DOI: 10.5937/vojdelo1708189T

БАЗА ЗА ПОДРШКУ КОМАНДОВАЊУ – ЕФИКАСНЕ, СИГУРНЕ И ПОСТОЈАНЕ ИКТ И ЕЛЕКТРОНСКЕ ОПЕРАЦИЈЕ У СВИМ СИТУАЦИЈАМА*

Jean-Paul Theler, *Daniel* Zuber**

База за подршку командовању обезбеђује модерне информационо-комуникационе технологије (ИКТ) и електронске операције и даје важан допринос ефикасности командовања војском у свим ситуацијама. Она обезбеђује везе и размену података непрекидно и свугде. За разлику од доприноса ефикасности командовања које пружа цивилни сектор, чији су уређаји и системи „подешени" на мирнодопско стање, база своје задатке у посебним и ванредним ситуацијама мора да извршава без прекида. Сигурна, аутономна и на кризе отпорна подршка ефикасности командовања и убудуће ће се очекивати, што је и разлог постојања базе.

Кључне речи: *ИКТ инфраструктура и системи, четири тезе о значају ИКТ, рачунарски центри, стационарни, полумобилни и мобилни информациони и комуникациони системи, Програм „Командна инфраструктура, информационе технологије и повезане мреже – инфраструктура војске"*

Кратак преглед четири тезе

У раду су кроз четири тезе представљене аргументације, сажета гледишта и наведене последице које указују на растући значај ИКТ у прикупљању и дистрибуцији информација. Поред тога, истакнута је разлика између цивилних ИКТ и специфичности једне аутономне војне ИКТ организације.

Теза 1

Значај ИКТ у прикупљању и дистрибуцији информација ће и наредних година знатно расти. Истовремено, то се неће свесно искористити (приметити).

---

* Овај текст је објављен у часопису швајцарске војске *Military Power Revue* бр. 1/2015, стр. 41-55, под насловом „Die Führungsunterstützungsbasis (FUB): für effiziente, sichere und permanente IKT – und elo Op-Leistungen in allen Lagen". Са немачког језика текст је превео и за објављивање припремио мр Здравко Зељковић, пуковник у пензији.

** Jean-Paul Theler (Жан-Паул Телер), дивизионар, dr oec, публициста, командант Führungsunterstützungsbasis FUB, jean-paul.theler@vtg.admin.ch и Daniel Zuber (Даниел Цубер), dr sc techn., dipl.el-ing, пуковник у ГШ, заменик команданта Führungsunterstützungsbasis FUB, daniel.zuber@vtg.admin.ch

Теза 2

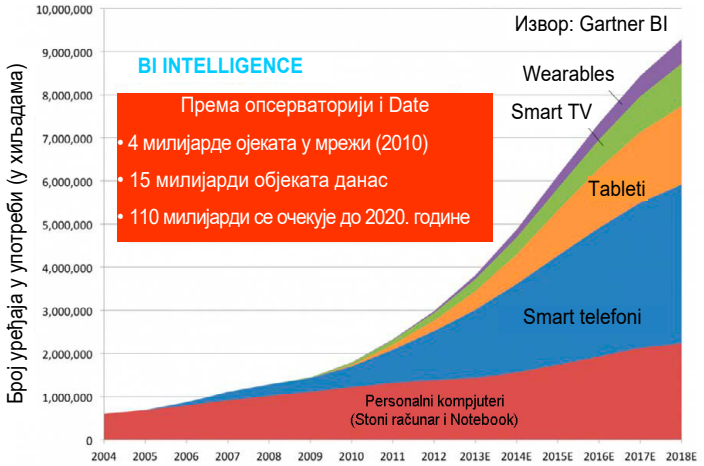
Степен заштите цивилних ИКТ не обезбеђује специфичне потребе војске.

Теза 3

Војсци је потребна сопствена ИКТ инфраструктура као и ИКТ системи, који ће аутономно функционисати.

Теза 4

Само организација која се састоји од цивилне и војне професионалне компоненте може обезбедити успех у свим ситуацијама.



Слика 1 – *Извор: gkofiannan.com*

Слика 2 – *Повезивање 50 милиона корисника: нове технологије имају све краћи период увођења у свакодневну употребу. Извор: gkofiannan.com*

Теза 1

Значај ИКТ у прикупљању и дистрибуцији информација ће и наредних година знатно расти. Истовремено, то се неће свесно искористити (приметити).

Растући захтеви, повећање аутоматизације и оптимизације

Развој ИКТ се последњих 10 година одвијао у два главна правца: с једне стране експоненцијално растући захтеви корисника на тржишту, а с друге стране кроз аутоматизацију и оптимизацију најразличитијих пословних процеса.

Са оптимизацијом пословних процеса постиже се већа ефикасност у производњи, и то кроз аутоматизацију фаза самог процеса. Даља оптимизација односи се на побољшање логистичког ланца временски усаглашене доставе роба ради смањења потребног складишног простора, по мери сачињеног списка захтева специфичних сегмената клијената.

Ови захтеви узрокују дуже и више конвергенције телекомуникационе и информационе технологије (ИТ), која ће се наставити и наредних година. На пример, то ће најмање мобилне апарате повезати са све повољнијим ценама за мобилни пренос података и водити ка томе да подаци и њихово коришћење буду практично свуда и у сваком тренутку доступни. „Укључивање" у праксу ове могућности у свакодневним пословима и приватном животу не искључује просту размену текстуалних садржаја (SMS) – они ће преживети и још више напредовати.

Будуће технолошке могућности

У будућности ће то водити ка још већим количинама података – могућности за огромну базу најразличитијих података (од online shoping-a, преко мобилних профила, па све до медицинских релевантних информација),[1] а с тим и ка великом броју нових могућности. Међутим, индустријски процеси, комерцијализовањем преноса и меморисања података добијају растућу базу података, што је добра основа за прикупљање информација и њихово преузимање са Big Data Methoden (алат за обраду великих количина информација, односно претраживач са алгоритмом огромног не структурираног мноштва података), што пружа могућност нпр. за проширење, (екстраполацију) потенцијалних жеља клијената на основу односа на тржишту (понуде и потражње), па све до сазнања о стању система умреженог комплексног уређаја.

