ŠOLA ZA ČASTNIKE
IZREDNA GENERACIJA JANUAR 2012
SPECIALIZACIJA ČASTNIK OBVEŠČEVALEC

ZAKLJUČNA NALOGA

VARNOSTNA ZAGOTOVITEV VOJAŠKIH AKTIVNOSTI IN NAČRTOVANJE VARNOSTNE ZAGOTOVITVE

Kandidat: Stotnik Rok Ravnak

Mentor: Major Jože Grbec

Maribor, maj 2012

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO

SLOVENSKA VOJSKA
POVELJSTVO ZA DOKTRINO, RAZVOJ, IZOBRAŽEVANJE IN USPOSABLJANJE
Šola za častnike

Številka:
Datum:

ZAKLJUČNA NALOGA

VARNOSTNA ZAGOTOVITEV VOJAŠKIH AKTIVNOSTI IN NAČRTOVANJE VARNOSTNE ZAGOTOVITVE

Kandidat-slušatelj: stotnik Rok Ravnak

Mentor: major Jože Grbec

Maribor, 25. maj 2012
Engelsova ulica 15, 2111 Maribor

POVZETEK

Med izvajanjem vojaških aktivnosti se tudi v mirnodobnem času pojavljajo številna tveganja za varnost osebja in MTS, zaradi česar je izredno pomembno poskrbeti za ustrezno varnostno zagotovitev teh dejavnosti. Za uspešno varnostno zagotovitev dogodkov in dejavnosti pa je potrebno izdelati načrt varnostne zagotovitve, v katerem moramo vključiti vse ukrepe in aktivnosti, ki jih je potrebno izvajati v okviru varnostne zagotovitve. Temelj za izdelavo načrta varnostne zagotovitve pa je izdelana ocena ogroženosti, ki mora temeljiti na realnih grožnjah, sicer je v veliki meri neuporabna ali celo zavajajoča. Brez kvalitetne ocene groženj realnega in uporabnega načrta varnostne zagotovitve namreč ni mogoče izdelati. Za varnostno zagotovitev nosi ključno odgovornost poveljnik enote, organi J/S-2 pa dejansko v skladu z njegovimi usmeritvami in sodelovanju z drugimi organi načrtujejo in vodijo izvedbo. Načrtovanje varnostne zagotovitve je kompleksen proces, katerega nosilec so sicer organi J/S-2, vendar je potrebno pri tem zagotoviti sodelovanje vseh relevantnih faktorjev, tako specialistov na posameznih področjih kot tudi vojaške policije, Obveščevalno varnostne službe ministrstva, pogosto pa tudi civilne policije in ostalih civilnih inštitucij. Za uspešno izvajanje načrtovanih varnostnih ukrepov pa je potrebno vse udeležence v aktivnosti ustrezno pripraviti, sicer načrtovanje varnostne zagotovitve ne doseže želenega učinka.

KLJUČNE BESEDE

Načrtovanje vojaških dejavnosti, varnost, varnostna zagotovitev, zaščita sil, viri ogrožanja, varnostni ukrepi.

SUMMARY

There are also many risks to the safety and security of personnel and material during the conduct of military activities in peacetime period, so it is extremely important to provide adequate security measures to ensure these activities. To ensure adequate security and safety of events and activities it is necessary to develop a security plan, which should include all steps and actions to be performed to provide adequate level of security. The foundation for the security plan is threat assessment, which must be based on real threats; otherwise it is largely useless or even misleading. Without adequate assessment of real threats effective operational plan to ensure security can not be made. Key responsibility to ensure security lies on the unit commander, while J/S-2 must conduct planning and execution of security measures in cooperation with other institutions. Planning of security activities is a complex process for which J/S-2 bears key responsibility, but it is necessary to ensure the participation of all relevant factors, both specialists in particular areas as well as military police, the Intelligence and Security Service of Ministry of Defense, and often, civilian police and other civic institutions. The successful implementation of planned security measures requires that all participants in the activities are properly briefed and prepared; otherwise security plan will not reach the desired effect.

KEY WORDS

Planning of Military Activities, Security, Force Protection, Threats, Security Measures

KAZALO

1. UVOD

1.1 IZHODIŠČE ZAKLJUČNE NALOGE

Med izvajanjem vojaških aktivnosti se tudi v mirnodobnem času pojavljajo številna tveganja za varnost osebja in MTS, zaradi česar je izredno pomembno poskrbeti za ustrezno varnostno zagotovitev teh dejavnosti. Kakovost varnostne zagotovitev je tesno povezana s pravočasnim pridobivanjem informacij o morebitnih grožnjah, ki lahko segajo od prometnih nesreč in disciplinskih prekrškov, pa vse do protiobveščevalnih in varnostnih groženj, ki jih predstavlja delovanje tujih obveščevalnih in varnostnih služb, teroristov in nenazadnje organiziranega kriminala.

Za uspešno varnostno zagotovitev dogodkov in dejavnosti pa je potrebno izdelati načrt varnostne zagotovitve (oziroma načrt varnostne oskrbljenosti), v katerem moramo zaobjeti vse ukrepe in aktivnosti, ki jih je potrebno izvajati v okviru varnostne zagotovitve. Upoštevati moramo sodelujoče akterje (npr. enote, VP in tudi civilne varnostne organe). Vse dejavnosti je potrebno časovno opredeliti z roki izvedbe in pripraviti varnostne ukrepe, ki se bodo izvajali v toku vojaške dejavnosti ali dogodka.

Temelj za izdelavo načrta varnostne zagotovitve je izdelana ocena ogroženosti, ki mora temeljiti na realnih grožnjah.

Realnih groženj je v mirnodobnem času relativno malo in najpogosteje izhajajo iz okolja izvajanja aktivnosti-npr. prometne in delovne nesreče, vremenske in okoljske grožnje. Nekoliko manj, a vseeno dokaj verjetno grožnjo predstavljajo razne zlorabe posameznikov znotraj sistema. Sem bi lahko uvrstili namerne poškodbe ali odtujitev materialnih ali finančnih sredstev, malomarnost, zlorabo opojnih substanc in podobno. Prikrito zbiranje informacij oziroma špijonaža s strani tujih entitet je vedno prisotna grožnja, vendar pa jo je težko zaznati. Teroristična grožnja je malo verjetna, vendar zaradi sodelovanja SV v mednarodnih vojaških operacijah in članstva RS v zvezi NATO lahko postane bolj izrazita. Grožnja s strani tujih oboroženih sil v obliki klasičnih vojaških delovanj pa je danes minimalna. Zaradi zakonskih omejitev organov J/S-2 je podatke za oceno ogrožanja potrebno pridobiti s strani Obveščevalno varnostne službe, kar terja določen čas.

Varnost je pomemben del širšega koncepta zaščite sil, ki je v NATO ena od ključnih operativnih zmogljivosti (essential operational capabililities) in je temeljno načelo vseh vojaških operacij (AJP-3.14). Zaščita sil so aktivnosti, ki se izvajajo za zmanjšanje ranljivosti moštva, opreme, objektov in delovanj pred vsemi grožnjami v vseh situacijah. Skrb za varnost moštva, ključnih sredstev in informacij je pomembna in omejuje svobodo delovanja pri doseganju cilja. Vendar ne sme po nepotrebnem voditi v izogibanje vsakemu tveganju, brez katerega ni odločne akcije (Vojaška doktrina, 2006).

V procesu načrtovanja delovanja na področju zaščite sil je po modelu AJP 3.14 ocena groženj tretji korak v načrtovanju, iz nje pa izhaja ocena ranljivosti in nato ocena tveganj. Šele po izdelani oceni tveganj pa je mogoče pristopiti k načrtovanju ukrepov za obvladovanje tveganj (AJP-3.14, poglavje 0202). Nosilec izdelave ocene groženj pa so organi J/S-2.

Varnostne zagotovitve vojaških aktivnosti torej ne moremo več obravnavati samostojno, ampak jo je potrebno vpeti v širši kontekst v okviru delovanja na področju zaščite sil. Tudi zaradi tega je izdelava ocene ogroženosti bistvenega pomena ne samo za izdelavo načrta varnostne

zagotovitve, pač pa tudi za pripravo drugih ukrepov za obvladovanje tveganj, ki ne spadajo v okvir varnostne zagotovite-npr. RKBO, zračne obrambe in podobno.

1.2 NAMEN ZAKLJUČNE NALOGE

Z nalogo želim podrobneje opredeliti grožnje, ki se pojavljajo ob izvedbi različnih vojaških aktivnosti v mirnodobnem času, opredeliti odgovornost pri načrtovanju varnostne zagotovitve in potek načrtovanja ter predlagati ukrepe za dvig učinkovitosti in poenotenje postopkov pri izvedbi varnostne zagotovitve v enotah SV.

1.3 METODE DELA

V nalogi bom na podlagi deskriptivne metode z analizo pisnih in elektronskih virov opisal in opredelil varnostno zagotovitev, kot jo določajo normativni akti SV in NATO, opredelil bom mogoče grožnje, ki se pojavljajo ob izvajanju vseh vrst delovanj SV v mirnodobnem času in na podlagi fiktivne vojaške aktivnosti izdelal vzorčni načrt varnostne zagotovitve.

Postavil sem naslednji hipotezi:

Hipoteza 1:
Za načrtovanje varnostne zagotovitve je realna in pravočasna ocena ogroženosti ključnega pomena. Iz nje izhajajo vsi potrebni ukrepi, ki morajo biti zadostni za nevtraliziranje predvidenih groženj, hkrati pa morajo omogočati gospodarno ravnanje s silami in sredstvi, ki so potrebni za njihovo kvalitetno izvedbo.

Hipoteza 2:
Za zagotovitev visoke stopnje varnosti pri vojaških aktivnostih je zelo pomembno zagotoviti varnostno usposabljanje oziroma osveščanje za vse udeležence. Potrebno jih je seznaniti s pravilnim ravnanjem ob različnih grožnjah in jih tudi opozoriti na posledice, ki jih lahko nepravilno ravnanje prinese. Brez varnostno osveščenih udeležencev je še tako natančen načrt varnostne zagotovitve neučinkovit.

1.4 STRUKTURA NALOGE

V prvem delu naloge bom opredelil posamezne pojme in povezave med njimi ter normativne dokumente, ki jih je treba upoštevati pri načrtovanju in izvajanju varnostne zagotovitve delovanja. Analiziral bom možne grožnje, ki se pojavljajo pri mirnodobnem delovanju SV doma in v tujini ter jih podrobno opisal. Poiskal bom tudi morebitne težave, ki se pojavljajo zaradi neustreznih normativnih podlag ali časovnih rokov ter predlagal rešitve.
V drugem delu naloge bom izdelal primer vzorčnega načrta varnostnega delovanja in vzorčni načrt fizičnega varovanja SV med izvajanjem različnih mirnodobnih delovanj.

