IKT teenuste kulud;
 - Personali kulud;
 - Majandus kulud;
- Väheneb reageerimise aeg kaitsejõudude transmissioonivõrgu rikke korral – regioonis esineva rikke korral suudab regiooni võrguseadmete administraator kas esinenud rikke

ASUTUSESISESEKS KASUTAMISEKS

kõrvaldada või tellida monitooringu keskuses tehnikutegrupilt vastavad vahendid rikke kõrvaldamiseks ;

- Suureneb spetsialistide hulk, kes oskab hallata ja vajadusel ümber konfigurereida kaitsejõudude transmissiooni võrku ja võrguseadmeid – hetkel on see võimekus vägagi minimaalne, kui isegi mitte olematu;
- Tsentraliseeritud IKT hanked aitavad kasutada eraldatud finantsressursse odavamalt – käibemahtudega saavutatavad soodushinnad;

IKT alane arendustegevus jääks ainult ühele asutuse - SIVAK`ile, kelle eelarvesse tuleb anda arendustegevuseks vajaminev finants- ja materjalne ressurss otse läbi J6;

Negatiivsed küljed uue süsteemi puhul

Peamiste negatiivsete külgedena näen ma alljärgnevat kitsas kohti;

- kaitsejõudude- ja väeosade juhtkonna soovimatus uue struktuuri rakendamiseks
 - väeosad ei saa aru tsentraalse juhtimise ja haldusega saavutatavat ressursi kokkuhoidu;
 - kartus, et antud väeosa „unustatakse ära” – IKT alane arendustöö ja vahendid lähevad teiste väeosade „hüvanguks”;
 - väheneb vabade töökohtade arv
- operatiivse reageerimise kadu väeosa siseselt – väeosade IKT teenistused ei suuda enam rahuldada tellimusi „juba eilseks oli vaja”, vaid peavad tellima vajaminevad vahendid regionaalse halduskeskusest;
- Väeosade IKT personali taseme langus – väeosadesse jääv IKT personal ei tegele enam arendustegevusega, vaid tarbivad juba valmis toodangut. Võimalikud probleemid
 - Igapäevase töö rutiinsus ;
 - Arendustegevuses osaletakse ainult lähteülesannete koostajatena;
- Hangete korraldamine läbi J6 pikendab vajaminevate IKT toodete soetamise ning kättetoimetamise aegu;

5. Kokkuvõte

Oma igapäevases elus me puutume pidevalt kokku erinevate IKT teenustega nii tööl, kui ka kodus. Kasutaja eeldab, et suurfirmas/asutuses toimuksid kõik protsessid kaasa arvatud ka IKT alased tsentraalselt juhitud ja koordineeritud. Oma töö alguses püstitasin eesmärgi tõestamaks, et tsentraliseeritud IKT juhtimine ning haldus on kaitsejõududele lõppkokkuvõttes kasulik, kui antud hetkel toimiv „süsteemitus” süsteemis.

Lõputöö kirjutamise käigus sain juurde palju teadmisi kaitsejõudude IKT teenistuste ja väeosades toimuvate protsesside kohta – millisel tasemel on mingi väeosa IKT haldus, millisel tasemel on seal personal. Uurisin väeosade IKT juhtidelt nende rahulolu antud hetke süsteemiga ja IKT alase koordineerimisega. Saadud tulemused olid küll mõneti jahmatavad – nimelt ei olnud eriti rahul hetke olukorraga, kuid ka tsentraalse juhtimise ning halduse loomisest ei tahtnud kuulda. Antud valdkonnas peab tegema suuresti selgitus tööd kaitseväe siseselt, et tõestada tsentraliseerimise vajadust ning sellega saadavat kasu. Samuti tuleb hakata tegema selgitus tööd J6^e, kaitsejõudude peastaabi ja kaitseministeeriumi siseselt et saada finantsressurss regionaalsete keskuste moodustamiseks.

Oma töös puudutasin põgusalt kaitsejõudude teket koos IKT teenistuste arenguga kuni aastani 2001, BALTNETⁱ ja transmissiooni võrgu teket ning ülesehitust.

Ise ma loodan, et tehtud töö kannab ka vilja kas siis töös välja toodud regionaalne juhtimine ja haldussüsteemi tekkimise näol või hoopiski kasutajate teadlikkuse tõstmisena kaitsejõudude IKT tegelikust hetke olukorrast.

Minu arvamus on ka peale küsimustikkudest saadud negatiivset tagasisidet, et tsentraalne juhtimine ning haldus tuleb taastada ning on lõppkokkuvõttes kasulik kaitsejõududele

Summary

In my work „Possibilities of centralized leadership and management of Information and Communication technology in Estonian Defence Forces” I described the situation of Information and Communication technology (ICT) in Estonian Defence Forces (EDF).