Да би се то могло превазићи, под оваквим захтевима и постојећим притиском трошкова, потребан је развој интелигентних алгоритама и промена парадигме код формулације питања вредновања података – посебно даљи технолошки развој брже, расположивије и веће меморије података синхронизоване са скалабилном[2] снагом рачунара.

[1] Данас од 4 милијарде умрежених објеката широм света на персоналне рачунаре (PC) отпада 50%. Године 2020. тај проценат ће се смањити на 10%, будући да ће умрежавање најразличитијих елемената (нпр. фрижидера, микро-таласних пећница, пумпи, аутоматизовање кућа/станова, итд.) и даље знатно расти („Internet of Things)". Извор: Gartner Business Inteligence

[2] Скалабилност је могућност апликације да поднесе повећање захтева и броја корисника, а да сама не мора да се мења. Што је апликација скалабилнија она ће лакше поднети повећан проток података. Циљ ко-

Концепти као Cloud, Grid или Fabric-Computing (умрежена рачунарска чворишта аналогно сађу, односно пауковој мрежи или „fabric" тканини) базираним на ранијим простим појединачним системима, могу се остварити тек у тесном повезивању и умрежености многих појединачних система и уз примену интелигентне контроле појединачних умрежених система.

Ефекти

Ефекти ових трендова развоја могу се разврстати у четири групе:

1. Друштвени ефекти

Јасно је да располагање информацијама у сваком тренутку, за најважније службе у сваком месту, расте и да ће се у будућности још повећавати и утицати на свакодневни живот: мобилно телефонирање, мобилни рад, online shopping, online voting или online banking само су део могућих области примене. Употребом дигиталних „помоћника" мењају се захтеви, способности и могућности (нпр. договор о раду и породица). С друге стране, овим развојем ће се транспарентност индивидуа знатно повећати и, адекватно опасности, дигитална умреженост и надзор ће престати. Неопходна инфраструктура и трошкови за њено функционисање за кориснике нису видљиви и тиме ће као „једноставни" и „дати" бити подразумевани.

2. Инфраструктурни ефекти

Захтеви корисника, да податке и услуге у свако време имају на располагању, а да за то плате ниску цену, води ка томе да фирме морају много инвестирати у модерну инфраструктуру. То почиње у великим рачунским центрима, чије потребе за енергијом генеришу велики део укупних трошкова. Постојеће ИТ инфраструктуре (сервер, меморија, мреже) током времена прогресивно расту и формирају платформе по мери корисника услуга. Пренос података од рачунских центара ка корисницима одвија се преко јаке фиксне мреже или преко на њих прикључених ћелијских инфраструктура (3G, 4G итд.) ради омогућавања мобилности корисника. С обзиром на то да су потребе рачунских центара за локацијама за зграде и електричну енергију ограничене, мобилно коришћење ширег пропусног опсега у фреквентном спектру са порастом протока података изискује већу густину антенских станица.

3. Функционални ефекти

На основу расположивих података из најразличитијих извора могуће је, начелно, боље аргументоване одлуке формулисати и донети их у краћем времену.

Са овим подацима и повећаним умрежавањем и прибављање информација и њихова дистрибуција знатно ће се убрзати. Постоји опасност да се дигитална „шу-

---

јем теже сви пројектанти система јесте да се постигне линеарност у брзини одговора на захтев и количине података са којима се манипулише. Када је реч о самом хардверу, постоји хоризонтална и вертикална скалабилност. Вертикална скалабилност значи да је апликација смештена на једном серверу, а на повећан проток се реагује тако што се серверу додаје меморија, јачи процесор, нова језгра или додатни хард диск. Хоризонтална скалабилност је квалитетније решење, посебно за велике системе. Додавањем нових чворова систем наставља да ради као до тада, само са новим играчем (чвором) у тиму. Чвор представља један сервер. Напомене преводиоца, извор: http://ns2.math.rs/~vladaf/Courses/Matf%20MNSR/Prezentacije%20Individualne%20Stare/Veljkovic_NoSql_baze_podataka.pdf, приступљено 18.11.2017.

ма од бучног дрвећа" више не може видети. Ипак, на основу модерних технологија обрада података (нпр. Big Data) смањиће се. Заокрет од стратегије „формулација питања покреће алгоритам" ка стратегији „подаци терају на формулацију проблема", ипак води ка дубљем промишљању у дефинисању захтева.

4. Економски ефекти

Увођењем скалабилних прилагодљивих технологија и њиховог брзог развоја, са оптимизираним инфраструктурама, могуће је држати трошкове на релативно ниским нивоу. На тај начин ће контрола и управљање аутоматизованим процесима бити јефтинији и водиће ка наредним корацима аутоматизације, односно повећању оптимизације.

Консеквенце

Са растућом умреженошћу услуга свих врста знатно се повећала ИКТ зависност модерног, дигитално организованог друштва. Привреда, саобраћај, снабдевање, комуникације и управа, али и извођење војних операција све више и јаче зависе од непрестаног и несметаног функционисања ИКТ.

Са сваким технолошким трендом расту и захтеви корисника услуге за напреднијим ИКТ. Аутоматизацијом ће се превазилазити све комплекснији процеси и задовољити очекивање за једноставним руковањем, а да се то свесно на користи (примети). При том се корисници не интересују за огромна средства која се морају инвестирати, како би се путем истраживања, развоја и примене могле задовољити данашње потребе.

На једној страни овај тренд нуди шансе да се нове технологије прихвате, а на другој постоји опасност да ће безбедност бити запостављена растућом аутоматизацијом и једноставнијом употребом. То у војном окружењу, посебно у домену подршке командовању, умножава специфичне безбедносне захтеве. Ипак, они могу бити реализовани само редуковањем на апсолутно неопходне за употребу и уз додатне издатке за безбедносне мере.

Теза 2

Степен заштите цивилних ИКТ не покрива специфичне потребе војске.

Функционалност изнад свега

Највиши степен умрежености и уз то највећи ниво услуга цивилном свету у свакодневном животу пружа знатан комфор. У цивилном окружењу функционалност за кориснике и профит за предузетнике налазе се у првом плану, а за њима безбедност најчешће шепа пратећи их.

