ŠOLA ZA ČASTNIKE
IZREDNA GENERACIJA JANUAR 2012
SPECIALIZACIJA OBVEŠČEVALEC

ZAKLJUČNA NALOGA

POMEN OCENJEVANJA GROŽENJ PRI IZVAJANJU PROTIOBVEŠČEVALNE IN VARNOSTNE DEJAVNOSTI V SV

Kandidat-slušatelj: stotnik Branko Poklič

Mentor: major Jože Grbec

Novo mesto, april 2012

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO
SLOVENSKA VOJSKA
POVELJSTVO ZA DOKTRINO, RAZVOJ, IZOBRAŽEVANJE IN USPOSABLJANJE
Šola za častnike

Engelsova ulica 15, 2111 Maribor

Številka:
Datum:

ZAKLJUČNA NALOGA

POMEN OCENJEVANJA GROŽENJ PRI IZVAJANJU PROTIOBVEŠČEVALNE IN VARNOSTNE DEJAVNOSTI V SV,

Kandidat-slušatelj: stotnik Branko Poklič

Mentor: major Jože Grbec

Novo mesto, april 2012

Povzetek

Informacija in podatek imata težo le, če sta pravilna in pravočasna. Le pravilna in pravočasna informacija bo lahko tudi obveščevalni podatek s težo, ki bo pripomogel k pravilni oceni situacije in s tem k pravilnim in pravočasnim preventivnim, pa tudi kurativnim ukrepom.

V tej nalogi bom obravnaval delo protiobveščevalnih in varnostnih organov SV glede na oceno ogroženosti. Skušal bom dokazati, da njihovo delo in ukrepi niso odvisni le od ocene ogroženosti, ampak je le-ta le pomoč v nihovem delu. Prav tako bom skušal dokazati trditev, da delo protiobveščevalnih in varnostnih organov SV vpliva tudi v obratni smeri. Podatki, ki jih zberejo protiobveščevalni in varnostni organi SV pri svojem delu v enotah na podlagi informacij in izkušenj ter dogodkov v praksi, morajo biti pomemben vir v izdelavi ocene ogroženosti!

Teza 1: Ocena ogroženosti ima velik vpliv na delo protiobveščevalnih in varnostnih organov SV. Vendar protiobveščevalni in varnostni organi v SV pri varnostni zagotovitvi kot osnovo ne uporabljajo le ocene ogroženosti ampak je potrebno le-to nadgraditi še z izkušnjami, trenutno situacijo, vrsto aktivnosti in strukturo ter številom udeleženih pri aktivnosti.

Teza 2: Tok obveščevalnih podatkov poteka tudi iz nižjih taktičnih ravni do obveščevalnih struktur na strateški ravni v MORS in so sestavni del pri izdelavi ocene ogroženosti.

Summary

The Information and the Data have the important weight only if they are correct and timely. Only correct and timely information will also be an Intelligence Data with the Importance, which will lead to the correct assessment of the situation and with that it will lead to the proper and timely preventive and curative measures.

This study will discuss the work of Slovenian Army Counterintelligence and Security Authority according to risk assessment. I will try to demonstrate that the work and actions of Counterintelligence and Security Authority are not only depending on the threat assessment, but that the threat assessment is also in support in their work. I will also try to demonstrate that the work of Slovenian Army Counterintelligence and Security Authority also have an affection the other way around. The Data collected by the Counterintelligence and Security Authority of Slovenian Army in their work in units, on the basis of information, experiences and events in practice, must be an important source in the production of threat assessments.

Ključne besede

Protiobveščevalni in varnostni organi SV, ocena ogroženosti, varnost, grožnja, zaščita sil, varnostna zagotovitev, obveščevalni podatek.

KAZALO

1 UVOD

Zaznava groženj in njihova narava vplivata na občutek ogroženosti organizacije (v našem primeru Slovenske vojske) ter posledično določata način, na katerega se jim bo organizacija zoperstavila. Vse bolj pomembno je, da so se sodobne vojske sposobne odzivati novim varnostnim izzivom, grožnjam in tveganjem tako na strateški ravni kot tudi na operativni in taktični ravni. Obenem so zaradi neprestanega povečevanja števila sodobnih varnostnih tveganj in groženj v nezavidljivem položaju, kajti z naraščanjem števila groženj in tveganj se povečuje tudi kompleksnost njihovih sestav in postopkov, kar vojskam in enotam še dodatno zapleta iskanje mehanizmov za njihovo omejevanje, nadzorovanje in odpravljanje. Poleg tega je zaradi pojava novih ali spremembe starih groženj varnosti potrebno (nekatere) varnostne postopke na novo opredeliti ali celo na novo definirati ter poiskati najbolj ustrezne in primerne rešitve za soočanje z njimi.
Dejstvo je, da nobena grožnja ne nastane brez povoda in tudi na vsako grožnjo se mora opraviti neka aktivnost za nevtraliziranje oz. zmanjšanje tveganja povezanega z grožnjo. Z vzpostavitvijo ukrepov proti grožnji pa se v primeru resne grožnje sorazmerno z ukrepi grožnja poveča ali spremeni. Torej lahko govorimo o nekem tokokrogu aktivnosti »akcija-reakcija«. Naloga obveščevalnih, protiobveščevalnih in varnostnih organov, pa tudi ostalih pripadnikov SV pa je predvsem biti z ukrepi vsaj en korak pred grožnjo in varnostnimi tveganji.