The main point at my work was that EDF urgently needs re-establishment of centralized leadership and management of ICT, because at today every base is developing at its own direction and mostly does it cost a lot of money and other resources – we don't have a strategic plan in ICT. Also there's a lot of equipment that we don't use as we should – we don't manage our layer2 or layer3 switches and routers. The ICT personal can't manage them – they don't have that qualification. In centralized leadership and management there will regional ICT centres manages their region switches and routers.

You can compare EDF ICT with a big company's ITC – the amount of computers is the same, but their purchasing procedures are different. Currently in EDF all bases are buying from different shops and don't get a discount from product. In centralised mode all activities (leading and purchasing) will be done by headquarters – it will save money and it will assure that all bases are using quite the same technology.

My suggestions were:

- Creating of regional ICT centres;
- Creating a strategic plan for ICT;
- Creating frameworks for ICT services;

Also I introduced EDF and his ICT systems till 2001, what is BALNET and how are different bases connected through EDF transmission net today.

My opinion is that centralized leadership and management of ICT will be the best solution for EDF.

Lisa 1

Küsimustik väeosa/asutuse sideülemale

Käesoleva küsimustiku eesmärgiks on koostada ülevaade kaitsejõududes kasutusel- olevatest IKT vahenditest ja nende haldamisest. Antud küsimustiku tulemusi rakendatakse minu magistritöös – Tsentraalse IKT juhtimise ja haldamise võimalikkusest Kaitsejõududes (esialgne pealkiri)..

Dokumentatsioon:

Kas Teie asutuses on kasutusel järgnevad dokumendid /eeskirjad? Tehke märke sobivasse lahtrisse. Kui Teie asutuses on kasutusel veel erine

	Jah	Ei	Planeeritud kasutusele võtta
Asutuse side-eeskiri			
Arvutivõrgu kasutamise eeskiri			
Varunduse eeskiri			
Serveri haldusraamat			
Juhend teenus(t)e operatiivseks haldamiseks			
Tarkvaralitsentside haldus			
Konfiguratsiooni haldus			
Võrguplaan			

Varundamine:

Kuidas toimub Teie asutuses andmete varundamine?

Millistes hoiustamis tingimustes hoitakse Teie asutuses varundatud andmeid?

Millisel meedial hoitakse Teie asutuses varundatud andmeid?

Milline on varundamise intervall?

ASUTUSESISESEKS KASUTAMISEKS

Tarkvara

Nimetage kasutuselolevad operatsioonisüsteemid ja nende kasutamise koht?

Litsenseeritud tarkvara osakaal?

Vabavara osakaal?

Nimetage kogu ülejäänud kasutuselolev tarkvara?

Kuidas soetate vajadusel uue tarkvara?

Kas kasutate tarkvaralist tule müüri? Kui jah, siis mis toodet?

Kuidas toimub vajamineva tarkvara soetamine? Iseostmise teel või läbi J6`e tsentraalselt?

Riistvara

Teie arvutipargi suurus?

Teie serveripargi suurus?

Kas kasutate terminale? Kui jah, siis mis otstarbel?

Nimetage Teie serveritel kasutuselolevad teenused ja tarkvara, millel see põhineb?

Kas kasutate riistvaralist tule müüri? Kui jah, siis kas isehitatut, tsentraalselt hangitud või poest ostetut?

Kes haldab Teie telefoni keskjaama?

Kuidas toimub vajamineva riistvara soetamine? Iseostmise teel või läbi J6`e tsentraalselt?

Arvutivõrgud

Kas Teie asutuse arvutivõrk on segmenteeritud?

Kes haldab Teie asutuse võrgulüliteid?

Kes haldab Teie asutuses kaitsejõudude transmissiooniseadmeid?

Kas kasutate asutuses VPN ühendusi?

Milliste tootjate võrgulüliteid kasutate?

Kuidas ja kelle poolt toimub võrgulaienduste planeerimine?

Serveriruumid

Tehke märge iga allpool loetletud punkti juurde, mis on kasutusel Teie serveriruumides:

Vajadusel lisage punkte juurde

- Elektrooniliselt piiratud ligipääs;

ASUTUSESISESEKS KASUTAMISEKS

- Videovalve koos salvestiga;
- Automaatne tulekustutussüsteem;
- Konditsioneer;
- Hügromeeter;
- Temperatuuriandur;
- Sundventilatsioon;
- Mittepõlevast materjalist põrand.

Terminid

Mida tähendavad alljärgnevad täheühendid:

ITIL –

OGC -

VLAN -

Subnet -

VoIP -

VPN -

WiMax -

Personal

Kui suur on Teie asutuse IKT teenistus?