Функционална способност ИКТ је у нормалној ситуацији изложена не само „логичким" опасностима у форми хакерских напада, уништења или манипулације пода-

цима, искључивања компоненти итд. И „физичко" уништавање (нпр. природне непогоде, криминалне активности итд.) или „техничке" хаварије (нпр. технички кварови, грешке у софтверу или хардверу или погрешно руковање персонала, итд.) могу трајно утицати на функционисање ИКТ. То значи да се ИКТ системи морају штитити још пре наступа случаја релевантне опасности.

Мере заштите

Мере заштите захтевају „логичко" јачање (нпр. раздвајање менаџерског од корисничког саобраћаја, имплементацију безбедног аутентичног идентификовања и приступних механизама) и „физичко" каљење (нпр. контролу приступа осетљивим просторијама, инсталацијама, електроагрегатима за случај нужде) које мора бити спроведено још у фазама развоја и изградње. Могуће даље мере су: „евалуациона техника" (нпр. она обухвата проверене производе) или „Multivendor-Strategie" тј. избегавање (пре)велике зависности од појединих добављача производа. Имплицитно, већ код дизајнирања система мора се обезбедити „способност против деградације" тј. осигурање бар минималне способности за функционисање код квара или сајбер напада. Да би се техничким мерама могао постићи пун ефекат потребно је имати довољно стручног кадра који располаже неопходним стручним способностима, који се редовно едукује и који ће се даље усавршавати.

Све ове мере значе, с једне стране, повећање обима инвестиција, а са друге губитак максималног степена слободе корисника.

Наведене мере заштите не интересују директно ни купца ни корисника на масовном ИКТ тржишту. Њихово очекивање примарно је фокусирано на функционалност крајњег уређаја и трошкове.

Подаци, информације или апликације морају бити доступни у свако време, свуда и на свим мобилним апаратима, преко најбољих и најбржих веза, укључивши и неопходну подршку. У том смислу цивилни добављачи нуде највећи комфор и највишу могућу флексибилност, с једне стране како би испунили растућа очекивања својих клијената, а са друге да би повећали профит. При томе они стално морају пазити на то да трошкови буду нижи од цене коју је корисник спреман да плати.

Расположивост, односно квалитет сервиса у томе има знатно нижу вредносну позицију него у војној варијанти или у професионалном пословном окружењу. Ипак, очекивања цивилног и војног окружења се не разликују битно. И припадници војске очекују да су сервиси увек расположиви и да све несметано функционише. Али, цивилни корисник (то је очигледна разлика у односу на припаднике војске) није сигуран да ће његова очекивања бити у потпуности испуњена, јер он ту најчешће и не трпи директну штету. То је у војном окружењу, односно у ангажовању, значајна разлика.

Али, шта се дешава ако се у садашњем комплексном и непредвидивом времену, са хаотичним и забрињавајућим тенденцијама, са хибридним опасностима које углавном нису видљиве, изненада и ни из чега деси саботажа на циљаној ИКТ? Умрежени свет отвара недржавним актерима са политичким, религиозним (џихадистичким), терористичким или криминалним намерама једно велико поље за акције, посебно у виртуелном простору.

Циљани сајбер напади

Данашњи и будући технолошки развој води ка томе да сваки оружани конфликт, али и војно ангажовање испод прага рата, буде пропраћено активностима у сајбер простору, односно припремама и извођењу сајбер напада.

Уопште, сајбер претње и ризичне ситуације су се, како за државне институције, тако и за привреду и приватна лица, драстично заоштриле. Један сајбер напад би, по правилу, неочекивано ограничио начин функционисања на великом простору, изазвао повремене или дуже сметње, прекиде или чак испадање из рада – посебно критичних инфраструктура као што су нпр. телекомуникације, снабдевања енергијом, јавног саобраћаја или спасилачких служби итд. – имао би фаталне последице по Швајцарску. Али, ни војска са њеним бројним ИКТ системима, експлицитно није поштеђена од овакве опасности.

У једној посебној или ванредној ситуацији, када цивилни провајдери због преоптерећења или могућег прекида у снабдевању енергијом више не могу пружати услуге, војска мора бити спремна да у свако време буде на располагању са својим ИКТ системима. Само тако војска, као „стратегијска резерва" савезне владе, може испунити своју уставну улогу: осигурање безбедности земље и становништва.

Поред осталог, војска мора:

– да обезбеди релевантне информације и да их ажурира,

– да своју спремност прилагођава према ситуацији како би била у стању да на брзо измењену ситуацију реагује и реализује своје задатке заштите,

– да средства за командовање штити од спољњих утицаја, јер без њих нема ефикасне употребе једне модерне војске,

– да располаже робусним средствима, како би у једном стварно озбиљном случају могла брзо и ефикасно да интервенише.

Консеквенце

Спектар ангажовања војске захтева функционалне способности и расположивост ИКТ у свим ситуацијама. Због тога дивергирају захтеви за ИКТ између цивилног и војног света по питању елиминисања ризика, као и у погледу робусности припремљених мера.

Слика 3 – *За заштиту од „физичких", „логичких" и „техничких" негативних утицаја потребне су адекватне мере, поред осталих у форми од „физичког" и „логичког" јачања до сајбер одбране. Али, потребни су и системи са изразитим разарајућим способностима. Извор: FUB (SYR/EYR)*

Слика 4 – У оквиру сајбер претњи актери се могу грубо разврстати у пет нивоа. Комплексност напада и за то неопходна know-how расту одоздо нагоре. Средства за ниже угрожавајуће категорије могу се у великој мери набавити на тржишту. Међутим, виши угрожавајући нивои ипак захтевају специјалне стручне компетенције, а делом и способности, сопствене специфичне мере развоја и примене. Извор: MPR Nr. 2/2013 Cyber-Defence: Quo Vadis? Abb. 2,3

Подразумева се да су целокупне, за командовање неопходне ИКТ инфраструктуре заштићене од активних и пасивних претњи. Ова заштита у поређењу са мерама заштите код цивилних инфраструктура исте врсте је робуснија, аутономна и на кризе отпорна, како би способност за командовање у свим ситуацијама била осигурана,

Укупне војне ИКТ инфраструктуре такође су „физички" заштићене од дејства оружја, у електромагнетном простору, као и у домену HPE (High Power Elektromagnetic), ABC (Atomar-Biologischer-Chemisch) (АБХ) итд. На пример, кабловске трасе треба инсталирати дубље у земљишту или ако треба прећи реку онда је то потребно радити испод, а не преко моста.