1.1 UPORABLJENE METODE

V okviru dela nameravam uporabiti naslednje metode:

1. analizo in interpretacijo primarnih virov (dokumentov, pravilnikov, poročil, resolucij, strategij),
2. analizo in interpretacijo sekundarnih virov bom uporabil za izpolnitev vrzeli in predstavitev dejanske in možne ureditve sistema varnosti na področju soočanja z grožnjami varnosti in stabilnosti ter znotraj tega procesa ocenjevanja ogrožanja varnosti v SV,
3. primerjalno raziskovanje,
4. metodo kompilacije, s katero povzemam stališča strokovnjakov do obravnavane strokovne tematike,
5. ankete, vprašalnike, javnomnenjske raziskave in analize (iz uradnih statistik).

1.2 OPREDELITEV TEMELJNIH POJMOV

1.2.1 Varnost

Pri ocenjevanju varnostnih razmer v sodobni družbi je osnovno vprašanje, kaj je varnost in kaj so varnostne razmere. Če hočemo pravilno opredeliti pojem varnosti, se moramo najprej vprašati za varnost koga ali česa, kjer nastane potreba po opredelitvi subjektov (npr. človek, država, družbene skupine, mednarodna skupnost…) ali objektov (varnost različnih vrst zasebne ali družbene lastnine, varnost intelektualne lastnine), na katere se varnost nanaša. Zatem sledi opredelitev, za kakšno vrsto varnosti gre, ali gre za varnost (obstoja, razvoja) subjekta ali objekta na splošno, ali pa gre za varnost pred specifičnimi vrstami ogrožanj. Postavlja se tudi vprašanje, ali je varnost objektivna ali subjektivna kategorija.

Pod pojmom varnost razumemo celo vrsto različnih vidikov človeškega obstoja in delovanja v družbi in naravi. Opredelimo jo lahko kot stanje, v katerem je zagotovljen uravnotežen fizični, duhovni in duševni ter gmotni obstoj posameznika in družbene skupnosti v razmerju do drugih posameznikov, družbenih skupnosti in narave. (Grizold, 1999: 23). Varnost je imanentna prvina družbe, ki zajema stanje oz. lastnost stanja in dejavnost oz. sistem. Varnost se nanaša tako na družbo kot tudi na državo. Je torej človekovo zavestno prizadevanje za vzpostavitev takšne civilizacijske in kulturne kategorije, ki bo zajemalo vse vidike varnosti: politične, gospodarske, pravne, znanstvene, socialne, kulturne in številne druge. To so torej tiste pojavne oblike družbenega življenja, ki jih ni mogoče uvrstiti v kategorijo družbenih vrednot in označujejo okvir politične in socialne skupnosti. Hkrati pa omogočajo obstoj družbene reprodukcije, notranji red in mir, razvoj notranje ureditve ter zagotovitev običajnih procesov diferenciacije in integracije znotraj družbe in države (Anžič, 2002: 455).

V AJP 2 je **preventivna varnost** je definirana kot » Organiziran sistem obrambnih ukrepov, uvedenih in zadržanih na vseh ravneh poveljevanja s ciljem, doseči in ohranjati varnost.« To je varovanje vseh komponent vključno z osebjem, od neželjenih dogodkov ali od kompromitiranja.

Obstajajo štiri kategorije preventivne varnosti, ki se nanaša na:

- Osebno varnost.
- Fizično varnost.
- Organizirane varnostne ukrepe.
- INFOSEC/ADP varnostne ukrepe.

1.2.2 Ogrožanje varnosti

Ogrožanje pomeni izpostavljanje škodi ali nevarnosti, lahko pa ga opredelimo tudi kot okoliščino, ki je notranja ali zunanja nekemu sistemu, proizvodu, opremi ali operaciji in ki lahko v primeru svojega aktiviranja povzroča veliko škodo in smrt. Posledica ogrožanja varnosti je obstoj ogroženosti, ki je resnična ali občutena izpostavljenost ljudi, živali, premoženja, kulturne dediščine in okolja nevarnostim naravnih in drugih nesreč (Zakon o varstvu pred naravnimi in drugimi nesrečami, Ur. l. RS, št. 64/94). V teoriji govorimo o stvarni ogroženosti, tj. o vojaško političnih razmerah v okolju skupnosti, pogostosti in moči naravnih ali drugih nesreč, ekološki izpostavljenosti itd. in o zaznavni ogroženosti, ki jo pripadniki

skupnosti subjektivno zaznavajo in se odraža v javnem mnenju (Malešič, 2005: 553). (Prezelj, 2006: 31, 32). V tem smislu je tudi Ullmanova (1983: 133)razmišljala o grožnjah varnosti, ki jih je opredelila kot tiste dogodke ali sekvence dogodkov, ki grozijo, da bodo v kratkem času drastično znižali kakovost življenja prebivalcev države ali da bodo drastično zožali izbiro možnih političnih reakcij, ki so na voljo državi in zasebnim nevladnim subjektom (posameznikom, skupinam, korporacijam) znotraj države. Arnejčič (1999: 14) pravi, da je grožnja varnosti usmerjena (direktna) sposobnost potencialnega nasprotnika ali pa drugih subjektov za krizne razmere ali vojno. Časovna in prostorska dimenzija sta pomembnejši kot pri tveganju. Varnostna grožnja predstavlja kratek časovni rok, v katerem lahko pride do dejavnosti nasprotnika.