2. VARNOSTNA ZAGOTOVITEV

2.1 OPREDELITEV VOJAŠKE VARNOSTNE DEJAVNOSTI

Natančna opredelitev vojaške varnosti v državah NATO izhaja iz Skupne obveščevalne, protiobveščevalne in varnostne doktrine AJP-2. Ta doktrina skupaj z AJP 2.1 in 2.2 tvori okvir za doktrinarno podlago za učenje skupnih obveščevalnih, protiobveščevalnih in varnostnih temeljev v procesu usposabljanja v zavezništvi ter za razvijanje ustreznih operativnih postopkov.

Varnostna zagotovitev je tesno povezana z protiobveščevalno dejavnostjo in je hkrati pomemben (a ne edini) del zaščite sil. AJP-2 določa, da: »Protiobveščevalno (CI) in varnostno delovanje sta dve ločeni toda povezani funkciji. Prva je aktivna in vsebuje pridobivanje varnostnih obveščevalnih podatkov in izvaja proti ukrepe skozi identifikacijo nasprotnikovih kapacitet ISTAR. Druga pa je aktivna in defenzivna ter vsebuje zaščitne varnostne ukrepe, ki so usmerjeni k zagotavljanju varnosti«. (AJP-2, poglavje 2101)

Doktrina NATO AJP-2 opredeljuje varnost kot » stanje, ki ga dosežemo, ko so določene informacije, materialna sredstva, osebje, aktivnosti, naprave in oprema zaščiteni pred vohunjenjem, sabotažo, uničenjem in pred terorizmom, kot tudi pred izgubo ali nepooblaščenim razkritjem. Varnostna zagotovitev poveljniku omogoča načrtovanje in izvajanje operacij brez vmešavanja in onemogočanja teh procesov s strani nasprotnika, hkrati pa je poveljniku zagotovljena možnost povečanja njegovih aktivnosti skozi uporabo elementov presenečenja. Varnost prispeva k celotni zaščiti sil in pomeni proces skozi katerega razmeščene enote ščitijo bojno moč«. (AJP-2, poglavje 2101)

Vse aktivnosti varnostne zagotovitve se izvajajo v okviru pojma **zaščite sil**. Zaščita sil je opredeljena kot »proces, ki ima za cilj ohraniti bojni potencial razmeščenih enot, zaščito njihove integritete in zmožnosti pred delovanjem širokega niza elementov nasprotnika ter na drugi strani nuditi zaščito pred naravnimi in okoljskimi nevarnostmi« (AJP-2, poglavje 2401, 2. odstavek). Pomemben del zaščite sil je t.i. preventivna varnost. Ta je definirana kot »organiziran sistem obrambnih ukrepov, uvedenih in zadržanih na vseh ravneh poveljevanja s ciljem, doseči in ohranjati varnost.« (AJP-2, poglavje 2404, 1. odstavek). To je varovanje vseh komponent vključno z osebjem, od neželjenih dogodkov ali od kompromitiranja. Obstajajo štiri kategorije preventivne varnosti, in sicer kadrovska, fizična, organizacijska in informacijska varnost.

AJP-2 tudi določa, da je »Izvajanje preventivnih varnostnih ukrepov, ki so predvideni v CM-49(2002) in AD 70-1 predvsem v okviru nacionalne pristojnosti. Skupine in sile, ki so razmeščene v drugih državah, izvajajo in uporabljajo varnostne ukrepe v skladu z njihovim območjem pristojnosti. Navedene sile morajo koordinirati svoje ukrepe izvajanja varnostnih ukrepov z državo gostiteljico. Varnost območja v zaledju ostaja v pristojnosti nacionalnih pristojnosti države gostiteljice. Izmenjava varnostnih obveščevalnih podatkov in koordinacija vseh dejavnikov na področju preventivne varnosti je predpogoj za doseganje ustrezne in zadostne varnosti«(AJP-2, 2404. Poglavje, 5. odstavek). Iz teh določil izhaja visoka stopnja nacionalne odgovornosti za zagotavljanje ustrezne varnostne zagotovitve tudi tedaj, ko enote delujejo v okviru zavezništva. Poudarjen je tudi pomen medsebojne koordinacije, zlasti z državo gostiteljico.

2.2 NORMATIVNA PODLAGA VARNOSTNE DEJAVNOSTI V SV

Varnostne naloge na vojaškem področju v SV v najširši obliki določa Zakon o Obrambi (ZObr) v 32. členu, kjer so določene obveščevalne in protiobveščevalne ter varnostne naloge. Drugi odstavek 32. člena varnostne naloge na vojaškem področju opredeljuje kot:

- odkrivanje, preiskovanje in preprečevanje ogrožanja varnosti določenih oseb, delovnih mest, objektov in okolišev, ki jih uporablja ministrstvo in Slovenska vojska v državi ali zunaj nje ter podatkov o razvoju ali proizvodnji določenega vojaškega orožja ali opreme;
- preiskovanje kaznivih dejanj v skladu z zakonom;
- proučevanje in predlaganje rešitev za fizično in tehnično varovanje;
- operativno varovanje določenih oseb, delovnih mest, objektov in okolišev, ki so posebnega pomena za obrambo;
- varnostno preverjanje oseb v skladu s predpisi;
- usmerjanje dela vojaške policije pri opravljanju določenih varnostnih nalog v skladu s tem zakonom.

Tretji odstavek določa, da »Obveščevalne in protiobveščevalne ter varnostne naloge na obrambnem področju opravlja obveščevalno-varnostna služba ministrstva«, vendar hkrati peti odstavek določa, da: »Ne glede na tretji odstavek tega člena štabni varnostni organi Slovenske vojske izvajajo preventivne naloge protiobveščevalne zaščite poveljstev, enot in zavodov vojske, štabno varnostne naloge ter usmerjajo in vodijo delo vojaške policije razen pri preiskovanju kaznivih dejanj v skladu s tem zakonom, ki je v pristojnosti obveščevalno varnostne službe ministrstva. Štabni varnostni organ generalštaba strokovno vodi in usmerja delovanje podrejenih štabnih varnostnih organov ter sodeluje z obveščevalno varnostno službo ministrstva.«

Iz ZObr izhaja, da štabno varnostne naloge izvajajo štabno varnostni organi SV, torej pripadniki odsekov/oddelkov J/S-2 na vseh ravneh poveljevanja. Varnostna zagotovitev vojaških aktivnosti je del štabno varnostnih nalog. Poleg tega pa je v varnostno zagotovitev vojaških aktivnosti potrebno vključiti še usmerjanje in vodenje dela vojaške policije- kar izhaja iz 32. člena, 5. odstavka ZObr.

Naslednji dokument, ki določa varnostno zagotovitev je Vojaška doktrina (2006). Ta varnost definira kot: »…načelo vojskovanja, ki narekuje izvedbo ukrepov za zagotovitev varnosti in zaščite lastnih sil. Varnostni ukrepi morajo onemogočiti sovražniku poznavanje načrtov, razporeditve, zmogljivosti in namer. Obsegajo zaščito sil in območij pred nenadnimi delovanji sovražnika in drugimi nepredvidenimi dogodki, zagotavljanje rezerve, oviranje ter odpornost sistema poveljevanja in kontrole (Vojaška doktrina, 2006: 105). Varnostno delovanje pa je definirano kot »…dejavnost Slovenske vojske, ki s pomočjo aktivnih in pasivnih ukrepov zagotavlja varnost sil tako, da onemogoča sovražniku poznavanje razporeditve, zmogljivosti in namer lastnih sil. Ukrepi so osredotočeni v tiste vsebine, ki odkrivajo ključne dejavnosti ali slabosti oziroma ščitijo bistvene podatke o lastnih silah« (Vojaška doktrina, 2006: 68).

Ob opredeljevanju varnosti pa je potrebno omeniti tudi koncept zaščite sil, saj je preventivna varnost pomemben del zaščite sil. Osnovni dokument, ki v SV opredeljuje zaščito sil je Direktiva o zaščiti sil v Slovenski vojski (GŠSV, št. 8042-223/2012-5 z dne 2.3. 2012). Ta opredeljuje šest glavnih možnih oblik zaščite sil, ki zajemajo celoten spekter dejavnosti, katere morajo izvajati vsa poveljstva, enote in posamezniki v Slovenski vojski. Te zmogljivosti so poleg preventivne

varnosti še inženirska zaščita sil, zračna obramba, zaščita zdravja, obvladovanje posledic in JRKB obramba.

Aktivnosti načrtovanja zaščite sil so sestavni del štabnega procesa dela, Direktiva pa med koraki načrtovanja zaščite sil določa tudi oceno groženj (obveščevalna analiza groženj in tveganj), ki je temelj in prvi korak za izdelavo načrta varnostnega delovanja in nato izvajanje varnostnih delovanj.

2.3 ODGOVORNOST ZA NAČRTOVANJE VARNOSTNE ZAGOTOVITVE IN ODVRAČANJE GROŽENJ

Odgovornosti na vseh nivojih določa že krovni dokument NATO, AJP-2, ki pravi, da so »poveljniki na vseh nivojih so odgovorni za izvajanje in vodenje varnostnih in protiobveščevalnih aktivnosti« (AJP 2, poglavje 2201, 1. odstavek). V drugem odstavku istega poglavja pa je določeno, da mora protiobveščevalno in varnostno osebje delovati na vseh nivojih poveljevanja. Varnostno osebje svetuje poveljniku o vseh protiobveščevalnih in varnostnih zadevah.

Po AJP- 2 (AJP-2, 2201. poglavje, 3. odstavek) so osnovni elementi odgovornosti protiobveščevalnega in varnostnega osebja na vseh nivojih poveljevanja:

a. Svetovanje poveljniku o vseh varnostnih zadevah.

b. Upravljajo proces CI in varnostnih nalog na vseh nivojih poveljevanja.

c. Obdelujejo varnostne obveščevalne podatke in jih procesirajo ter pošiljajo na ustrezne nivoje v skladu z oceno ogroženosti.

d. Vsebujejo OPSEC štabni proces vključno s planiranjem, koordinacijo in uvajanjem zaščitnih varnostnih ukrepov v enote.

e. Usmerjajo in izdajajo naloge varnostnim enotam, kjer je to potrebno.

f. Vzpostavljajo in vzdržujejo povezavo in sodelovanje s civilnimi policijskimi strukturami.

Velik poudarek je dan tudi pomenu odgovornosti za zagotavljanje varnostnih in protiobveščevalnih informacij, saj so: »protiobveščevalne in varnostne informacije so najpomembnejše za izvajanje načrtovanja pasivnih in aktivnih varnostnih ukrepov ter morajo biti v večji meri izvedene s strani odgovornih poveljnikov, njihovih obveščevalno štabnih elementov in komponent za zaščito sil« (AJP 2, 2404. poglavje, 7. odstavek).

Tudi Direktiva o zaščiti sil v Slovenski vojski opredeljuje, da so »poveljniki na vseh ravneh poveljevanja odgovorni za izvajanje ukrepov zaščite sil«. To določilo Direktive ponovno poudari poveljniško odgovornost tudi v primeru varnostne zagotovitve, saj je le ta del celotnega spektra zaščite sil.