Наравно, све мреже су „логички" потпуно криптолошки заштићене – „од краја до краја" („End to End„) „закључане" (веза између две тачке или места), а то све указује на њихову високу отпорност на уништење. Активности у мрежама контролишу се и предузимају неопходне мере против покушаја напада из сајбер простора (преко професионалних организација или сајбер криминала, циљно усмерених и непрепознатљивих агената/организација и служби високоразвијених ИТ земаља) за заштиту рачунара и система.

За осигурање аутономије војска поседује сопствене моћне рачунске центре за меморисање (чување) података и за функционисање критичних апликација. Од тренутка одвајања од приватних провајдера она ставља у функцију независну командну мрежу Швајцарске за комуникацију и сигурну размену података у свим ситуацијама. Што се тиче отпорности на кризе, издржљивост професионалне организације са војном компонентом је знатно већа. Све неуралгичне ИКТ инфраструктуре (нпр. рачунски центри, комуникациона чворишта итд.) снабдевене су сопственим агрегатима за производњу електричне енергије и опремљене одвојеним резервоарима дизел горива за функционисање код дужег прекида јавног снабдевања струјом. Уз то, само је један део ИКТ система намерно (свесно) аутоматизован, с једне

стране, како би се постигла што већа аутономија од добављача, а, с друге стране, како би се услед кварова система спречиле последице на широј територији.

Док су раније цивилни провајдери покушавали испунити комерцијалне, тржишне и профитно оријентисане потребе својих клијената и тако даље наставити нове трендове, за војску је примарна била робустност производа и безбедност. Наиме, робусност је од одлучујућег значаја за способност командовања војском у свим ситуацијама. Проблем се састоји у томе што на основу производно-економске логике цивилног предузетника тако специфични безбедносни захтеви нису изводљиви, јер би се на тај начин његова профитна стопа знатно смањила. Због тога је за посебне и ванредне ситуације потребна једна ваљана ИКТ алтернатива коју ће војска у потпуности искористити.

Теза 3

Војсци је потребна сопствена ИКТ инфраструктура и ИКТ системи, који ће аутономно функционисати.

База за подршку командовању пружа свеобухватне мере подршке и омогућава способност командовања електронским операцијама савезне владе и војске у свим ситуацијама. База у домену подршке командовању гради стационарну (фиксну) и штићену ИКТ инфраструктуру и за друге техничке делове командне инфраструктуре. Командна инфраструктура и њене техничке инсталације тесно су умрежене са ИКТ инфраструктуром, што обухвата комуникационе мреже, инфраструктуре рачунских центара и сензорских уређаја.

Комуникационе мреже

Комуникационе мреже обезбеђују везе између сталних командних постројења, сензорских (и предајних) уређаја, кључних инфраструктура војске (нпр. аеродрома, логистичких постројења) и инфраструктура рачунарских центара. Пренос података ће се реализовати помоћу јаких стационарних системима са усмереним зрачењем и опремом са оптичким кабловима. За по(у)везивање привремених, полумобилних система или јединица (положаја) постоји низ прикључних места (прикључака) на високо расположиву и врло моћну комуникациону мрежу.

Повезивање ће се обезбедити, с једне стране, са усмерено зрачећом прикључном мрежом на висока (виша) постројења (на вишим нивоима), а, са друге стране, осигурано је пољским широко појасним прикључним кутијама, опремљеним оптичким каблом.

Инфраструктуре рачунских центара

Инфраструктуре рачунских центара обезбеђују главне и потпуне рачунарске услуге за команде, информационе и оружане системе. Тежишно се одвија из заштићених рачунских центара које у потпуности контролише војска. То омогућава да велике количине података у свим ситуацијама остану у рукама војске и не могу бити неовлашћено коришћени нити изузимани.

Сензорска постројења

Сензорска постројења обухватају активне (нпр. радарски системи) и пасивне сензоре, нпр. сензоре за вођење електронског рата (Elektronische Kriegsführung – EKF), који прикупљају податке за приказ ситуације у ваздушном простору. Сензорска постројења су тако распоређена да се унутар Швајцарске увек може добити максимална количина података с обзиром на географске пропорције на копну и у ваздуху. Са полу мобилним сензорским системом може се добити слика стања и, сходно ситуацији и задатку, изражавати тежиште и добијати додатни подаци.

За потпуни успех биће потребни, поред стационарних и сталних, и полумобилни и мобилни информациони и комуникациони системи.

Полу мобилни информациони и комуникациони системи

Са полу мобилним, односно, према потреби, привремено стационарним широко појасним комуникационим системима (нпр. усмерено-зрачећи, релејни и телефонски системи) омогућено је да се нова подручја (простори) искористе за „погушћавање" постојеће мреже и радио-интеграција за мобилне, тактичке комуникационе системе. То се базира на прикључним местима (усмерено-зрачеће прикључне мреже и пољске широко појасне прикључне кутије), сталним, високо расположивим, широко појасним и заштићеним комуникационим мрежама.

Са полу мобилном инфраструктуром постићиће се максимална модуларност, а тиме и повећање слободе деловања (укључујући могућност повезивања у пограничном појасу са суседним земљама). Поред тога, постоји и могућност прикључења полу мобилних командних уређаја, као и широко појасних сензора и ефектора (нпр. у BODLUV), директно или индиректно на сталну високо расположиву мрежу података.

Мобилни информациони и комуникациони системи

Командне, извиђачке, мреже управљања ватром и логистичке мреже ангажованих копнених састава и бригада на свим нивоима биће тежишно снабдевени мобилним тактичким системима радио-везе. За специфичне задатке на земљи и у ваздуху биће употребљени тактички линкови података. Ангажованим системима то омогућава сигурану, али пре свега уско појасну предају компримованих дефинисаних података. Са радио-интеграцијом тактичких везе у полу мобилну и сталну мрежу може се обезбедити „проходност" ка крајњим стационарним уређајима или крајњим цивилним мобилним уређајима. Поред тога, мобилни корисници тактичке мреже могу се повезати на велике даљине помоћу сталних, стационарних инфраструктура.