1.2.3 Grožnja

Opaziti je tudi, da pogosto pride do enačenja ali celo zamenjevanja pojmov grožnja in tveganje. Zelo negativni varnostni pojavi so enkrat poimenovani kot grožnje (»threats«), drugič kot tveganja (»risks«), tretjič kot izzivi (»challenges«), četrtič kot nevarnosti (»insecurities«), včasih pa celo kot priložnosti (»oppurtunities«). Konsenz glede uporabe teh terminov ne obstaja, prav tako tudi ni zaslediti njihovih definicij. Posledica je tudi njihova nekonsistentna in neprecizna uporaba.

Grožnje največkrat izvajajo (AJP 2.1:11):

a. Tuje obveščevalne službe (FIS).
b. Subverzivne organizacije, skupine ali posamezniki.
c. Teroristične organizacije, skupine ali posamezniki.
d. Specialisti (nasprotnikovi), enote kot so naprimer 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.

Slika 1: Model nastanka grožnje

Vir: http://www.crn.ethz.ch/_docs/Bohkari.ppt#14, (12. 12. 2006).

Varnostni interesi sodobnih družb se vse bolj selijo na področje nevojaških groženj, na soočanje z naravnimi katastrofami, ekološkimi grožnjami. Hkrati pa so tudi vojaške grožnje vse bolj nedržavne narave, se pravi, da tudi vse manj politične narave. To pomeni, da je varnostni interes še vedno povezan z obstojem vojaške sile, toda teroristične grožnje in vodenje novih vojn zahtevajo nove varnostne mehanizme (Jelušič, 2002: 618).

Susan Strange (2005) meni, »da so se pojavile t.i. transdržavne grožnje, ki se jih lahko označi kot paradigma za razumevanje načinov, v katerih nedržavni akterji (mednarodne

teroristične skupine, transnacionalna etnično-verska gibanja, mednarodni kriminalni karteli...) lahko regionalno ali globalno delujejo in vplivajo na varnost. Za razliko od državocentričnih groženj, je ta vrsta groženj povezana z nedržavnimi organizacijami ali skupinami, ki lahko ogrozijo posameznikovo, nacionalno ali mednarodno varnost regionalno ali globalno ne glede na geografski prostor. Dejstvo je, da nove grožnje dobivajo vse bolj globalno naravo in razsežnosti.«

Pomembna pa je še ena značilnost sodobnih varnostnih tveganj in groženj, namreč ta, da se njihovo število ves čas povečuje. Pojav novih varnostnih tveganj in groženj namreč praviloma ne nadomesti prejšnjih, ampak jih večinoma samo zasenči in morda odrine na nižje mesto na hierarhični lestvici. Vendar ta še vedno obstaja, čeprav morda ne v aktivni, vsekakor pa pogosto v latentni obliki. Posledica tega procesa je poleg povečevanja števila varnostnih tveganj in groženj tudi povečevanje njihove raznolikosti, kar dodatno zapleta iskanje mehanizmov za njihovo omejevanje, nadzorovanje in odpravljanje. Več kot je različnih virov ogrožanja, bolj multifunkcionalne mehanizme za njihovo obvladovanje potrebujemo. Pri tem je zaznaven paradoks hkratne funkcionalne specializacije in univerzalizacije varnostnih mehanizmov, posebej oboroženih sil nerazvitih industrijskih držav. Zaradi univerzalizacije in globalizacije ter posledične visoke stopnje soodvisnosti je v sodobnem svetu težko klasificirati vire ogrožanja na manj in bolj pomembne, na dolgoročne in kratkoročne, na zunanje in notranje, na nacionalne in mednarodne in vse pogosteje celo na naravne in tiste, ki jih povzroča človek (Kotnik, 2000/2001: 218).

Tako imenovana »**kompleksna grožnja varnosti**« sodobnih družb, se je razvila vzporedno z razvojem netradicionalnega pojmovanja varnosti. Kompleksna narava varnostnega okolja po koncu hladne vojne je generirala oblikovanje kompleksne grožnje varnosti, ki temelji na (Prezelj, 2001a: 810, 2002: 60):

1. hkratnem obstoju vojaške, politične, okoljske, gospodarske, zdravstvene, teroristične, kriminalne, informacijske, identitetne, kulturne itd. razsežnosti ogrožanja varnosti in
2. visoki povezanosti med temi razsežnostmi ogrožanja varnosti.