V načrtovanje in izvajanje varnostne zagotovitve je potrebno vključiti tudi entitete, odgovorne za zaščito sil in po potrebi tudi specialiste za določena področja (npr. inženirce, RKBO, letališko varnostno osebje, vojaško policijo, gasilce, ipd.). V primeru dogodka, v katerega so vključene tudi civilne strukture in širša javnost (npr. dnevi odprtih vrat) morajo varnostni organi SV v načrtovanje vključiti tudi civilno policijo in po potrebi lokalno skupnost.

Iz zgoraj navedenih dokumentov izhaja, da za varnostno zagotovitev nosi ključno odgovornost poveljnik enote, organi J/S-2 pa dejansko v skladu z njegovimi usmeritvami in sodelovanju z drugimi organi (tu je mišljena predvsem vojaška policija in Obveščevalno varnostna služba) načrtujejo in vodijo izvedbo varnostne zagotovitve.

2.4 OPREDELITEV VIROV OGROŽANJA

Kot vire ogrožanja publikacija AJP-2 v 2. odstavku 2104. poglavja navaja naslednje kategorije:

a. Tuje obveščevalne službe (FIS).

b. Subverzivne organizacije, skupine ali posamezniki.

c. Teroristične organizacije, skupine ali posamezniki.

d. Specialisti (nasprotnikovi), enote kot so na primer specialne sile (SF).

e. Izvidovanje in nadzorovanje iz zraka morja in kopnega s sredstvi za slikovno zbiranje podatkov in zbiranje s pomočjo sredstev zvez, vključno satelite.

f. Kriminalne organizacije in skupine.

g. Posamezniki z nejasno določenimi nameni.

Vsi omenjeni viri ogrožanja (z izjemo nasprotnikovih specialnih sil) so v večji ali manjši meri prisotni tudi v mirnodobnem okolju. V trenutni situaciji pa so verjetno najbolj nevarni posamezniki z nejasno določenimi nameni. V to kategorijo bi lahko uvrstili širok spekter posameznikov, tako civiliste kot posamezne pripadnike SV ali uslužbence MORS. Njihovi motivi in nameni so različni in segajo od želje po pridobitvi materialnih koristi do želje po maščevanju zaradi resničnih ali namišljenih krivic. Ker se v svojih dejanjih praviloma ne povezujejo z drugimi osebami jih je zelo težko odkriti, zlasti v primeru ko gre za poskuse nezakonitega pridobivanja materialne koristi. Nekoliko lažje je odkriti posameznike, ki jim je motiv maščevanje, saj praviloma ljudje svoje nezadovoljstvo zelo glasno izražajo. Takšni posamezniki so v obeh primerih zelo dojemljivi za novačenje s strani tujih obveščevalnih služb, subverzivnih in terorističnih organizacij in ne nazadnje s strani organiziranega kriminala.

Tuje obveščevalne službe poleg z zgoraj opisanimi motivi pridobivajo sodelavce še s pomočjo izsiljevanja in ideološke ali nacionalne bližine posameznika s sovražno obveščevalno službo. Obseg delovanja tujih obveščevalnih služb je težko določiti, saj delujejo prikrito in je že samo delovanje skoraj neopazno. Kljub temu ne gre dvomiti, da tuje obveščevalne službe delujejo tudi v Sloveniji in med drugim zbirajo tudi podatke o SV.

Teroristične organizacije niso izrazit vir ogrožanja RS in SV, saj naj na območju RS ne bi delovale. Bolj izrazite so v času opravljanje nalog v tujini-tako mednarodnih vojaških operacij kot tudi med različnimi vojaškimi vajami v državah, kjer je terorizem bolj izrazita grožnja.

Tudi izvidovanje z sredstvi za slikovno zbiranje podatkov in spremljanje sredstev zvez je stalno prisotno. To velja zlasti za spremljanje sredstev zvez, kar je z ustrezno opremo dokaj lahko izvajati tudi iz ozemlja sosednjih držav. Ta grožnja postane še bolj izrazita med izvajanjem nalog

(tudi mirnodobnih, kot so recimo vojaške vaje) v tujini. Teh aktivnosti ne moremo preprečiti, lahko pa z ustreznimi ukrepi (disciplina pri uporabi sredstev zvez, uporaba tablic signalov, izogibanje uporabi mobilnih telefonov v službene namene, uporaba žičnih zvez…) v veliki meri zmanjšamo učinke tovrstnega zbiranja podatkov.

Pomemben, čeprav ne toliko izrazit vir ogrožanja SV so tudi kriminalne organizacije, zlasti tiste, ki se ukvarjajo z preprodajo orožja. Vojska je zanje vir najučinkovitejšega orožja, za katerega so njihovi odjemalci pripravljeni veliko plačati. V tem primeru so najbolj ogrožena skladišča oborožitve na bolj osamljenih krajih. Z ukrepi tehničnega varovanja je mogoče zmanjšati nevarnost vdora, ključna za uspešno varovanje tovrstnih objektov pa je budnost moštva varovanja.

2.5 OPREDELITEV GROŽENJ

AJP-2 dokaj podrobno opredeljuje splošne vrste groženj. Vrste groženj razdeli na direktne (pridobivanje informacij, špijonaža, sabotaže, ofenzivne informacijske operacije oziroma INFO OPS) in posredne (pridobivanje informacij, subverzije, sabotaže, terorizem in organizirani kriminal). Neposredne grožnje so tiste, ki prihajajo od nasprotnika, medtem ko so posredne grožnje tiste aktivnosti, ki jih potencialni nasprotnik podpira v miru in vojni z namenom izboljšati svojo operativno pripravljenost in ekonomske zmožnosti. Te grožnje oziroma aktivnosti torej ne prihajajo neposredno od nasprotnika, ampak od entitet, ki jih ta prikrito ali neprikrito podpira.
V četrtem odseku publikacije je navedena okvirna opredelitev različnih vrst groženj. Treba pa je poudariti, da AJP-2 ne omenja groženj, ki so sicer v mirnodobnem času najbolj pogoste in realne in lahko potencialno povzročijo veliko materialne škode in tudi človeške žrtve. Sem bi lahko uvrstili prometne in delovne nesreče, katerim pogosto botruje malomarnost in nedisciplina izvajalcev vojaških aktivnosti . V nadaljevanju bom na kratko opisal različne vrste groženj.

2.5.1 ŠPIJONAŽA

Špijonaža je lahko opredeljena kot prikrita metoda uporabljena s strani sovražne obveščevalne službe, ki zbira informacije povezane z nacionalno varnostjo, katere jim niso znane. Sem spada tudi pridobivanje podatkov iz javnih oziroma odprtih virov, saj »vsakodnevno opazovanje in zbiranje informacij z odprtimi metodami s strani posameznikov ali organizacij, predstavlja stalno in pomembno grožnjo varnosti« (AJP-2, poglavje 2105). Sovražne obveščevalne službe pa bodo pridobivale predvsem tajne informacije in tiste, ki niso tako lahko dostopne. Pri tem bodo skušali za sodelovanje pridobiti osebe, ki imajo možen dostop do tajnih informacij oziroma drugega pomembnega materiala ali pa ga bodo v bodočnosti šele pridobile. Osebe, ki so lahko cilj delovanja sovražnih obveščevalnih služb so lahko tudi operaterji IT sistemov in programersko osebje. Obveščevalne službe pridobivajo sodelavce s pomočjo denarja in materialnih ugodnosti, izsiljevanja (zaradi spolnih afer, kriminalne dejavnosti ali drugih pomanjkljivosti izsiljevanega posameznika), osebnega maščevanja za resnične ali namišljene krivice ter ideološke ali nacionalne bližine posameznika s sovražno obveščevalno službo. Pomembno sredstvo špijonaže so tudi moderne naprave za prisluškovanje, snemanje in fotografiranje. Te so danes lahko dostopne tudi posameznikom, saj se prodajajo preko spletnih trgovin. Špijonaža je sicer zelo tvegano dejanje in se uporabi le tedaj, ko ključnih podatkov ni mogoče pridobiti na drug način. Usmerjena bo v pridobivanje pomembnih podatkov na strateškem in operativnem nivoju. Na nižjem taktičnem nivoju pa so zaradi uporabe informacijskih omrežij ogrožene zlasti baze podatkov.

Posebno veliko nevarnost predstavlja odtekanje podatkov preko informacijskih omrežij, ki je lahko namerno (npr. zaradi nezadovoljstva posameznik določene podatke zaupne narave objavi

na internetnih straneh ali socialnih omrežjih) ali pa nenamerno (neprevidna in malomarna uporaba USB ključkov za prenos podatkov, pošiljanje dokumentov zaupne narave preko običajne elektronske pošte, ipd.). Za zmanjšanje tveganja odtoka informacij je potrebno dosledno upoštevati predpise, ki določajo varovanje tajnih podatkov, vendar le ti pogosto otežujejo ali v primeru pomanjkljive opreme celo onemogočajo delo s tajnimi podatki, zato je skušnjava po ubiranju bližnjic zelo velika, s tem pa se povečuje tudi tveganje.

2.5.2 SABOTAŽE

Sabotaže se izvajajo večinoma v času krizne situacije in vojne. Širok in koordiniran spekter sabotažnih aktivnosti je potrebno pričakovati takoj po začetku sovražnosti in sicer, ko imajo taka dejanja največji negativni učinek (AJP-2, poglavje 2106). Sabotaže lahko z relativno skromnimi in improviziranimi sredstvi dosežejo velik učinek, če je cilj sabotaže premišljeno izbran. Posebej nevarne pa so, če jih izvedejo posamezniki znotraj SV, ki dobro poznajo določen objekt in rutino znotraj in lahko natančno predvidijo učinke sabotaže. Zato je posebej pomembno pravočasno odkriti posameznike, ki bi lahko zaradi različnih razlogov takšno dejanje izvedli.

2.5.3 SUBVERZIJE

Subverzija je dejanje, ki želi oslabiti vojaško, ekonomsko in politično moč države s spodkopavanjem morale, lojalnosti ali zanesljivosti njenih državljanov. Takšen napad na lojalnost državljanov je lahko zelo razdiralen in ga je zelo težko odkriti ter se mu zoperstaviti (AJP-2, poglavje 2107).

»Subverzivne organizacije izvajajo ilegalne in neustavne metode s ciljem doseči zamenjavo vlade v njihovo korist. Posamezniki so tudi lahko prevratniki in sicer tako, da se njihova lojalnost spremeni tako, da postanejo primerni za uporabo s strani tujih obveščevalnih služb ali subverzivnih organizacij. Danes obstaja veliko tehnik subverzivnega delovanja in modernih metod komunikacije, kot so na primer tiskani mediji, radio in televizija, ki subverzivnim organizacijam, skupinam in posameznikom omogočajo, da preko njih dosežejo veliko množico poslušalstva« (AJP-2, poglavje 2107, 2. odstavek).

Pri metodah komunikacije velja posebej izpostaviti internet in v sklopu tega predvsem socialna omrežja, kot sta Twitter, Facebook. Znano je, da so nedavne revolucije v arabskih državah bile sprožene ravno preko socialnih omrežij. V Sloveniji pa je bilo in je še na različnih spletnih forumih in komentarjih k internetnim člankom opaziti pozive posameznikov k demonstracijam, a očitno zaenkrat brez učinka.