Функционисање ИКТ инфраструктура и ИКТ система

За функционисање стационарне (сталне) ИКТ инфраструктуре примарна је професионална организација – база за подршку командовања (FUB) коју, по потреби, у сваком тренутку подржавају припадници војске, односно Бригада

за подршку командовања 41/SKS (FU Br. 41/SKS = системи – обука кадра – подршка).[3]

Функционисање полу мобилних ИКТ система одвија се кроз батаљон усмереног зрачења (Ristl Bat.) базе за подршку FU Br. 41/SKS. То обезбеђује интегрисани војни телекомуникациони систем (Integriertes Militärisches Fernmeldesystem – IMFS) прикључним местима за потребе оперативног органа великих војних састава и њихових делова. Командна места великих састава ће преко батаљона за подршку командовању (FU Bat) на чвориштима бити прикључена на интегрисани војни телекомуникациони систем IMFS. Оперативни састави, али и тактичке јединице РВ и ПВО, располажу сопственим IMFS средствима, па се тако самостално могу интегрисати у полу мобилне ИКТ инфраструктуре.

Батаљони усмереног зрачења (тип Б) стоје на располагању за радио-интеграцију (Radio Access Point – RAP) дуж комуникационих оса или простора ангажованих састава. Коначно, за ангажоване мобилне радио-системе (VHF, UHF, HF) могу се користити сви састави, односно припадници војске.

Пројекат „Командна инфраструктура, информационе технологије и по(у)везивање у мрежу – инфраструктура војске"

Да би се ефикасност ИКТ могла дугорочније обезбедити, до сада су била покренута три пројекта: 1. Рачунски центри МО/Савеза 2020 („Rechenzentren VBS/Bund 2020" – RZ VBS/Bund 2020); 2. Командна мрежа Швајцарске („Führungsnetz Schweiz" – Fhr N CH) и 3. Телекомуникације војске („Telekomunikation der Armee" – TKA), који су усаглашавани и обједињени у програм *Командна инфраструктура, информационе технологије и по(у)везане мреже – Инфраструктура војске* („Führungsinfrastruktur Informations – Technologie und Anbindung Netzwerk – Infrastruktur der Armee" (FITANIA).

а) Пројекат *Рачунски центри МО и Савеза 2020* („*Rechenzentren VBS/Bund 2020*")

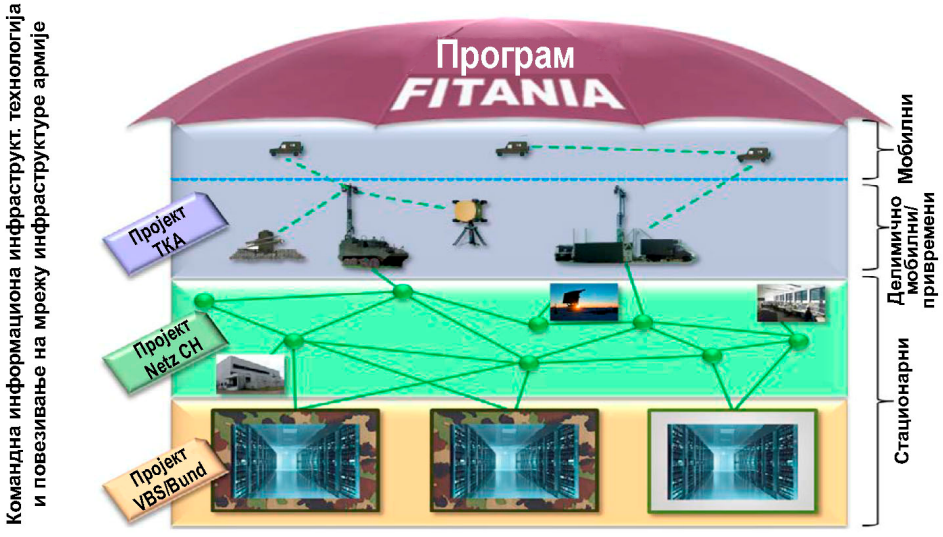
Као последица брзог раста количине података, Савез је са постојећим ИКТ инфраструктурама „ударио" у границе снага и границе капацитета. Како би војска и даље могла стално, сигурно, аутономно и на кризе отпорно да контролише и сачува своје податке Министарство одбране, заштите становништва и спорта, а тиме и База, планирало је да у сарадњи са „цивилним" министарствима Савеза формирају „Центар података" на националном нивоу. Спровођење пројекта „RZ VBS-BUND 2020" предвиђа, на основу високих безбедносних захтева, с једне стране, два војна рачунарска центра са потпуном заштитом („Härtung") и цивил-

[3] Бригада за подршку FU Br. 41/SKS има 14 активних састава (батаљона, чета, група). Она, с једне стране: 1. подржава ситуационо и по месту деташиране делове и пружа им помоћ (нпр. деташираном батаљону усмереног зрачења – Det Ristl Bat. 4.); 2. омогућава рад деташираног батаљона за вођење електронског рата 46 – Det. EKF Abt. 46; 3. пружа подршку у прикупљању информација за центар за електронске операције – омогућава информисање становништва преко савеза у кризним ситуацијама (предајни уређаји) (IBBK – Information der Bevölkerung durch den Bund in Krisenlage) (Sendanlage). С друге стране, делови бригаде задужени су да са другим јединицама различитог нивоа пружају директну подршку командовању при употреби великих састава на вежбама војске (нпр вежба INTERARMES).

ног рачунарског центра са делимичном заштитом. Инфраструктура рачунарског центра је осигурана, како централизовано, тако и децентрализовано како би високо расположивим могућностима меморисања и обраде података „хранила" информационе, командне сензорске и оружане системе. На тај начин је обезбеђено да се у свако време може приступити релевантном систему у раду и апликацијама. Поред осигурања високе расположивости и безбедности, централизацијом на мање и ефикасније рачунске центре могуће је рационализовати трошкове коришћења.