Tabela 1: **Kompleksnost groženj**

	MEDDR-ŽAVNI KONFLIKT	ZNOTRAJ-DRŽAVNI KONFLIKT	TERORIZEM	OROŽJE + TEHNOLOGIJA	MEDNA-RODNI KRIMINAL	BOLEZNI	PODNEBJE +OKOLJE	POVEZANI Z INFRASTRUKTURO
TRADICIONALNI	x	x	? x	x		? x		
ASIMETRIČNI			x	x	x	? x	? x	x
NOVI AKTERJI (KORPORACIJSKI, DRUŽBENI, INDIVIDUALNI)	x	x	x	x	x	x	x	x
ČLOVEKOVA VARNOST	? x	x	x	? x	x	x	x	x

Vir: A.J.K Bailes (2005).

Beat (2006) pravi, da lahko definiramo štiri različne vrste tveganj z različnimi časovnimi okvirji:

- tveganja kot jasne in prisotne grožnje, vendar brez zadostnih informacij (npr. terorizem),
- kratkoročna nova tveganja, ki so v določeni meri vidna na obzorju (pandemična gripa),
- dolgoročna znana potencialna tveganja (npr. učinki klimatskih sprememb),
- morebitna hitro premikajoča se, nova, neodkrita tveganja (npr. astronomski dogodki).

2 ZAZNAVANJE IN OCENJEVANJE GROŽENJ

2.1 ZAZNAVANJE GROŽENJ

Na osnovi predstavljene razlike lahko ugotovimo, da besede izziv, tveganje in grožnja vzpostavljajo časovno in hkrati intenzivnostno stopnjevanje varnostnih vprašanj. To pomeni, da se ob uporabi obravnavane triade najprej in na najnižji stopnji intenzivnosti srečamo z varnostnimi izzivi, ki lahko bodisi sami prerastejo v varnostna tveganja bodisi jih spodbudijo kot intervenirajoči dejavnik, na naslednji stopnji pa se po preobrazbi ali spodbujevalnem delovanju varnostnih tveganj že lahko srečamo z varnostnimi grožnjami. Ali je umestno govoriti o negotovosti, izzivu, tveganju, grožnji ali nevarnosti, je torej odvisno od verjetnosti (to je od trenutne prisotnosti/odsotnosti varnostno zanimivih pojavov/procesov) in (potencialne) intenzivnosti stika med pojavom/procesom in subjektom, ki se z njim (lahko) sooča. O varnostni negotovosti torej govorimo takrat, ko se pojavi vsaj minimalna možnost, da pride do stika med določenim varnostno zanimivim pojavom/procesom in subjektom (potencialna ogroženost), o varnostnih grožnjah in še posebej nevarnosti pa takrat, ko dejansko že prihaja do negativnega spreminjanja oz. znižanja dosežene ravni kakovosti posameznikovega in/ali družbenega življenja (realna ogroženost) (Kotnik, 2000/2001: 216).

2.1.1 Globalne grožnje

Kot globalne grožnje sem opredelil predvsem v primerih, ko prihaja grožnja izven SV, največkrat tudi izven meja RS.

2.1.1.1 Organizirani kriminal

V zadnjih desetletjih v ospredje prihaja predvsem varnostna grožnja, ki jo predstavlja **organizirani kriminal**, za katerega ne moremo trditi, da je nov pojav v sodobni družbi. Vendar se zaradi njegovih posledic in značilnosti zdi, da sta novejša predvsem njegov obseg in oblika, v kateri se pojavlja. K razvoju in vse večjim (negativnim) posledicam kriminala je prispevala predvsem globalizacija, ki je z vsemi svojimi prednostmi (in slabostmi) vplivala na razraščanje kriminalnih dejavnosti ter odprla možnosti za vse večje povezovanje kriminalnih združb, kjer so se med nekaterimi vzpostavila zavezništva, osnovana na temelju recipročnosti. V zadnjem desetletju je prišlo tudi do pomembnejših sprememb v strukturi in strategiji skupin organiziranega kriminala na mednarodnem nivoju. Po eni strani je prišlo do oblikovanja zavezništev in okrepitve povezav med organiziranimi skupinami, po drugi strani pa so kriminalne združbe razvile večjo fleksibilnost in decentralizirano strukturo. Značilno za njih je tudi, da te kriminalne mreže vzpostavljajo oblike sodelovanja tako z ilegalnimi kot tudi z legalnimi akterji:

- *nezakonita trgovina s prepovedanimi drogami in drugimi opojnimi substancami,*
- *nedovoljena trgovina z orožjem,*
- *trgovina z »belim blagom«,*
- *»pranje« denarja, ki izhaja kot dobiček iz kriminalne dejavnosti,*
- *ilegalna trgovina s ponarejenimi artikli svetovnih blagovnih znamk,*
- *ilegalna trgovina z radioaktivnimi snovmi,*
- *tatvine in kraje…*