AJP 2 v poglavju 2107 navaja, da metode subverzivnega delovanja omenjenih organizacij lahko vključujejo:

a. Propagando, agitacijo, demonstracije, ulične nemire ter širjenje letakov in brošur s sporno vsebino.

b. Uporaba prikritih organizacij za zakritje njihovih pravih aktivnosti.

c. Novačenje privržencev, ki zavedno ali nezavedno delujejo v njihovo korist.

d. Vzpostavljanje splošnega vzdušja, ki vodi v nezaupanje in diskreditacijo vodij in posameznikov.

e. Razširjanje lažnih govoric ali prikrajanje resničnosti s ciljem porušitve zaupanja v voditelje ali zaveznike.

Subverija je najbolj razširjena aktivnost in ponavljajoča se grožnja varnosti v obdobju miru. V času povečanja krizne situacije se bo tudi aktivnost subverzivnega delovanja močno povečala. Subverzija se ne pojavlja samo v okviru opisanih oblik delovanja temveč se v nekaterih državah pojavlja tudi v obliki dobro načrtovanih pohodov ali demonstracij, v določenih javnih medijih in drugih medijskih produktih, ki so lahko subverzivne narave. Lahko rečemo, da Republika Slovenija in s tem tudi Slovenska Vojska lahko v času današnje vsesplošne krize postane cilj (v kolikor že ni) različnih subverzivnih delovanj iz tujine in domačega okolja.

Aktivnosti subverzivnih organizacij in posameznikov lahko vplivajo tudi na posamezne pripadnike SV, ki bi lahko bili tako bolj dovzetni za izvedbo različnih dejanj-sabotaž, špijonaže, širjenja propagande, ipd.

2.5.4 TERORIZEM

AJP 2 terorizem definira kot »Nezakonita uporaba ali grožnja uporabe sile ali nasilja proti posameznikom ali lastnini s ciljem prisile ali zastraševanja vlade ali službe za doseganje političnih, verskih ali ideoloških ciljev.« (AJP-2, poglavje 2108) Čeprav je terorizem v svojem učinku in bistvu del subverzivnega delovanja je postal tako razširjen, da se ga smatra kot samostojno in zelo veliko grožnjo.

Izvajanje terorizma lahko vključuje uporabo naslednjih metod:

a. Vznemirjenje in grožnje.

b. Propagando.

c. Krajo denarja, orožja in druge opreme.

d. Oboroženi napadi, bombne eksplozije in pohabljanje.

e. Atentate in ugrabitve.

Danes je terorizem ena glavnih groženj oboroženim silam držav zveze NATO, zlasti na mednarodnih vojaških operacijah. V domačem okolju trenutno grožnja s strani terorizma ni visoka, vendar se moramo zavedati, da je kljub temu stalno prisotna.

2.5.5 CYBER TERORIZEM

Je posebna oblika terorizma, ki je usmerjena na delovanje v informacijskih omrežjih. Praviloma se šteje kot posebna grožnja, saj so sredstva za izvedbo napada bistveno drugačna kot pri klasičnem terorizmu, posledice pa so lahko ravno tako hude ali pa še hujše. Definira se ga lahko kot zloraba računalniškega sistema tarče napada z namenom povzročanja fizične škode ali resno onemogočanje oziroma motenje delovanja različne infrastrukture. Vdor v računalniški sistem nek organizacije ali državnega organa lahko povzroči kaos v prometu, prekinjeno oskrbo prebivalstva z vodo in električno energijo, težave v plačilnem prometu in delovanju bank in podobno. Najpogostejša posledica tovrstnih napadov pa je kompromitiranje ali celo izguba podatkov ali tajnih podatkov, ki se nahajajo na v omrežje povezanih računalnikih in podatkovnih diskih. Storilce je težko odkriti še preden izvedejo svoje dejanje, saj jim ni potrebno pred

napadom organizirati nabave orožja in razstreliva-kar varnostno obveščevalne službe in policija pogosto pravočasno odkrijejo. Glavno orožje cyber terorizma so različni računalniški virusi, ki jih v sistem vnesejo preko interneta ali s pomočjo notranjih sodelavcev, ki imajo dostop do internega omrežja. Motivi izvajalcev so zelo različni in segajo od zgolj radovednosti in užitka do materialnih koristi in političnih motivov. Najpogostejši so sicer napadi v obliki t.i. Web site defancing, kjer storilci spremenijo vsebino in obliko spletnih strani tarče napada, pogosta oblika napada pa je tudi Denial-of-service (DoS). Ta lahko povzroči več škode, gre pa zato da se internetni strežnik tarče zasuje z zunanjimi zahtevami za povezavo, kar povzroči preobremenitev in posledično izpad sistema. DoS je bil uporabljen v cyber napadih na Estonska omrežja v letu 2007, ki so povzročili izpad informacijskega sistema dveh glavnih bank in skoraj vseh vladnih internetnih strani.
Zaradi tovrstnih groženj so ukrepi na področju informacijske varnosti ali (INFOSEC) zelo pomembni. Prvo zaščito predstavlja že fizična ločenost internega informacijskega omrežja (intraneta) od interneta, tveganje pa zmanjšujejo še različni organizacijski ukrepi, npr prepoved vnosa lastne informacijske opreme na delovno mesto. Izvajanje ukrepov pa je potrebno redno nadzirati.

2.5.6 ORGANIZIRAN KRIMINAL

AJP-2 definira organiziran kriminal kot »dejavnost organizacij kriminalnega značaja, ki so organizirani kot mreža z enim ali več voditelji in večimi podrejenimi skupinami, razširjenimi po večjem delu teritorija. Cilj organiziranega kriminala je nelegalno pridobivanje moči preko vplivov in denarja, neupoštevajoč demokratične zakone, ki veljajo v državi v kateri organizirani kriminal deluje. Kriminalne združbe izvajajo podobne aktivnosti, ki so opisane v predhodnih poglavjih ter poleg tega lahko izvajajo tihotapljenje blaga, ilegalnih drog in človeškega blaga z namenom, da se ogrozi nacionalna in vojaška varnost v državi« (AJP-2, poglavje 2109).

Organiziran kriminal predstavlja grožnjo SV zlasti v obliki odtujitve ali poskusov odtujitve vojaške opreme, orožja, streliva in minsko-eksplozivnih sredstev (v nadaljevanju MES) z namenom preprodaje na črnem trgu ali pa uporabe v dejavnostih organiziranega kriminala. Organiziran kriminal je lahko tudi vir oskrbe terorističnih organizacij z orožjem in MES, zato je v tem primeru še posebno nevaren. Kriminalne združbe lahko tudi pridobijo posameznike znotraj SV za pomoč pri izvedbi kaznivih dejanj, ki bi bila uperjena zoper premoženje MORS in SV.

Ob tem ne smemo pozabiti tudi na kriminalna dejanja posameznikov, ki niso povezana z organiziranim kriminalom. Znan je pregovor, da priložnost dela tatu in v primeru, ko za varnost sredstev ni dovolj poskrbljeno lahko pride do tatvin ali drugih oškodovanj premoženja SV, ki ga povzročijo posamezni pripadniki SV ali redkeje osebe izven sistema MORS in SV. Tovrstna, neorganizirana oblika kriminala je tudi pogostejša.

2.5.7 NESREČE

Delovne in prometne nesreče so najbolj splošna in hkrati najpogostejša grožnja vojaškemu delovanju v mirnodobnem času. Do njih prihaja zaradi različnih materialnih in človeških vzrokov, pri tem pa je pri človeških vzrokih posebej potrebno izpostaviti malomarno opravljanje dolžnosti, oziroma nedisciplino, pri materialnih pa iztrošenje in zastarevanje sredstev. Vse vzroke je sicer mogoče z ustreznim usposabljanjem, nadzorom in pravilnim ravnanjem s sredstvi mogoče zmanjšati, v popolnosti odpraviti pa jih ni mogoče. Zato je potrebno imeti pripravljene postopkovnike oziroma SOP, kjer so opredeljeni ukrepi, ki jih je potrebno v primeru nesreč izvesti z namenom zmanjšanja in odprave posledic nesreče.

3. NAČRT VARNOSTNE ZAGOTOVITVE

3.1 OCENA OGROŽENOSTI

Izdelava ocene ogroženosti je temelj za načrtovanje varnostne zagotovitve. Brez ocene groženj ni mogoče izdelati realnega in uporabnega načrta varnostne zagotovitve. Pri izdelavi ocene moramo biti pozorni, da upoštevamo vse grožnje in jih tudi ovrednotimo in razdelimo na verjetne in manj verjetne. Vsekakor pa je pri izdelavi ocene potrebno izhajati iz realnih groženj.

AJP-2 v poglavju 2308 določa, da je »razvoj ocenjevanja groženj prvi korak, ki mora biti izveden za zoperstavljanje grožnjam in je pomemben zato, ker vsi ostali varnostni mehanizmi izhajajo iz tega. Zaradi tega mora vsaka država, vsaka CI služba in vsak nivo poveljevanja izdelati ustrezno oceno groženj, ki pa jo mora stalno dopolnjevati in obnavljati v okviru novih spoznanj in sprememb, ki se dogajajo v operativni situaciji«.

Preden se lotimo izdelave ocene ogroženosti je potrebno pridobiti oceno ogroženosti s strani OVS, ki razpolaga z podatki o širši varnostni ogroženosti. Ta ocena potem predstavlja temelj, na osnovi katere izdelamo lastno oceno.

Ocena grožnje naj bi vsebovala (Grbec; 2011):

- Proučevanje moči, zmožnosti, metod in morebitnih namenov vseh organizacij, skupin, posameznikov in drugih možnih groženj;
- Grožnje in ranljivosti pomembnih ciljev, ter iz teh izhajajočo oceno tveganja uresničitve grožnje ciljem;
- Definiranje ciljev, ki bi bili lahko najbolj verjetna tarča napadov.

V nekaterih primerih za izdelavo ocene ogroženosti nimamo dovolj časa na razpolago. V tem primeru je potrebno izdelavo ocene skrajšati, vendar mora še vedno vsebovati vse bistvene elemente, vendar osredotočene na zgolj najpomembnejše podrobnosti. V tem primeru je oceno smiselno izdelati v obliki ppt. predstavitve in jo po potrebi lahko uporabimo tudi za pripravo udeležencev dogodka.

Najbolj pregledno se izdela opis po naslednjih točkah (Grbec; 2011):

1. Situacija
V tej točki na kratko opišemo objekt SV (vojašnico, tabor, skladišče, orožarno) in dogodek – aktivnost (sestanek, seminar, vajo, usposabljanje). S pridobljenimi podatki lažje določimo pomembnosti ciljev in njihovo ranljivost. Če imamo na razpolago premalo časa za izdelavo popolne ocene groženj, opis situacije osredotočimo predvsem na dogodek, za katerega oceno izdelujemo in iz njega potegnemo cilje in njihovo ranljivost.