б) Пројекат: *Командна мрежа Швајцарске* („*Führungsnetz Schweiz*")

За достављање информације, односно података, морају се испунити високи безбедносни захтеви и захтеви расположивости рачунских центара због чега војска гради и користи сопствену, од цивилних провајдера независну комуникациону мрежу – мрежу командовања Швајцарске. То је на низ места (гарнизона) повезана стална транспортна мрежа, која се базира на широко појасним везама оптичких каблова и усмерених радио-веза. Да би се обезбедила висока расположивост везе, она ће бити „развучена" и прилично комплексно израђена. С једне стране, подаци ће пре достављања бити шифровани, а с друге стране инфраструктура командне мреже је ојачана, тиме и заштићена од употребе силе, прислушкивања и сајбер напада. Једино тако војска може стално, сигурно, аутономно и на кризе отпорно осигурати податке између стационарних командних уређаја, рачунарских центара, сензорских и предајних уређаја, као и кључне инфраструктуре војске.



Слика 5 – *Програм FITANIA обухвата три пројекта: RZ VBS/Bund 2020, Fhr N CH и TK A. Извор: FUB (BJ)*

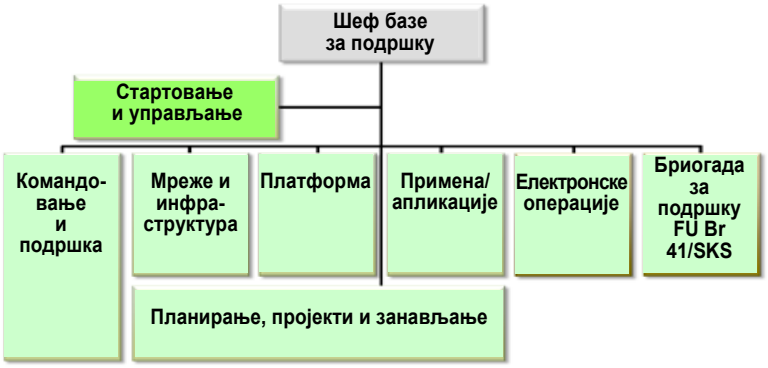
в) Пројекат *Телекомуникација војске* („*Telekomunikation der Armee*")

Телекомуникација војске обухвата говорну, фото, видео комуникацију и комуникацију података за потребе мобилног или полу мобилног командовања. Како би све то било пренесено од фиксних командних места, односно преко командне мреже Швајцарске до мобилних и полу мобилних елемената, потребна је сопствена, осигурана, модуларна, полу мобилна и мобилна телекомуникациона мрежа. И овај пројекат поставља високе безбедносне захтеве – да пренос података између фиксних, делимично мобилних и мобилних ИКТ система буде сталан, сигуран, аутономан и на кризе отпоран. За повезивање мобилних корисника неопходне су аутономно функционални и самоорганизовани комуникациони уређаји. Крајњи мобилни уређаји ће, поред осталог, имати неопходне софтвер апликације које ће преко безбедносних улазано-излазних капија (Gateways) (обухвата све ИТ системе, који су надлежни за ИТ безбедност) омогућити приступ за коришћење неопходних података командно- информационих система (Führungsinformationssysteme-FIS) војске.

Консеквенце

Целокупне ИКТ инфраструктуре и ИКТ системи, који су потребни за командовање у свим ситуацијама, морају преко професионалне организације базе за подршку командовању (FUB) и њеног војног дела FU Nr 41/SKS бити контролисани и коришћени. То конкретно значи: планирати, израђивати, користити (подршка крајњих корисника у случају квара, идентификација неисправне компоненте укључујући и њену замену), одржавати и штитити.

Изузетак су специфичне апликације код којих способност за аутономну импровизовану поправку мора постојати, пошто високоспецијализованих стручњака има врло мало на тржишту рада. Специфична безбедносна стручна знања (нпр. криптологија, шифровање, безбедносна архитектура итд.) и контролисање система неопходних за рад морају и даље развијати специјализовани стручњаци из професионалне организације базе за подршку (FUB). Војска се при том штити технолошким развојем и производима, које су приватни предузетници преконтролисали и понудили, јер јој за аутархично планирање и развој недостају финансијски и персонални ресурси. Слично се односи и на употребу не релевантних комуникационих мрежа, које се користе за управљање, као нпр. мрежа приправности (Bereitschaftnetz-Ber N). Сва средства и снаге које нису директно релевантне за употребу, тзв. базне снаге, могу бити, у сарадњи са цивилним партнерима, изостављене или чак сведене на услужне.



Слика 6 – *Нова организација базе за подршку командовању. База је организована на „производном" принципу како би потпуно покрила потребе „производима" као што су: мреже, платформе, апликације, електронске операције, употреба и вежбе бригаде за подршку командовању FU Br. 41. Извор: FUB (SYR/EYR)*

Теза 4

Само организација која се састоји од цивилне и војне професионалне компоненте може обезбедити успех у свим ситуацијама.

Растући захтеви ка добављачима

Технолошке промене и из њих произишле нове потребе, односно очекивања корисника, преламају се преко војске. Корисници на основу својих доктрина и из њих проистеклих захтева дефинишу код базе (FUB) своје ИКТ потребе. Захтеви стоје у центру и дефинишу обим и квалитет производа које треба да добију од базе (FUB).

Велики изазов сада је у томе како спојити децентрализоване интересе различитих корисника који су, углавном, независни једни од других, а базирају се на истом ИКТ „силос" систему, са јединственом функционалном целином (јединствена платформа). Као начин решења проблема за уједначавање служи платформа као сервис („Platform as a Service" – PaaS) која је постављена на свим модерним апликацијама. С тим се тренд од „Све као сервис" („Everything as a Service") може ставити на располагање толико масовно колико је то могуће и потребно и у оквирима војске. За решење уједначавања за даље трајно пружање услуга, као и спровођење (великих) пројеката, ИКТ инфраструктура, која је потребна добављачима мора да буде обновљена и прилагођена новим технолошким способностима. Обнова напредује, али је праћена са повећаним захтевима за дуже радно време (7x24 часа), као и новим системом коришћења (нпр. „Unified Communication and Colaboration" тј. интегрисане комуникационе инфраструктуре које нуде палете могућности за оптимизацију комуникације између тимова као и између појединаца). Истовремено, у оквиру да-

љег развоја војске (WEA) планирано функционисање базе (FUB) прилагодиће се захтевима наредних година. Намерно или не прећуткује се захтев за финансијском ефикасношћу. Ови фактори воде ка томе да база (FUB) сада мора прилагодити своје структуре како би нове инфраструктуре и системе могла ефикасно и оптимално користити и потпуно искористити своје задатке са почетком планираног даљег развоја војске.