Kas IT spetsialistidel on konkurentsivõimeline töötasu? Sisaldab endas nii põhipalka, kui ka lisahüvesid?

Kas IT spetsialistidele võimaldatakse piisavalt täiendkoolitusi?

Üldine

Kuidas olete rahul Kaitsejõudude IKT-alase hetkeolukorraga?

Kas tsentraliseeritud IKT juhtimise taastamine oleks Teie arvates otstarbekas?

Kas Teie asutuse IKT eelarve on piisav, et vastata väeosa juhtkonna soovidele?

Teiepoolne visioon, kuidas peaks olema IKT teenistus koordineeritud Kaitsejõududes.

Lisa 2

Küsimustik edastati Kaitsejõudude väeosade IKT teenistuste ülematele ja Kaitsejõudude Üksik-Sidepataljoni statsionaarse sidekeskuse juhtkonnale ning SIVAK`i arendusjaoskonnale täitmiseks. Sellise valiku tingisid alljärgnevad asjaolud:

- Väeosa IKT teenistuse ülem kujundab suuresti antud väeosa IKT teenistust;
- Reeglina on ta töötanud oma ametis kauem kui IT spetsialist;
- Mõistab ja saab paremini aru Kaitsejõudude üldisest ülesehitusest ja arengukavadest – IT spetsialist puutub kaitsejõududega esmakordselt kokku alles sinna tööle asudes.
- Üksik-Sidepataljon`i statsionaarne sidekeskus

Valimiks oli 9 maaväe väeosa, 2 mereväe väeosa, 2 õhuväe väeosa, 3 keskalluvusega asutust, Kaitseliidu Peastaap ja Kaitsejõudude Peastaap - kokku 18 väeosa. Vastused sain 14 väeosalt, mis moodustab 77,8% kogu valimist.

Küsimustiku dokumentatsiooni osa alusel koostatud graafik on eelnevalt välja toodud punktis [4.4.2](#). Dokumentatsiooni osa tulemused näitavad, et enamus loeteldud dokumentatsioonist on kas kasutusele võetud või planeeritud kasutusele võtta, mis iseenesest annab suuresti positiivse hinnangu IKT teenistustele.

Küsimustiku varundamise osas saadud vastused aga kahjuks viitvad suuresti sellele, et andmete varundamine toimub sõltuvalt väeosa teadlikkusest – vastanutest tervelt 3 väeosa ei teosta andmete varundamist üleüldse ja 3 väeosa varundab andmeid igakuiselt. Ülejäänud väeosad varundavad kas igapäevaselt, iganädalaselt või 2 korda kuus. Varundamis meedia oli optilistest seadmetest (CD/DVD, LTO/DLT) eraldi varundusserveriteni (lihtsalt server või Network Attached Storage) välja.

Küsimustiku tarkvara osas selgub et enamus kasutatavat tarkvara on MS toodangust pärinevad operatsiooni süsteemid nii lauaarvutitele, kui ka serveritele. Sama kehtib ka kontori tarkvara kohta. Tarkvara hangitakse peamiselt ise soetamise teel välja arvatud MS toodang, mis saadakse reeglina läbi J6`e.

ASUTUSESISESEKS KASUTAMISEKS

Küsimustiku riistvara osas oli eesmärgiks välja selgitada kasutusel oleva IKT tehnika hulk ja erinevad liigid. Lisaks sellele uurisin kuidas toimub riistvara soetamine ning telefonikeskjaama haldus. Kogu kaitsejõudude kasutuses olev arvutipark on oma suuruse poolest võrreldav pangandusega ning arvutite juurde soetamine toimub peamiselt kas tsentraalse riigihankena läbi J6^e või ise soetamise teel. Telefoni keskjaama esmast haldust (abonementide lisamine, õiguste muutmine) teostab väeosa, kuid raskemad operatsioonid (numbriplaaan, trunkide loomine/seadistamine) tehakse monitooringukeskuse tehnikute grupi poolt.

Arvutivõrkude osas oli eesmärk saada informatsiooni kasutusel olevate võrgulülite sortimendi ja nende kasutamise kohta, kaitsejõudude transmissiooni võrguhaldus ning kuidas toimub väeosa arvutivõrgu laienduste planeerimine. Küsimustikust selgus et kõik väeosad kasutavad kas Enterasys'i või Cisco toodangut koos erinevate funktsionaalustega, kuid ainult ainult pooled (50%) väeosadest haldavad ja on seadistanud oma võrgulüliteid ise – ülejäänutel on võrgulülid kasutusel tehase seadistustega. Kaitsejõudude transmissiooni võrgu haldus on täielikult (100%) monitooringu keskuse tehnikute grupi poolt.