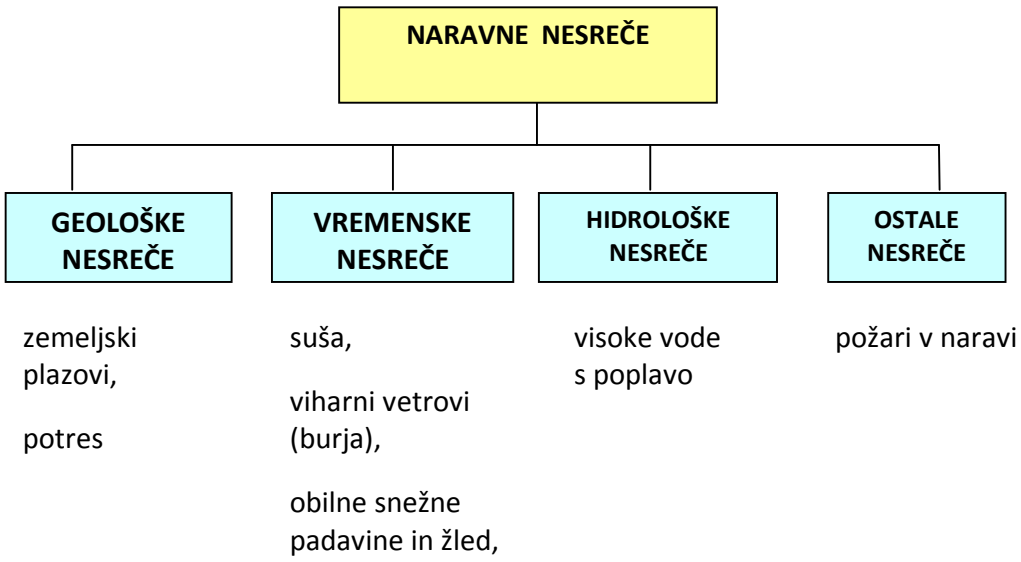
2.1.1.2 Terorizem

Terorizem predstavlja v sodobnem svetu eno izmed ključnih groženj organizacijski, nacionalni in mednarodni varnosti. Zaradi številnih vzrokov, metod in posledic sodi med pojave, ki kompleksno ogrožajo nacionalno varnost. Značilno za terorizem kot grožnjo nacionalni varnosti je, da ima veliko posledic oz. učinkov, ki se vidijo tako v številu žrtev, povzročenem strahu, kot tudi v materialni (gospodarski) škodi. Glavne lastnosti sodobnega terorizma so prožna in ohlapna organizacijska struktura, samozadostnost v smislu financiranja in vse večje mednarodno povezovanje. Med zelo kompleksnimi vzroki zanj pa se pojavljajo tako kulturni, družbeni, politični in globalizacijski vidiki. Predvideva se, da bo v prihodnosti verjetno postal še bolj razširjen, ekstremen, mednaroden in avtonomen. Zaenkrat še ni videti, da bi se glavni dejavniki, ki so prispevali k njegovemu pojavu, zmanjšali, še več, pričakujemo lahko, da bo v prihodnosti njegova intenzivnost še bolj naraščala (Boc, 2007: 27).

2.1.1.3 Naravne in druge nesreče

Naravne in druge nesreče (predvsem antropogene) ostajajo stalen vir ogrožanja, pri čemer se intenzivnost in pogostost nekaterih vrst naravnih nesreč povečujeta kot posledica verjetnih podnebnih sprememb.

Slika 2: Vrste naravnih nesreč v RS



(Vir: Boc, 2007: 33)

2.1.1.4 Zdravstveni viri ogrožanja

Varnost lahko ogrožajo tudi **zdravstveni viri ogrožanja**, ki s svojimi posledicami prizadenejo tako posameznika kot tudi delovanje države. Kljub temu, da so nalezljive bolezni tudi v daljni preteklosti bile vzrok številnih smrtnih žrtev, je sedaj narava in velikost grožnje, ki jo predstavljajo nalezljivi patogeni, danes večja kot je bila kadarkoli v preteklosti, k temu pa pripomoreta predvsem moderna znanost in moderni način življenja.

2.1.1.5 Računalniški kriminal (terorizem)

Z razvojem računalnika in pojavom interneta so se izgubile meje med državami in svet je praktično postal eno. Meje so se izbrisale v pomenu informacijsko komunikacijske tehnologije. Seveda pa je to postal tudi raj za novodobno zlo – računalniški kriminal. Ravno zaradi nenehnega razvoja IKT in povezljivosti sveta se računalniški kriminal izvršuje s pomočjo računalnika proti njemu ali omrežju v raznih oblikah in vrstah. Hiter razvoj IKT je posledica različnih oblik računalniškega kriminala.

Marish Lunker (vir: http://in.linkedin.com/in/drmanishlunker) deli računalniškegi kriminal v tri skupine:

1. Proti posamezniku:

   a. Proti osebi: nadlegovanje po elektronski pošti, elektronsko nadlegovanje, širjenje neprimernega gradiva po spletu, obrekovanje, vdiranje v računalniške sisteme.
   b. Proti imetju posameznika: računalniški vandalizem, prenašanje virusa, spletni vdori, nepooblaščeni nadzor na računalniškim sistemom, vdiranje v računalniške sisteme.