Слика 7 – *Сталне и повремене активности базе: база (FUB) извршава сталне и повремене задатке. Сталне извршава помоћу професионалне организације FUB, а повремене преко војног састава базе FU Br. 41/SKS. Кључне задатке извршава професионална организација FUB у свим ситуацијама безбедно и стално. Основна ИКТ средства купују се од цивилних провајдера и у принципу се не користе у посебним и ванредним ситуацијама. Извор. FUB (SYR/EYR)*

Реорганизација базе за подршку командовању (FUB)

Нова структура базе (FUB) заснива се на производном принципу („Managed Service Provider") и покрива укупне потребе командовања: мреже, платформе, употребу (примену) и електронске операције, а то и јесу производне области базе (FUB). Поред тога, биће изграђена два попречна пресека: подршка командовању и подршка (укључујући и употребу) и планирање пројеката и за обнављање планирања, одржавања и даљег развоја ИКТ могућности. Као штабна функција образује се област стратегије и управљања везама ка потчињеним саставима и осигурава дугорочна концепција.

Као и до сада, бригада за подршку FU Br. 41/SKS остаје „војна рука" Базе за подршку командовања (FUB). Ова нова структура ослања се на постојећу организацију и оптимизира је у кључним областима. Командант базе (FUB) сноси пуну одговорност за управљање ИКТ у одбрани, па зато и има функцију „ИКТ специјалиста за командовање одбраном" („IKT-Fachführung Verteidigung") у тиму начелника Генералштаба. Еластичнијом структуром постојећи задаци ће се једноставније и ефикасније решавати. И нови дизајн појединачних продуката током укупног животног циклуса треба рационално уредити.

Профил задатака базе (FUB)

База (FUB) јесте компетентан провајдер за потпуну подршку командовања и ИКТ послова за потребе војске. У каталогу производа она, као давалац услуга, нуди корисницима у МО информатичке услуге у виду обимне палете производа: „експлоатација и подршка", „апликације", „ИТ платформе" или „мреже". База (FUB) може пружати услуге и другим министарствима, а по одобрењу министра одбране и организацијама ван савезне владе, као нпр. Безбедносном савезу Швајцарске (Sicherheitsverbund Schweiz – SVS). То, укључује и компетенције у области интегралне архитектуре, односно безбедносног концепта, као и експлоатацију система са високом безбедношћу података и расположивошћу, који ће увек бити достављани на захтев корисника.

Следећа надлежност FUB је домен „Рачунарске мрежне операције" (Computer Netzwerk Operationen – C NO) и „Рачунарски тим за брзе интервенције" (Computer Emergency Response Team – milCERT) за заштиту војне рачунарске инфраструктуре и развој и проверу решења у домену информатике и телекомуникација (област информационе безбедности и криптологије). Али, и активности у домену вођења електронског рата (elektronischen Kriegführung – EFK) са сензорима и ефекторима и у то укључено прикупљање информација за потребе обавештајне службе, такође припада портфолију базе (FUB).

База (FUB) пружа подршку војсци током вежби и њене стварне употребе. Преко Service Desk-а претплатници/корисници услуга могу директно добити Центар за помоћ у случајевима проблема и сметњи. Осим тога, база (FUB) са својим специјалистима брине о даљем развоју апликација и система. Коначно, као централни стручно-специјалистички ИКТ орган, она руководи одбраном у овом делу Министарства одбране.

База (FUB): Целокупан систем састављен од професионалаца и војне организације

База данас пружа континуиране услуге са 800 људи, већином цивила професионалаца (FUB), а у зависности од ситуације подржавају их и припадници војске из бригаде FU Br. 41/SKS[4] који су специјализовани за профил услуга потребних војсци. У једној заоштреној ситуацији бригада FU Br. 41/SKS би децентрализовано, као „Force Provider", сама пружила потребну подршку, као (целокупна) база за подршку командовању – FUB. Овакав спектар подршке омогућава бригадних 14 активних јединица, које се састоје од професионалног кадара и ИКТ инфраструктуре.

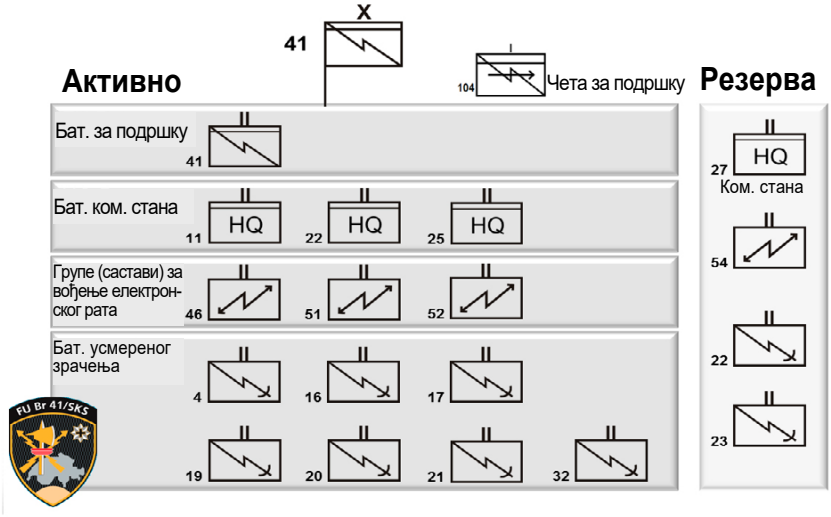
Бригада за подршку – FU Br. 41/SKS са својим батаљонима усмереног зрачења (Ristl Bat) опслужује комуникационе мреже војске, са батаљонима команде стана

[4] Профил услуга бригаде FU Br. 41/SKS детерминише њен бројчани састав од 30 људи из команде система, обуке кадра и подршке (Kdo SKS) стациониране у Rämling-u. То доноси задатке као што су: сарадња на пројектима наоружања, припрема система, подршка ангажовању, одржавање система, обука кадра у прикупљању и достављању информација и подршка командовању.

(ГШ) (HQ Bat.) системе за командовање савезне владе и војске, а са њеним специјалним групама вођење електронског рата (elektronische Kriegsführung – EKF). Батаљон за подршку – FU Bat. 41 стоји на располагању за посебне задатке (нпр. информатика, криптологија или специјалисти за стране језике).