2. Grožnje
V tej točki je potrebno proučiti moč, zmožnosti, metode in morebitne namene vseh organizacij, skupin, posameznikov kot tudi možne grožnje našim entitetam. Grožnje okvalificiramo kot zelo verjetne, verjetne in manj verjetne. Morajo biti realne in vpete na področje, ki ga smiselno zahteva pomembni cilj - entiteta. Potrebno je opisati tudi manj verjetne, a še vedno realne grožnje. V primeru skrajšane ocene pa se osredotočimo zgolj na najverjetnejše grožnje.

3. Ocena tveganja
V tej točki opisanim pomembnim ciljem - entitetam določimo najbolj verjetne grožnje in ocenimo njihovo verjetnost kot zelo verjetno, verjetno in manj verjetno. Če za izdelavo popolne ocene nimamo časa, opišemo le ključne cilje in jim določimo najbolj verjetne grožnje.

4. Ukrepi
Ukrepe načrtujemo po kategorijah preventivne varnosti (kadrovska, fizična, organizacijska, INFOSEC). Za vsako kategorijo načrtujemo specifične ukrepe, prilagojene glede na situacijo in grožnjo.

Med ukrepe na področju kadrovske varnosti spadajo med drugim: skrben izbor kadra za občutljiva delovna mesta, izdaja dovoljenj za dostop do tajnih podatkov na osnovi potreb po vedenju (need to know), dosledno izvajanje določil Pravilnika o varovanju tajnih podatkov v MORS, kjer je določeno sprotno obveščanje o spremembah v vprašalniku iz 25. člena Zakona o tajnih podatkih, redno izvajanje pregleda zanesljivosti oseb, dobro in pravilno upravljanje s kadri, itd.

Ukrepi na področju fizične varnosti so: učinkovita uporaba straže in reakcijskih sil ter strukturnih in tehničnih ukrepov (npr. fizične ovire, ključavnice…) ki preprečujejo vdore v varovana območja, preprečevanje nepooblaščenega snemanja ali slikanja (npr. obvezna oddaja naprav, ki omogočajo slikovno in akustično snemanje-to so predvsem mobilni telefoni). Ukrepe fizične varnosti je potrebno dopolniti z drugimi ukrepi, ki lahko v čim krajšem času odkrijejo poskus nepooblaščenega dostopa. Sem bi lahko uvrstili sisteme tehničnega varovanja, kot so elektronska kontrola dostopa, videonadzor in različni alarmni sistemi.

Organizacijski varnostni ukrepi temeljijo na vzpostavljenih procedurah, ki so določene v dokumentih zveze NATO (npr. AJP-2, AD-70-1) in v nacionalni zakonodaji (ZTP in iz njega izhajajoči podzakonski akti in predpisi). Na nivoju taktičnih enot SV pa praktično izvedbo opredeljujejo različni akti poveljevanja (npr. ukazi in standardni operativni postopki). Sem spada določitev varnostnih območij različnih stopenj, njihova vzpostavitev, varovanje in nadzor nad vstopi, izdelava načrtov varovanja, izvajanje nadzorov, inšpekcij in različnih preverjanj varnostnih območij, ustrezno določanje stopenj tajnosti dokumentom ob izdelavi, ustrezne priprave za uničevanje tajnih dokumentov, izvajanje varnostnih usposabljanj in osveščanj v različnih oblikah, različni varnostni postopki na letališčih za zagotavljanje varnostnih območij za vojaška letala.

Ukrepi na področju INFOSEC so zelo pomembni, saj lahko do izgube zaupnih informacij najhitreje pride ravno zaradi neustreznega ravnanja z dokumenti v elektronski obliki. Zato je potrebno dosledno izvajati naslednje ukrepe: sistemi za računalniško obdelavo podatkov morajo vedno delovati in biti shranjeni v ustreznih varnostnih območjih določenih stopenj tajnosti z omejenim dostopom v omenjena območja; dostop v sistem mora biti dovoljen samo osebju, ki je ustrezno preverjeno na najvišje stopnje tajnosti glede na informacije in podatke, ki se obdelujejo ali procesirajo v sistemu; dostop do medijev (CD-ROM, diski itd.) pri sistemu za računalniško obdelavo podatkov mora biti omejen in strogo nadzorovan; oprema za računalniško obdelavo podatkov, ki ima ustrezno TEMPEST zaščito mora biti uporabljena vedno kadar kapacitete, ki so na razpolago, ne zadostujejo ustreznim kriterijem in standardom, še posebej če je sistem nameščen na terenu; Obvezno je potrebno redno spreminjati gesla za dostop v sistem; vojaško omrežje ne sme biti priklopljeno na javno omrežje, kot je internet, razen, če so na razpolago ustrezni tehnični sistemi, ki preprečijo nepooblaščene dostope v sistem. Temeljni varnostni

ukrep pa je dosledno izvajanje varnostnih usposabljanj in osveščanj za zaposlene, s katerimi se jih seznani s pravilnim ravnanjem in samozaščitnimi ukrepi pri delu z informacijskimi sistemi.

V primeru izdelave skrajšane ocene načrtujemo specifične ukrepe, prilagojene glede na situacijo in grožnjo zgolj za kategorije varnosti, ki so ob določenem dogodku najbolj relevantne. Ukrepe pa moramo ne glede na skrajšan čas podrobno načrtovati.

5. Ostala navodila za preprečevanje groženj
V tej točki podamo dodatne usmeritve, pojasnila, navodila in ukrepe ki ne spadajo v ostale kategorije varnostnih ukrepov. Če izdelujemo skrajšano oceno je v nasprotju z ostalimi točkami ta lahko širša kot v primeru izdelave popolne ocene, saj v njej podamo dodatna pojasnila.

Izdelana ocena groženj mora imeti tudi ustrezno stopnjo tajnosti. Za vojaške mirnodobne aktivnosti praviloma zadostuje stopnja tajnosti do INTERNO. Ko smo grožnje pravilno ocenili, lahko pristopimo k načrtovanju varnostne zagotovitve za ustrezen dogodek. Oceno ogroženosti priložimo kot dodatek k prilogi O/D/1, torej načrtu varnostne zagotovitve.

3.2 PRIMER OCENE OGROŽENOSTI

V nadaljevanju podajam vzorec ocene ogroženosti za dogodek, ki se v vojašnicah SV redno izvaja, in sicer dan odprtih vrat. Namenjen je predstavitvi SV širši javnosti, med udeleženci pa se lahko znajdejo tudi pripadniki tujih obveščevalnih služb, terorističnih organizacij in kriminalci. Kontrole dostopa v tem primeru ni, oziroma je omejena, zato je potrebno varovanje dogodka še toliko bolj skrbno načrtovati.

Ob tovrstnih dogodkih se poveča verjetnost odtujitve premoženja SV, zlasti na stojnicah, kjer se javnosti predstavlja oborožitev in oprema SV. Naval obiskovalcev je pogosto zelo velik, zato mora biti osebje, ki opremo predstavlja zelo pozorno, sicer lahko hitro izgine kak manjši kos opreme, v skrajnem primeru pa celo orožje ali radijske postaje. Tako ima lahko izguba denimo radijske postaje, ki je programirana za kriptiran način govora zelo resne posledice, ki presegajo zgolj materialno vrednost same postaje. Tatvine pa niso omejene samo na lastnino MORS in SV, ampak je potencialno ogrožena tudi lastnina obiskovalcev. Če se med množico obiskovalcev znajde kak žepar in uspešno opravi svoje delo, SV neposredno materialno ne bo oškodovana, trpel pa bo ugled vojske, ki ni uspela preprečiti oškodovanja obiskovalcev.

Drug realna grožnja na tovrstnih prireditvah so prestopki zoper javni red in mir. Te lahko povzročijo obiskovalci ali celo pripadniki SV pod vplivom alkohola, ki se ob dogodku toči tudi v vojašnicah. Manj verjetna, a nikakor neobstoječa pa je možnost zlorabe dneva odprtih vrat za izvedbo demonstracij ali drugačnih manifestacij, ki bi bile v prvi vrsti usmerjene zoper SV. Takšne manifestacije bi lahko izvedli posamezniki ali civilno družbene organizacije, ki nasprotujejo vojski. Pri tem je lahko povzročena tudi materialna škoda, v prvi vrsti pa bo prizadet ugled SV.

Ne nazadnje pa je potrebno omeniti še grožnjo špijonaže. Med obiskovalce se lahko pomešajo tudi sodelavci tujih obveščevalnih služb, ki jim prireditev tako omogoči iz prve roke videti določen objekt, oborožitev in opremo. Z navidez nedolžnimi vprašanji lahko od sodelujočih izvlečejo določene informacije in ocenjujejo usposobljenost in opremljenost enote. Zato je potrebno že v oceni groženj določiti območja, kamor obiskovalci ne vstopajo, sodelujoče pa varnostno pripraviti na dogodek. Pripadniki morajo zlasti vedeti, kaj je vojaška skrivnost in kaj ni.

Dodatek 1 k prilogi O/D/1
k Ukazu za organizacijo dneva odprtih vrat v vojašnici Zelena Gora

OCENA OGROŽENOSTI DNEVA ODPRTIH VRAT V VOJAŠNICI ZELENA GORA

S ciljem zmanjšanja možnosti uresničitve grožnje zoper sodelujoče pri dnevu odprtih vrat v počastitev dneva Slovenske vojske podajamo oceno ogroženosti, ki sledi v nadaljevanju. Izdelana je po terminologiji izdelave ocene ogroženosti, ki jo zahteva sprejeti AJP 2.2. Namen izdelave ocene ogroženosti je:

- Detekcija in zmanjšanje ogrožanj pripadnikov SV, pripadnikov tujih vojska, MORS, civilnih oseb in drugih materialnih sredstev (v nadaljevanju entitet), ki v aktivnostih sodelujejo;
- Zagotovitev kvalitetne izdelave načrta varnostnega delovanja pri varovanju entitet med samimi aktivnostmi;
- Izvajanje določil iz AJP 2.2 in drugih aktov, ki določajo naloge štabno varnostnega organa.

1. SITUACIJA

Dne 9. 5. 2012 je v vojašnici Zelena Gora načrtovan dan odprtih vrat v počastitev Dneva Slovenske vojske. Na aktivnosti bodo sodelovali visoki častniki SV, povabljeni gostje, pripadniki SV in civilno prebivalstvo.

Aktivnost bo v celoti potekala v vojašnici Zelena Gora (v nadaljevanju VZG).

Najbolj izpostavljeni objekti v VZG:

1. Pot od vhoda v vojašnico do parkirišča za obiskovalce (za objektom E)
2. Razstavna mesta oborožitve in opreme ter okrepčevalnica (pred objektom A)
3. Orožarne v objektu B,
4. Stavba poveljstva, vključno z VO II. Stopnje (objekt A)
5. Avtopark, skladišča (objekti C, D, E)
6. Nastanitveni objekt (objekt B).

Vzroki povečane ranljivosti navedenih objektov:
1. površno in nedosledno izvajanja varnostnih ukrepov in malomaren odnos do varovanih oseb in stvari od strani nekaterih posameznikov,
2. možnost vstopa civilistov z kriminalnimi nameni,
3. povečan promet ob vhodu v vojašnico,
4. možnost zlorabe alkohola s strani obiskovalcev.