2. Proti organizaciji: v tem primeru so dejanja uperjenja zoper vlado, državne službe, zasebna podjetja in družbe ter skupinam posameznikov. Ta dejanja so: vdiranje v računalniške sisteme, posedovanje nedovoljenih informacij, elektronski terorizem zoper vladne strukture, razpošiljanje piratske programske opreme.

3. Proti družbi: pornografija (še posebej otroška), nemoralno delovanje zlasti pri mladini, spletkarjenje.

2.1.2 Ostale grožnje in tveganja

Razmejitev med globalnimi in lokalnimi oziroma drugimi grožnjami je zelo nejasna. Velikokrat prihaja lokalna grožnja in globalne oziroma ima globalna grožnja vpliv na lokalno. Za primer vzemimo mednarodni kriminal. Organizirani mednarodni kriminal je razvejan na lokalne ravni in in vpliva na stopnjo kaznivih dejanj v manjše organizacije in lokalne skupnosti. Tudi znotraj enot SV je bilo nekaj primerov povezovanja storilcev kaznivih dejanj z združbami na mednarodni ravni.

Na splošno pa lahko o grožnjah in tveganjih na lokalni oz. V našem primeru interni ravni znotraj enot SV govorimo predvsem o naslednjih grožnjah in tveganjih:

- Poškodbe in bolezni,
- Prometne nesreče,
- Nesreče s strelivom in eksplozivi,
- Tatvine in izgube MTS,
- Razkritje ali izgubo oz. uničenje tajnih podatkov,
- Šikaniranje in vse vrste nadlegovanj,
- Nedovoljena trgovina z opojnimi substancami,
- Tihotaplenje blaga preko državnih meja,
- Uživanje alkohola in nedovoljenih opojnih substanc,
- Nepooblaščeno komuniciranje z mediji,
- Širjenje dezinformacij in klevet,
- Incidenti z lokalnim prebivalstvom in s pripadniki tujih oboroženih sil (doma in v tujini),
- Vohunjenje in špijonaža,
- Delikti povezani z denarjem (goljufije, izposojanje...),

- Ponarejanje listin,
- Opustitev dolžnosti,
- Kršenje ali neizpolnjevanje ukazov,
- Lažno in nedosledno poročanje,
- Internetni kriminal...

2.2 OCENJEVANJE GROŽENJ

Sprotno in zgodnje ocenjevanje ogrožanja varnosti je prva faza kriznega upravljanja, ki mora potekati hkrati z zbiranjem informacij iz varnostnega okolja. poleg tega je potrebno zagotoviti, da bo ocenjevanje ogrožanja varnosti neprekinjena dejavnost, prav tako tudi zbiranje podatkov in informacij iz varnostnega okolja. Sodobne vojske so še vedno tisti družbeni akterji, ki imajo največjo odgovornost za odzivanje na številne grožnje, kar je tudi eden izmed razlogov njihovega obstoja. Zato je izvajanje ocenjevanja ogrožanja pomemben korak vsake vojske in njenih enot in na podlagi tako pridobljenih ugotovitev oz. ocen se enota lahko odziva na grožnje varnosti.
Če hočemo izdelati celovito oceno ogroženosti, ki bi zajemala vse varnostne dimenzije, moramo proces specializirati na posamezne vsebinske sklope glede na naravo in lastnosti virov ogrožanja ter jih na koncu integrirati v celoto, kajti celovita ocena ogroženosti je nujni pogoj za usmerjeno, načrtno in organizirano izvajanje dejavnosti na področju sistema varnosti. Zelo verjetno - ni pa nujno - je ogrožanje varnosti največje na področju največje relativne ranljivosti (Boc, 2007: 37).

Analiza ranljivosti je torej aplikacija identificiranih groženj varnosti, predvidevanje kriznih posledic in reakcij kriznega sistema ter sklepanje o nadaljnjih ukrepih za zmanjšanje ranljivosti (Prezelj, 2005: 79). Iz tega izhaja, da je zelo težko določiti, kaj bi morala vsebovati ocena ogroženosti, še najbolj takrat, ko se določa celovita ocena ogroženosti in ne samo ocena za posamezno varnostno dimenzijo ali sektor. Poleg tega posamezni avtorji zastopajo svoje vidike in rešitve. Tako npr. Arnejčič (1999: 14) pravi, da bi bilo pri **oceni grožnje** treba upoštevati naslednje elemente:

- ocena ranljivosti nasprotnika (kje so slabe točke in na katerih točkah je nasprotnik močan),
- okoliščine, pod katerimi so nastali grožnja, situacije ali scenariji, znotraj katerih bo prišlo do kriznih razmer, spopada ali vojne,
- zmožnosti in namere nasprotnika.

Zaradi težav natančnega merjenja je mogoče izdelati samo oceno groženj varnosti oziroma oceno nevarnosti. Ocene groženj varnosti se zato lahko opirajo zgolj na številčno ocenjevanje intenzivnosti (Prezelj, 2000: 41):

- pojavljanja pojavov, ki zelo verjetno v svojih ekstremih predstavljajo grožnje varnosti družb oz. držav in
- posledic (število žrtev, velikost škode) ter na
- oceno verjetnosti dogodka.