Примерено положају и ситуацији може се обезбедити повећање густине ИКТ система и повећање капацитета постојећих мрежа или, штавише, постоји могућност интеграције додатних комуникационих средстава. С друге стране, у будућности се могу градити и децентрализована тежишта са полу мобилним и мобилним рачунарским центрима.

Коначно, и издржљивост, посебно професионалне организације базе (FUB), може се повећати и осигурати. Да би у посебним ситуацијама и догађајима могла брзо пружити неопходну подршку, бригада FU Br. 41/SKS у свом саставу има чету за подршку, која се налази у високом степену готовости (FU Ber Kp 104) и која на целој територији Швајцарске током целе године обезбеђује војну подршку корисницима.



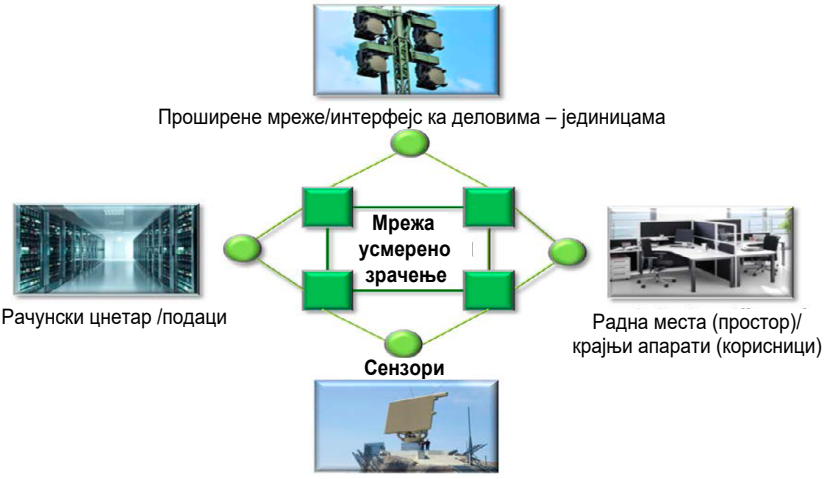
Слика 8 – *Бригада Br. 41/SKS, као „Force Provider" базе за подршку командовању (FUB): њених 14 активних јединица (батаљона, чета, група) и четири јединице у резерви попуњене су војницима на одслужењу војног рока (служе одједном и у целини – војници тзв. „Durchdiener"-и[5]). Бригада је најорганизованији и најјачи део базе за подршку командовању. Извор: FUB (SYR/EYR)*

[5] „Durchdiener" је припадник швајцарске војске, који своју укупну војну обавезу у трајању од 300 дана служи добровољно и без прекида (одједном). Овакав начин служења војног рока је законски ограничен на максимално 15% регрута једног годишта.

Војник који војни рок служи на овакав начин регрутује се према конкретним потребама центара за обуку и распоређује се тамо где је потребна висока спремност и издржљивост. Ови војници извршавају веома важне задатке заштите, чувања, подршке и пружања помоћи у катастрофама.

Остали војници служе војни рок у укупном трајању од 260 дана у више годишњих курсева обуке (кондицирања) у трајању од 19 дана. Тенденција смањења броја курсева и дана обуке се наставља. (напомена преводиоца).

Слика 9 – *Средства и снаге првог сата: бригада за подршку – Br. 41/SKS, са својим елементима одговорна је за ситуацију (стање) током првог сата (чета за брзе интервенције 104, деташман за вођење електронског рата – група 46 и деташман усмереног зрачења – батаљон 4, FU Durchdiener Kompanie 104, Detchement EKF Abt. 46 и Detachement Ristl Bat 4) у обезбеђењу правовремених мера подршке командовању у Швајцарској. Извор: FUB (SYR/EYR).*



Слика 10 – *За успешно командовање војском неопходан је ИКТ систем који добро функционише, рачунарски центри, јака стационарна мрежа, проширена мрежа (нпр. IMFS) са мобилним везама, радни простор и неопходне апликације. Извор: FUB (SYR/EYR)*

Слика 11 – *Девиза базе за подршку командовању (FUB)*

Консеквенце

Појединачни задаци базе за подршку командовању су усаглашени и обликоваће профил послова на нивоу Швајцарске.

Да би се обезбедило ефикасно командовање војском у свим ситуацијама неопходни су: функционалан систем који се састоји од: мреже, квалитетне усмерено-зрачеће везе за фиксну мрежу, рачунски центри, сензори и ефектори, проширене везе (нпр. IMFS), као и квалитетне везе (интерфејси) ка потчињеним јединицама. Посредством оваквих веза корисницима ће се преко радних места и крајњих уређаја ставити на располагање потребне апликације. Али, база (FUB) неће се моћи увек концентрисати на најбитније послове, него ће од свих задатака, преко свих технолошких нивоа, морати доставити оне које су неопходни, па ће ипак војска у свим ситуацијама моћи испунити своје задатке. Ове задатке ће са данашњим, а у будућности још бољим структурама, моћи да изврши. Коначно, импресивно је како целокупан систем базе за подршку командовању (FUB) функционише у тесној сарадњи између професионалне и војне организације (бригаде FU Br. 41/SKS). Истовремено су „производи" базе за подршку командовању (FUB) и база за подршку командовању других састава војске.

Закључак

База за подршку командовању (FUB) има задатак да осигура ефикасно командовање војском у свим ситуацијама. За то јој је потребна организација која се састоји од професионалне цивилне и војне компоненте. Под овом премисом целокуп-

не сталне ИКТ активности и дејства у електронским операцијама могу се сигурно, аутономно и на кризе отпорно реализовати. Робусна безбедност података и система је од одлучујућег значаја за висок степен њихове заштите. Цивилне ИКТ не покривају специфичне безбедносне потребе и безбедносне захтеве војске. Потреба за безбедношћу расте са повећањем значаја ИКТ, као и за прикупљањем и дистрибуцијом информација, које увек имају централно место. Ови захтеви изискују, поред оптимизације послова, и хармонизацију платформи са којима база за подршку командовању (FUB) може обезбедити ефикасне, сигурне и сталне ИКТ активности и дејства у електронским операцијама у свим ситуацијама, а да корисници и не примете за то неопходне токове.