Skladno z nalogami iz direktive za delovanje organa S-2 podajamo naslednjo oceno ogroženosti Dneva odprtih vrat.

2. GROŽNJE

Slovenija je nizko ogrožena s strani terorizma. To pomeni, da teroristični napadi niso verjetni, so pa možni. Nikoli jih namreč ne moremo izključiti.

Realne grožnje

Kot realne grožnje so možne tatvine predmetov, dokumentov s strani posameznikov ali kriminalnih združb, kršitve zoper javni red in mir ter grožnje pojava nesreč v cestnem prometu.

Grožnja pojava nesreč v cestnem prometu je verjetna predvsem pri premiku na določene lokacije v smislu materialne škode.

1. *Prometne nezgode* so mogoče predvsem v naselju Zelena Gora in samem križišču za vojašnico ter na označeni dovozni poti do osrednjega parkirišča.

Predlagani varnostni ukrepi:
- Obveščena lokalna Policija o aktivnosti,
- Znotraj vojašnice prisotnost patrulj VP, ki usmerjajo promet,
- Obveščanje, reševanje.

2. *Grožnje tatvine* predmetov, dokumentov, denarnic, mobitelov, fotoaparatov, nakita s strani posameznikov je verjetna na prireditvenem prostoru.
Predlagani varnostni ukrepi:
- Patruljiranje VP po prireditvenem prostoru.
- Vzdrževanje zveze z civilno policijo.

3. *Vdor tujih obveščevalnih služb* za pridobivanje podatkov s fotografijo in spraševanjem posameznikov (HUMINT), verjetnost je srednja.
Predlagani varnostni ukrepi:
- Z varnostnimi in protiobveščevalnimi pripravami ter osveščanjem pripadnikov SV se lahko zmanjša učinkovitost tujih obveščevalnih služb, ne more pa se tveganje zmanjšati.
- Opazovanje in takojšnje obveščanje organov S-2 o sumljivih posameznikih in dogodkih.
- Dosledno izvajati prepoved vstopa obiskovalcev v objekte v vojašnici, ki niso predmet dneva odprtih vrat.

4. *Prestopki zoper javni red in mir* s strani posameznih obiskovalcev.
Predlagani varnostni ukrepi:
- Patruljiranje VP po prireditvenem prostoru.
- Vzdrževanje zveze z civilno policijo.

Manj verjetne grožnje

3. *Ugrabitev* posameznikov, skupine, izsiljevanje.
Predlagani varnostni ukrepi:
- Znotraj vojašnice prisotnost patrulj VP in S-2,
- Obveščanje po liniji PINK in funkcijski liniji.

4. *Bombni napad (IED)*, na določenih lokacijah kjer je množica ljudi, ob cesti (manj verjetno).
Predlagani varnostni ukrepi:

- Prisotnost patrulj VP in S-2 znotraj vojašnice.
- Pravočasno obveščanje in evakuacija oseb iz ogroženega območja.
- Pravočasno obveščanje po liniji PINK in funkcijski liniji.

3. OCENA TVEGANJA

J-2 PSSV nas je obvestil, da jih je J-2 GŠSV je z dopisom Ocena ogroženosti – dan odprtih vrat v vojašnicah SV, št. 850-6/2012-43, z dne 5. 5. 2012, obvestil, da OVS trenutno ne razpolaga z informacijami ali podatki, ki bi predstavljali varnostno grožnjo izvedbe načrtovanih dogodkov.

Ocenjujemo, da je ocena tveganja uresničitve navedenih groženj zoper entitete med potekom dneva odprtih vrat, po sprejetju opisanih varnostnih ukrepov sprejemljiva.

V primeru pojava večjih sprememb groženj pa so poleg spodaj zahtevanih, potrebni še dodatni ukrepi.

4. UKREPI

a. Ukrepi na področju kadrovske varnosti (organizatorji in izvajalci nalog)

- Izbor kadra za občutljiva delovna mesta (ocena var. tveganja 35. člen ZOBr);
- Dovoljenje za dostop do tajnih podatkov (po ZTP-UPB2) za izbrano osebje, ki bo imelo dostop do tajnih informacij na podlagi potrebe po vedenju »need to know«;
- Stalno izvajanje določb Pravilnika o varovanju tajnih podatkov v MORS, ki določajo, da se vse spremembe iz vprašalnika sproti sporočajo. Cilj tega je ugotoviti razloge za morebitno zmanjšanje zanesljivosti osebe, ki ima dostop do tajnih podatkov;
- V okviru splošnega nadzora konstantno izvajanje pregleda zanesljivosti oseb, ki imajo dostop do tajnih podatkov (strokovnost – ocena pripadnika je tudi pomembna, prisotnost alkohola, prisotnost drog…);
- Dober sistem upravljanja s kadri (motivacija, kariera, napredovanje, nagrajevanje), nadzora in izobraževanja;

b. Ukrepi na področju fizične varnosti

- Varovanje pripadnikov ob dnevu odprtih vrat s strani VP in S-2 med aktivnostmi;
- Varovanje mora obsegati ustrezno število mož na varovanju in stalni nadzor nad izvajanjem varnostnih ukrepov,
- Vzpostavitev stalne mobilne zveze z objektom in nadzornim centrom in javljanje stanja;
- Obveščanje in reševanje v primeru pomembnega varnostnega pojava;

c. Organizacijski varnostni ukrepi

- Izdelava načrta varnostne zagotovitve, ki zajema varovanje, izredne dogodke in postopke ob njih;
- Varnostna priprava izvajalcev na dnevu odprtih vrat.

d. Ukrepi na področju INFOSEC

Z namenom preprečitve nepooblaščenega dostopa do digitalnih informacij, moramo upoštevati naslednje ukrepe:

- Med dnevom odprtih vrat so računalniki po pisarnah izključeni;

- Gosti (svojci) ne vstopajo v pisarne in objekte, ki niso predmet dneva odprtih vrat.

5. OSTALA NAVODILA ZA PREPREČEVANJE GROŽENJ

Vsi sodelujoči pri organizaciji in izvedbi varnostnega delovanja morajo sodelovati s protiobveščevalnim in varnostnim organom in ostalimi pripadniki. Pri sodelovanju se zahteva od njih in tudi sprejema njihove nasvete.
Izvajanje stalnih varnostnih nadzorov in pregledov se izvaja po liniji PINK.

Oceno izdelal: STOT. xxxx, S-2

3.3 NAČRT VARNOSTNE ZAGOTOVITVE

Z izdelavo ustrezne ocene ogroženosti smo identificirali glavne grožnje in določili ukrepe, s katerimi se bomo tem grožnjam zoperstavili. Sledi izdelava načrta, v katerem bomo opredelili naloge udeležencem in časovne roke za izvedbo nalog in ukrepov, ki so del varnostne zagotovitve. Načrt je najbolje izdelati v tabelarni obliki, kot je bila predpisana v Metodologiji načrtovanja izobraževanja in usposabljanja (GŠSV, 2001) kot priloga O/D/1. Kljub temu, da je omenjen dokument zdaj že preklican, je format načrta še vedno uporaben. Kot prilogo poleg ocene ogroženosti dodamo različne skice ali karte, ki natančno opredelijo lokacije ukrepov ali potek dogodkov. Načrt mora čim bolj jasno opredeliti naloge posameznim entitetam v procesu varnostne zagotovitve in določiti časovne roke za njihovo izvedbo. Sestavljen je iz štirih delov, ki opredeljujejo aktivnosti, ukrepe, izvedbo in izvedbene roke v času priprav, v času premika , v času izvajanja aktivnosti in v času po končani aktivnosti.

V nadaljevanju podajam vzorčni načrt varnostne zagotovitve za izvedbo vojaške vaje z bojnim streljanjem v tujini. Varnostna zagotovitev vojaške vaje v tujini je kompleksnejša, saj zahteva tudi sodelovanje z varnostnimi organi države gostiteljice. Zato je potrebno dati poseben poudarek na varovanje občutljivih informacij, ne glede na to da gre za prijateljsko ali celo zavezniško državo.

Za izdelavo kvalitetnega načrta varnostne zagotovitve pa seveda potrebujemo tudi oceno ogroženosti. Ker se dogodek izvaja v tujini, je pravočasna pridobitev ocene Obveščevalno varnostne službe ključna, saj OVS razpolaga z natančnejšimi in analitično obdelanimi informacijami o stanju in virih ogrožanja v državi gostiteljici (naloge po 32. členu, 1. odstavek ZObr) kot jih lahko pridobimo sami iz javno dostopnih (odprtih) virov.

Za odtekanje informacij so v tujini zlasti občutljiva sredstva zvez. Na varnostnih pripravah za dogodek je potrebno udeležence natančno seznaniti z pastmi pri komuniciranju in še posebej odsvetovati, oziroma prepovedati uporabo mobilnih telefonov za komuniciranje o službenih zadevah in opozoriti na previdnost pri pošiljanju elektronske pošte v javnem internetnem omrežju.

Zelo pomembno je tudi načrtovanje varnostnih ukrepov ob premiku na prizorišče vaje, zlasti če je le to daleč od Republike Slovenije in je pri tem potrebno prečkati več držav. Premik po cestah na velike razdalje lahko pomeni velik izziv tako za voznike (utrujenost, drugačna vozniška kultura) kot tudi za tehniko (okvare, do katerih pride zlasti na starejših in iztrošenih vozilih). Pri morebitnih nesrečah bo potrebno sodelovanje z organi tranzitne države ali države gostiteljice, pri čemer lahko zelo hitro pride do nenamernega odtekanja podatkov.

Grožnjo na vojaški vaji v tujini lahko predstavlja tudi lokalna flora in favna, predvsem strupene rastline, kače, žuželke ali večji plenilci, ki v domačem okolju ne bivajo. Zato je v tem primeru potrebno načrtovati tudi določene varnostne ukrepe, denimo prepoved odlaganja kuhinjskih odpadkov v bližini tabora, izogibanje območjem, kjer bi se lahko nahajale nevarne živali, ipd., predvsem pa je pomembno na pripravah sodelujoče seznaniti z nevarnostmi in osnovnim samozaščitnim ravnanjem.

Ena od osnov za uspešno izvajanje načrta varnostne zagotovitve je izvedba obveščevalne, varnostne in protiobveščevalne priprave vseh udeležencev aktivnosti, ki mora biti dovolj natančna, a hkrati čim krajša in jedrnata. Pri predolgi pripravi udeleženci pozabijo pomembne podrobnosti, prekratka ali nenatančna pa ne more vsebovati vse potrebne snovi in je zgolj sama sebi namen.