Iz vsega navedenega izhaja, da bi ocena ogroženosti morala vsebovati podatke in ocene o:

- virih groženj oz. iz kje izhajajo,
- kateri referenčni objekti so lahko ogroženi oz. koga je potrebno zaščititi (ljudi, živali, okolje, premoženje, dediščina naroda),
- ali so viri groženj dejanski ali potencialni,

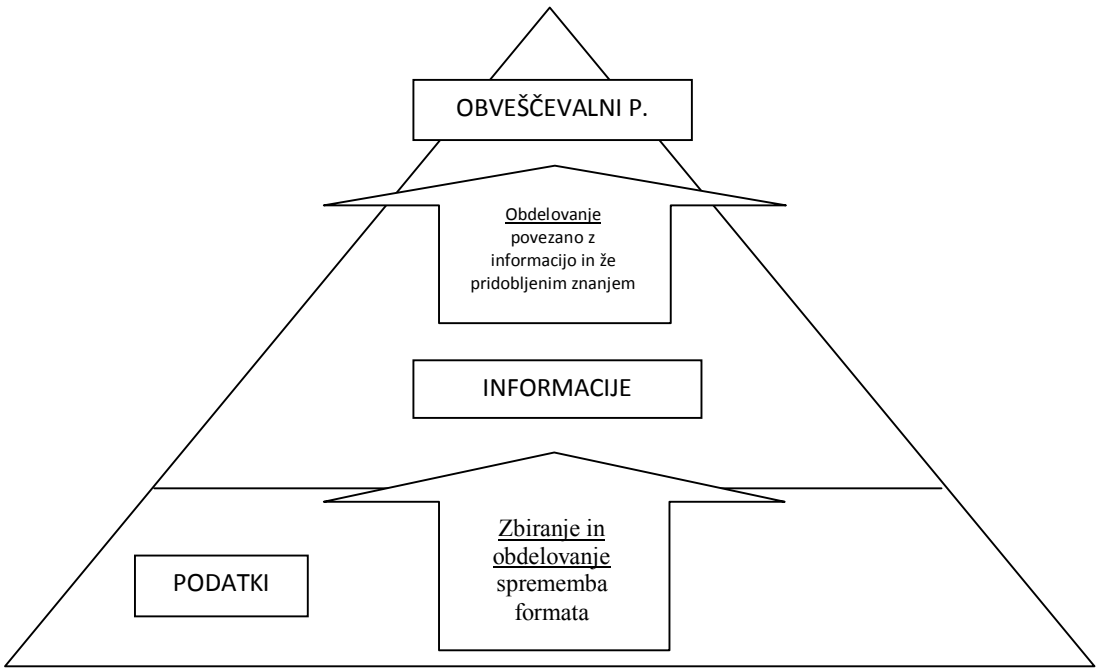
- potencialnih vzrokih groženj,
- verjetnosti pojavljanja groženj,
- vrsti, oblikah in stopnji ogroženosti,
- časovni okvir, ki ga lahko predstavlja grožnja,
- katera področja ocenjujemo (gospodarsko, okoljsko, kulturno, zdravstveno…),

OVS opravlja strokovne obveščevalne, protiobveščevalne in varnostne naloge na področju obrambe skladno z Zakonom o obrambi in Odlokom obrambnega ministrstva o obveščevalni varnostni službi. Naloge OVS so odkrivanje vojaških in asimetričnih groženj nacionalni varnosti in obrambnemu sistemu ter nuditi obveščevalno podporo Slovenski vojski.

2.3 ZBIRANJE INFORMACIJ IN PODATKOV

Informacija ima posebno vrednost, kadar lahko iz nje izdelamo določene zaključke. To pa je lahko tudi rezultat njene povezave s kakšno drugo informacijo, ki smo jo že predhodno pridobili, ali pa povezava pridobljene informacije s predhodnimi izkušnjami. Sami po sebi imajo podatki pridobljeni s pomočjo različnih senzorjev manjšo uporabno vrednost. Podatki zbrani s pomočjo senzorjev postanejo informacije, ko so primerno predelani v ustrezen format. Informacija je sama po sebi dejstvo ali niz dejstev. Če pa jo povežemo z že znano informacijo oziroma umestimo v okvir predhodno znanih dejstev bo nastal nov niz dejstev, ki jih imenujemo obveščevalni podatek. Obveščevalni podatek se od informacije razlikuje po tem, da nastane kot rezultat v procesu subjektivne ocene, ni popolnoma nedvoumen in je odprt za spremembe. Povezovanje enega niza informacij z drugim ali ocenjevanje informacij s primerjavo že zbranih dejstev in informacij v bazah podatkov ter zaključki, ki jih izdela analitik predstavljajo vrh v izdelavi obveščevalnih podatkov iz informacij. Razmerje med podatki, informacijami in obveščevalnimi podatki prikazuje spodnji diagram (AJP-2: 22).

Slika 3: Razmerje med informacijo in obveščevlnim podatkom



Vir: AJP-2: 26

Prej navedena shema kaže, da razmerje med podatki, informacijami in obveščevalnimi podatki ni zapleteno. Zbrani podatki prerastejo v informacijo. Ustrezno obdelane informacije so obveščevalni podatki. Obveščevalni podatki so rezultati sklepov ali zaključkov, ki temeljijo na analizi dejstev.