Serveriruumide osas on kaitsejõud suhteliselt sarnases seisus – see on peamiselt tingitud sellest, et serveri ruumid on ehitatud või rekonstrueeritud enamuses viimase kolme-nelja aasta jooksul. Küsimustiku tulemusena võib väita et üheksakümnel protsendil (90%) serveriruumidest puudub automaatne gaaskustutussüsteem ning selle asemel on ruumi paigaldatud käsi süsihappegaasi kustutid.

Terminite osas oli eesmärgiks juhtida IKT juhtide tähelepanu terminitele, et viimased endale teeksid selgeks mis vahe on VLAN'il ja WLAN'il.

Küsimustiku personali osa kasutasin peamiselt punktides [3.2](#) ja [4.3](#).

Küsimustiku üldises osas soovisin väeosa IKT teenistuste ülematelt arvamust hetke olukorra kohta, väeosa IKT eelarve kohta ning tsentraalse juhtimise ja halduse taastamise vajalikkuse kohta. Hetke olukorda ei hinnanud keegi heaks, kuid ideelisi lahendusi, kuidas olukorda muuta

ASUTUSESISESEKS KASUTAMISEKS

ka välja ei pakutud. Eelarvega on alati nii, et seda võiks rohkem olla, kuid antudhetkel kasutatava eelarve suurusega oli rahul 64,3 % vastanutest. Tsentraalse juhtimise ning haldamise taastamisega oli aga samas nõus kõigest 14,3 % ning ära ootaval seisukohal 21,4 %. Küsimustiku tulemusena võib väita, et väeosad kas ei saa aru tsentraalse juhtimise ja haldamise vajalikkusest või kardavad, et arendus protsess jätab nende väeosa vahele.

Viited:

1. Kaitsejõud <http://www.mil.ee/index.php?menu=juhtimine&sisu=juhtimine#2> 10.04.07;
2. Kompanii taseme raadiojaam R-108
<http://www.armyradio.com/arsc/customer/pages.php?pageurl=/publish/Articles/WilliamHowardRussian/50-73CompanyBattalionRadios.htm> 10.04.07;
3. Pataljoni raadiokomplekt R-142
<http://www.armyradio.com/arsc/customer/pages.php?pageurl=/publish/Articles/WilliamHowardRussian/73-PresentBaseFixedStationRadios.htm> 10.04.07;
4. Raadiospekter http://en.wikipedia.org/wiki/Radio_spectrum 10.04.07;
5. EDACS <http://www.macom-wireless.com/products/pve/edacs.asp> 10.04.07;
6. SINCGARS http://www.olive-drab.com/od_electronics_singars_m.php 11.04.07;
7. Avaliku teenistuse seadus §20 lg 1 <https://www.riigiteataja.ee/ert/act.jsp?id=742925>
03.03.07
8. Riigisaladuse seadus §6 lg 7 ja lg 8;
<https://www.riigiteataja.ee/ert/act.jsp?id=12751455> 10.03.07
9. Foreign Military Financing <http://www.usemb.ee/odcprograms.php> 11.03.07;
10. Foreign Military Financing
http://www.dsca.osd.mil/home/foreign_military_financing%20program.htm 11.03.07;
11. OSI mudel http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introint.htm
13.03.07;
12. Linear Tape Open <http://www.ultrium.com/newsite/html/about.html> 24.04.07;
13. Digital Linear Tape
14. DSL tehnoloogiad http://en.wikipedia.org/wiki/Digital_subscriber_line 20.04.07;
15. Structured Query Language <http://en.wikipedia.org/wiki/SQL> 20.04.07;
16. Snapshot http://en.wikipedia.org/wiki/Snapshot_%28computer_storage%29 21.04.07;
17. ITIL <http://www.iti.org.uk/> 21.04.07;

Kasutatud kirjandus.

L. Allmann, „Eesti riigikaitse juhtimine”, 2003;

„Eesti sõjalise kaitse strateegia” – Vabariigi valitsuse korraldus 156-K, 28.02.01;

A.Aamer „Strateegiline juhtimine”, 1998;

J.Leimann, P.-H. Skärvald, J. Teder „Strateegiline juhtimine.“ 2003;

„Kaitsejõudude side-eeskiri” kinnitatud kaitseväejuhataja poolt 2001;

„Kaitsejõudude infotehnoloogia eeskiri” kinnitatud kaitseväejuhataja poolt 2000;

„Riigisaladuse seadus” Vastu võetud 26. 01. 1999 riigikogu poolt;

„Elektroonilise side seadus” Vastu võetud 8. detsembril 2004. a riigikogu poolt