Priloga O/D/1

k ukazu za izvedbo TVBS » KAČA 2012«

NAČRT VARNOSTNE, OBVEŠČEVALNE IN PROTIOBVEŠČEVALNE ZAGOTOVITVE

zap. št.	NALOGE		IZVEDBA		ROK	Nadzor nad izvedbo	Opomba
	AKTIVNOSTI	VARNOSTNI UKREPI	Odgovorni za izvedbo	Sodeluje			
1	2	3	4	5	6	7	8
I. V ČASU PRIPRAV							
1.	Načrtovanje vaje.	• Izdelava načrta varnostne in protiobveščevalne zaščite. • Usposabljanje oz. obveščevalna in varnostna priprava sodelujočih. • Pridobiti protiobveščevalno in varnostno oceno ogroženosti vaje • Priprava vadbenih dokumentov po obveščevalnih zadevah.	S-2 OVS	PE	po org. ukazu	S-2	
2.	Varovanje zaupnih podatkov.	• S podatki zaupne narave postopati v skladu z določili ZTP in ostalimi podzakonskimi akti, ki opredeljujejo postopke z zaupnimi podatki.	Poveljstva in enote		stalna naloga	S-2	
3.	Izbira PM, rajonov izvajanja aktivnosti in mest namestitve	• Preučevanje varnostnih razmer. • Ocena tveganja zaradi naravnih dejavnikov (podnebje, flora, favna…) v kraju aktivnosti. • Ocena ekoloških tveganj v kraju aktivnosti. • Ocena prometnih razmer na širšem območju vaje.	J/S-2	PE	do konca vaje	S-2	
4.	Prenos zaupnih podatkov.	• Zaščita zaupnih podatkov, ki se prenašajo po brezžičnih zvezah.	J/S-6	PE	stalna naloga	S-2	

		• Prepoved uporabe mobilnih telefonov za posredovanje občutljivih podatkov.					
5.	Zaznava dogodkov in negativnih pojavov.	• Analiza dogodkov in negativnih pojavov, seznanitev sodelujočih z ugotovitvami, ter načrtovanje ukrepov.	vsi	PE	do konca vaje	S-2	
6.	Sodelovanje z zunanjimi organizacijami.	• Vzpostavitev sodelovanja s civilno in vojaško policijo Republike Mirzije na območju izvajanja aktivnosti. • Vzpostaviti sodelovanje z lokalnimi oblastmi • Vzpostavitev sodelovanja z OVS.	S-2 S-5	S-2, VP	do konca vaje	S-2 in 5	vsakdo na svojem območju pristojnosti
7.	Sodelovanje z lokalnimi skupnostmi.	• Obveščanje lokalnih skupnosti. (po potrebi) v sodelovanju z mirzijskimi lokalnimi in vojaškimi oblastmi.	S-5	Pooblaščeni organ	do konca vaje	Poveljnik	
8.	Protiobveščevalna zaščita priprav.	• Obveščevalna in varnostna priprava sodelujočih. • Obveščanje strokovnih organov o zanimanju s strani nepooblaščenih oseb. • Javnost seznanjati le s podatki, ki niso zaupne narave. • Upoštevanje zaščitnih ukrepov pri komuniciranju preko sredstev zvez.	S-2 Pomočnik SJ	Vsi	do konca vaje	S-2	
9.	Obveščevalno – varnostna priprava	• Seznanitev vseh sodelujočih z obveščevalno - varnostnimi razmerami in okoljskimi tveganji na področju izvajanja vaje	S-2	S-2 PE	do konca vaje	S-2	
10.	Priprava MTS, m/v, bojnih vozil, oborožitve, streliva in MES.	• Preverjanje brezhibnosti MTS, m/v, bojnih vozil in artificij. • Izločitev MTS, m/v, bojnih vozil, oborožitve, streliva in MES, ki ni v brezhibnem stanju.	S-4	PE	do konca vaje	S-4	
11.	Obveščanje javnosti	• Javnost seznaniti le s podatki, ki niso zaupne narave.	Pomočnik SJ	PSSV	Po prilogi O/X/2	Vodstvo vaje	
II. V ČASU PREMIKA							
1.	Premiki enot na območje vaje.	• Dosledno upoštevanje predpisov o letalskem prometu. • Dosledno upoštevanje Pravilnika o udeležbi vojaških vozil v javnem cestnem prometu. • Upoštevanje navodil VP. • Upoštevati CPP držav po katerih se izvaja premika.	PE	S-4, VP, častnik za varnost letenja	V času trajanja premikov na vajo in iz vaje	S-4, častnik za varnost letenja	

		• Dosledno upoštevati navodila, ki so izdelana za prevoz pripadnikov in materiala po železnici (varovanje materiala, sklanjanje preko oken, gibanje po vlaku, upoštevanje voznega reda,…).					
2.	Postanki v času premika	• Dosledno izvajati varovanje moštva, MTS in vozil v času postankov. • Zaklepanje vozil. • O protiobveščevalno in varnostno zanimivih pojavih poročati po liniji PINK.	PE	S-4, VP	V času trajanja premikov na vajo in iz vaje		
3.	Ukrepi ob morebitnih prometnih nesrečah	• Prva pomoč prizadetim. • Zavarovanje kraja dogodka. • Sodelovanje z VP gostujoče države. • Sodelovanje s pristojnimi letalskimi preiskovalnimi organi.	PE	S-4, VP, častnik za varnost letenja		S-4, častnik za varnost letenja	
III. V ČASU IZVAJANJA AKTIVNOSTI							
1.	Premiki enot.	• Dosledno upoštevanje predpisov o letalskem prometu. • Dosledno upoštevanje Pravilnika o udeležbi vojaških vozil v javnem cestnem prometu. • Upoštevanje navodil VP. • Upoštevati veljavne CPP Republike Mirzije.	PE	S-4, VP, častnik za varnost letenja	do konca vaje	S-4	
2.	Varovanje poveljstev in rajonov razmestitve enot.	• Varovanje PM in rajonov razmestitve enot izvajati v skladu z oceno ogroženosti. • Varovanje zračnih plovil na letališču Skobčev Grob izvajati v skladu z oceno ogroženosti.	PE	enote	do konca vaje	vodstvo vaje in poveljstva	
3.	Zagotovitev varnosti sodelujočih in ostalih.	• Dosledno upoštevanje predpisov o varnosti letenja. • Seznanitev sodelujočih z omejitvami in dosledno upoštevanje omejitev. • Bojna sredstva, MES in strelivo uporabljati ob doslednem upoštevanju predpisov. • Omejitev gibanja nepooblaščenih na območja izvajanja aktivnosti. • O protiobveščevalno in varnostno zanimivih pojavih poročati po liniji PINK.	PE	VP		S-2	
4.	Zagotovitev varnosti oborožitve in streliva.	• Organizirati varovanje oborožitve, MES in streliva v skladu s predpisi. • Organiziranje iskanja v slučaju izgube.	PE	Vsi		Poveljniki	

		• Obveščanje po liniji poveljevanja.					
5.	Prenos zaupnih podatkov.	• Prenos podatkov po zaščitenih zvezah. • Zaščita zaupnih podatkov, ki se prenašajo po brezžičnih zvezah. • Prepoved uporabe mobilnih telefonov za posredovanje občutljivih podatkov.	S-6	Vsi		S-2	
6.	Hranjenje zaupnih podatkov	• Udeležence vaje opomniti na pomen varovanja in pravilnega ravnanja s TP. • Zagotoviti hranjenje in varovanje TP na območju vaje v skladu s predpisi.	PE	Vsi	do konca vaje	S-2	
7.	Obiski varovanih oseb	• Izdelava načrtov varovanja.	PSSV	S-2, VP	29SEP12	S-2	VIP day
8.	Nastanek dogodkov in izrednih dogodkov.	• Obveščanje po liniji poveljevanja. • Ukrepanje v skladu s pristojnostmi. • Sodelovanje s pristojnimi organi (VP, OVS).	PE	S-2, VP	po potrebi	S-2 in S-3	
9.	Ukrepi ob morebitnih nesrečah	• Prva pomoč prizadetim. • Zavarovanje kraja dogodka. • Sodelovanje z VP in preiskovalnimi organi Republike Mirzije. • Sodelovanje s pristojnimi letalskimi preiskovalnimi organi. • Obveščanje po liniji PINK in strokovni liniji.	PE	S-4, VP, častnik za varnost letenja		S-4, častnik za varnost letenja	
IV. PO KONČANI AKTIVNOSTI							
1.	Urejanje opreme.	• Pregled in preverjanje stanja. • Ugotavljanje morebitnih manjkov. • Organiziranje iskanja.	PE VP		do konca vaje	Poveljniki	
2.	Premiki enot na matične lokacije	• Dosledno upoštevanje predpisov o letalskem prometu. • Dosledno upoštevanje Pravilnika o udeležbi vojaških vozil v javnem cestnem prometu. • Upoštevanje navodil VP. • Upoštevati CPP držav po katerih se izvaja premik. • Dosledno upoštevati navodila, ki so izdelana za prevoz pripadnikov in materiala po železnici (varovanje materiala, sklanjanje preko oken, gibanje po vlaku, upoštevanje voznega reda,…)	PE	S-4, VP	Po ukazu za premik	S-4	
3.	Analiza vaje	• Zaščita zaupnih podatkov.	vsi		stalna	S-2	

					naloga		
4.	Zaznava dogodkov in negativnih pojavov.	• Analiza dogodkov in negativnih pojavov, seznanitev sodelujočih z ugotovitvami, ter načrtovanje ukrepov.	S-2	PE, OVS		S-2	

Načrt izdelal: STOT xxxx , S-2

5. NAČRT FIZIČNEGA VAROVANJA

Načrt fizičnega varovanja je najbolje izdelati kot grafični dodatek k prilogi O/D/1. V njem del varnostnih ukrepov, ki smo jih predvideli v načrtu varnostne zagotovitve tudi konkretno umestimo v čas in prostor. Gre za karto, na katero vrišemo položaje stražarskih mest, smeri delovanja patrulj, objekte, ki jih je potrebno posebej varovati, kritična območja in po potrebi tudi časovnico, denimo čas izvajanja patrulj, čas odpiranja vhodov, menjave straž, ipd.

Najlažje in najpregledneje se izdela v programu Powerpoint, ki omogoča tudi poljubno kombiniranje fotografij, skic in načrtov ter nudi orodja za vrisovanje različnih simbolov. Načrt v elektronski obliki je mogoče tudi natisniti in razdeliti osebam, ki ga potrebujejo. Izdelava načrta na klasični način zahteva več časa, ne omogoča toliko različnih kombinacij, razmnožuje pa se lahko s fotokopiranjem. Fotokopiran material pa je pogosto slabše vizualne kakovosti in so zato podrobnosti manj razvidne.

V prilogi 1 podajam vzorčni načrt fizičnega varovanja.

6. ZAKLJUČEK

Načrtovanje varnostne zagotovitve je kompleksen proces, katerega nosilec so sicer organi J/S-2, vendar je potrebno pri tem zagotoviti sodelovanje vseh relevantnih faktorjev, tako specialistov na posameznih področjih kot tudi vojaške policije, Obveščevalno varnostne službe ministrstva, pogosto pa tudi civilne policije in ostalih civilnih inštitucij.

Načrt varnostne zagotovitve nam omogoča smotrno in učinkovito izrabo razpoložljivih virov pri izvajanju varnostne zagotovitve vseh delovanj in sprejemanje ustreznih ukrepov, ki so prilagojeni obstoječim realnim grožnjam. Temelj za uspešno načrtovanje pa je izdelana ocena ogrožanja, v katerem na osnovi razpoložljivih informacij ocenimo vrste groženj in vire ogrožanja, ki bi lahko prizadele naše sile, ocenimo tveganje in določimo varnostne ukrepe, ki bodo zmanjšali stopnjo tveganja. Brez realno ocenjene grožnje bodo tudi ukrepi nerealni in s tem neučinkoviti proti realni grožnji. Nobenega smisla nima podrobno načrtovati ukrepov za npr. malo verjetno grožnjo terorističnega napada, ob tem pa zanemariti ukrepe za varnost v prometu z vojaškimi vozili ali za varovanje premoženja SV pred odtujitvijo.

Poudarek mora biti dan ukrepom, ki se zoperstavljajo grožnjam, ki jih ocena ogroženosti podaja kot najbolj verjetne, oziroma realne. Realna ocena ogroženosti oziroma ocena tveganja uresničitve grožnje ciljem, ki je njen del nam omogoči tudi učinkovito načrtovanje izrabe razpoložljivih človeških in materialnih virov pri izvedbi varnostne zagotovitve. Tako npr. ne bomo uporabili večjega dela razpoložljivega moštva za varovanje praznega skladišča, ob tem pa zanemarili varovanje sredstev, ki se nahajajo na prostem znotraj vojaškega objekta.

Na osnovi izkušenj in preučevane literature lahko tako potrdim svojo hipotezo, ki pravi, da je za načrtovanje varnostne zagotovitve realna in pravočasna ocena ogroženosti ključnega pomena. Iz nje izhajajo vsi potrebni ukrepi, ki morajo biti zadostni za nevtraliziranje predvidenih groženj, hkrati pa morajo omogočati gospodarno ravnanje s silami in sredstvi, ki so potrebni za njihovo kvalitetno izvedbo.

Še tako dobro pripravljen načrt varnostne zagotovitve pa je brez pomena, če udeleženci v aktivnosti niso seznanjeni z osnovnimi in izhajajočimi varnostnimi ukrepi. Čeprav smo recimo realno ocenili, da obstaja velika verjetnost prisluškovanja našim sredstvom zvez in nato natančno opredelili varnostne ukrepe pri komuniciranju s sredstvi zvez (npr. uporaba tablice signalov, frekvenčnega skakanja, ipd.), ob tem pa pozabili udeležence opozoriti tudi na disciplino pri uporabi osebnih mobilnih telefonov in prepovedati razgovore o službenih zadevah po mobilnih omrežjih, bo imel naš načrt veliko luknjo, skozi katero bodo informacije uhajale. Še tako nepomemben podatek, ki ga obdela izkušen obveščevalni analitik in ga postavi na svoje mesto lahko tvori del ključnega podatka o lastnih silah. Zato je osveščenost in samozaščitno ravnanje pripadnikov SV izredno pomembno, zagotovi pa ga lahko le redno izvajanje varnostnih osveščanj in usposabljanj ter ustrezen nadzor nad njihovim ravnanjem.

Tudi drugo hipotezo, ki pravi, da je za zagotovitev visoke stopnje varnosti pri vojaških aktivnostih zelo pomembno zagotoviti varnostno usposabljanje oziroma osveščanje za vse udeležence lahko potrdim. Udeležence je potrebno seznaniti s pravilnim ravnanjem ob različnih grožnjah in jih tudi opozoriti na posledice, ki jih lahko nepravilno ravnanje prinese. Le tako se bo naš načrt varnostne zagotovitve začel izvajati že na osnovni ravni in bo lahko v končni fazi učinkovit, seveda če bodo tudi druge predpostavke in ukrepi v načrtu uresničeni. Če pa bo naš načrt padel že pri samozaščitnem ravnanju udeležencev, bodo tudi ostali ukrepi v veliki meri zaman.

Pri načrtovanju varnostne zagotovitve pa je nekaj nedorečenosti. Sam format ocene ogroženosti izhaja iz dokumenta NATO AJP-2.2 in ni predpisan z ukazom ali drugim aktom poveljevanja v SV. Tudi obrazec za izdelavo načrt varnostne oskrbljenosti izhaja iz Metodologije načrtovanja izobraževanja in usposabljanja, torej dokumenta ki je zastarel (iz leta 2001) in je že tudi preklican. Zato predlagam, da se načrtovanje varnostne oskrbljenosti predpiše s posebnim aktom poveljevanja, najbolje z SOP, ki bi vseboval tudi potreben format za izdelavo načrta varnostne zagotovitve skupaj z dodatki.

Sklenem lahko, da je za načrtovanje učinkovite varnostne zagotovitve potrebno najprej ugotoviti realne grožnje našemu delovanju, nato pa se teh groženj tudi zavedati in zavedanje o njih vcepiti vsem udeležencem aktivnosti, ki bodo naloge in ukrepe iz načrta varovanja tudi izvršili. Brez izpolnitve teh dveh pogojev bo varnostna zagotovitev ostala zgolj priloga k ukazu in nič več.

VIRI IN LITERATURA:

Zakon o obrambi (Ur. l. RS št. 103/04 – UPB-1),

SVS STANAG 2190(1), AJP 2.0. Skupna obveščevalna, protiobveščevalna in varnostna doktrina, 6. 1. 2005,

Allied Joint Doctrine for Force Protection AJP-3.14, 26 November 2007

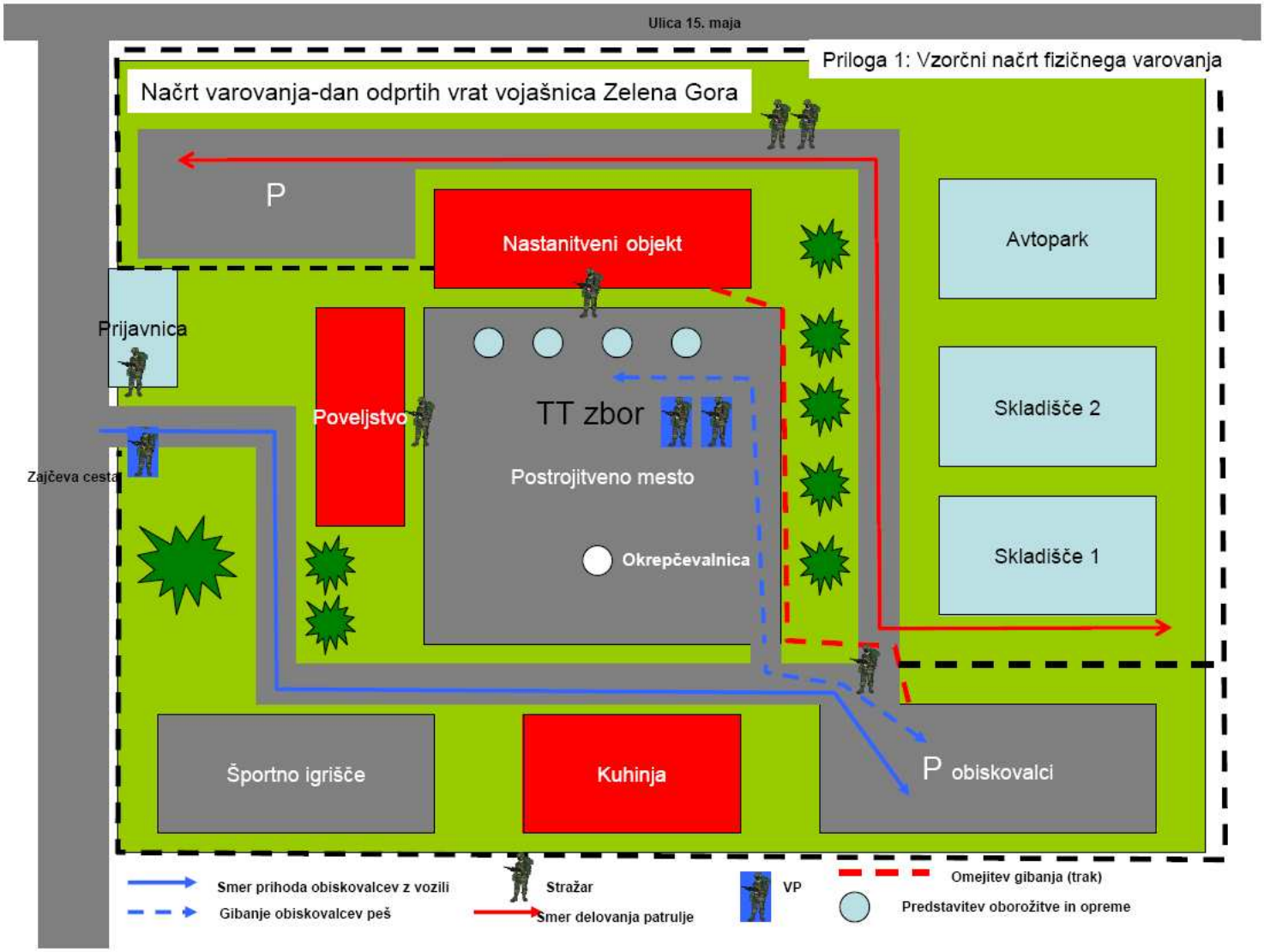
VOJAŠKA DOKTRINA, Poveljstvo za doktrino, razvoj, izobraževanje in usposabljanje, Ljubljana 2006

D I R E K T I V A O ZAŠČITI SIL V SLOVENSKI VOJSKI, GŠSV, št. 8042-223/2012-5 z dne 2.3.2012

Metodologija načrtovanja izobraževanja in usposabljanja, (GŠSV, številka: 811-02-1/01-10 z dne 4. 12. 2001)

Različni internetni viri.

PRILOGE
PRILOGA 1: NAČRT FIZIČNEGA VAROVANJA



IZJAVA O AVTORSTVU ZAKLJUČNE NALOGE

Kandidat (ka) / Slušatelj stotnik Rok Ravnak izjavljam, da sem avtor/ica zaključne naloge z naslovom Varnostna zagotovitev vojaških aktivnosti in načrtovanje varnostne zagotovitve , ki sem jo napisal/a pod mentorstvom majorja Jožeta Grbca .

S svojim podpisom zagotavljam da:

- je zaključna naloga izključno rezultat mojega lastnega dela,
- so vsa dela in mnenja drugih avtorjev, ki jih uporabljam v zaključni nalogi, navedena oziroma citirana v skladu s SOP ŠČ za izdelavo in oblikovanje zaključne naloge na ŠČ,
- se zavedam, da je plagiatorstvo kaznivo po Zakon-u o avtorskih in sorodnih pravicah, (uradno prečiščeno besedilo – ZASP UPB3, Uradni list RS, št. 16/2007, z dne 23. 2. 2007), prekršek pa podleže tudi ukrepom disciplinske odgovornosti v skladu z Zakonom o obrambi in Pravili službe v Slovenski vojski,
- se zavedam posledic, ki jih dokazano plagiatorstvo lahko predstavlja za predloženo zaključno nalogo in moj status v Slovenski vojski.

S podpisom se odrekam vsem materialnim pravicam v zvezi z zaključno nalogo in dovoljujem uporabo zaključne naloge v študijske namene.

V Mariboru, dne 25.5.2012 Podpis: _____