2.3.1 Obveščevalni podatek

Obveščevalni podatki so definirani kot: »Produkt, ki nastane pri obdelavi podatkov o drugih narodih sovražnih ali potencialno sovražnih silah ali elementih ali območjih dejanskega ali možnega delovanja. Izraz se uporablja tudi za dejavnost katere rezultat je navedeni produkt in organizacije, dejavne na tem področju (AJP-2: 24).«

Obveščevalni podatki omogočajo možnost predvidevanja o možni taktiki potencialnega nasprotnika ali oceno njegovih zmogljivosti. Posedovanje obveščevalnih podatkov prinaša ključno prednost pred nasprotnikom oziroma grožnjo, saj lahko predvidi namen nasprotnika, njegove aktivnosti in reakcije v določenih dogodkih. To pa zmanjšuje tveganja prisotna v konvencionalnem in nekonvencionalnem bojevanju in povečuje možnosti uspeha.

Obveščevalni podatki ne bodo nikoli popolnoma kompletni. V mislih osebe, ki si poizkuša ustvariti celotno sliko o nasprotniku, se bodo vedno pojavljala neodgovorjena vprašanja. Nikoli ni zagotovo, da je obveščevalni podatek popolnoma točen. Na podlagi izvedene ocene o njegovi natančnosti je omogočeno, da se odloči kakšno težo bomo dali obveščevalnemu podatku v procesu odločitve (AJP-2: 25).

2.3.2 Nivoji in tipi obveščevalnih podatkov

Za pomoč pri vodenju obveščevalnega procesa so obveščevalni podatki razvrščeni na podlagi nivojev in tipov. Obstajajo trije nivoji v kategorizaciji obveščevalnih podatkov na podlagi katerih je predviden njihov namen uporabe (AJP-2: 27):

a. Strateška obveščevalna dejavnost. Strateška obveščevalna dejavnost je »Obveščevalna dejavnost, ki je potrebna za oblikovanje politike in vojaških načrtov na državnih in mednarodnih ravneh«.To je najvišji nivo obveščevalnih podatkov izdelan iz informacij pridobljenih skozi najširše možno področje, ki pomeni odgovor na zahteve nacionalnih vlad, ki se odražajo skozi celoten spekter nacionalnih in mednarodnih vojaških, diplomatskih, političnih in ekonomskih zadev.

b. Operativna obveščevalna dejavnost. Operativna obveščevalna dejavnost je »Obveščevalna dejavnost, ki je potrebna za načrtovanje in izvajanje vojaških operacij na operativnem nivoju«. Še natančneje predstavlja obveščevalno dejavnost zahteva za načrtovanje, izvajanje in podporo vojaških aktivnosti in operacij v združenem območju operacij (JOA) s strani združenega poveljstva. To je obveščevalna dejavnost, ki se izvaja v okviru območja obveščevalnega interesa (AII) poveljnika združenega štaba.

c. Taktična obveščevalna dejavnost. Taktična obveščevalna dejavnost je »Obveščevalna dejavnost, ki je potrebna za načrtovanje in izvedbo operacij na taktičnem nivoju.« Obveščevalna dejavnost uporablja nivo informacij podrejenih poveljstev, ki so izdelane v okviru njihovega formacijskega območja.

V okviru vsakega nivoja se obveščevalni podatki lahko nadalje delijo v tri tipe obveščevalnih podatkov (AJP-2: 22):

a. Osnovni obveščevalni podatki. Osnovni obveščevalni podatki so obveščevalna podlaga o zadevah, ki so zajete v bazah podatkov ter se v miru in med izvajanjem operacij stalno nadgrajujejo. Princip uporabe osnovnih obveščevalnih podatkov je, da se jih postavi v situacijo na začetku izvajanja operacij. Povezujemo jih s opredeljevanjem obveščevalnih zahtev, ki jih postavljamo s proučevanjem stalnih dejavnikov, kot sta bojišče in vreme. Na njih pa lahko odgovorimo s postavitvijo novih zahtev v toku izvajanja operacij. Osnovni obveščevalni podatki so definirani kot: » Obveščevalni podatki o kakršni koli temi, ki se jih lahko uporabi kot oporni material za načrtovanje ali kot osnovo za obdelavo nadaljnih podatkov ali obveščevalnih podatkov.«

b. Trenutni obveščevalni podatki. Obveščevalni podatki, ki so izdelani kot odgovor na obveščevalne zahteve katere so povezane s trenutnimi operacijami ter se nanašajo na dogodke v času izvajanja operacij. Trenutni obveščevalni podatki so definirani kot: » Obveščevalni podatki, ki odražajo trenutno situacijo na strateškem ali taktičnem nivoju.«

c. Obveščevalni podatki o cilju. Obveščevalni podatki o cilju so definirani kot: » Obveščevalni podatki, ki podrobno opredeljujejo in določajo komponenete cilja ali celoten cilj in nakazujejo njihove pomanjkivosti in relativno pomembnost«. Ciljna obveščevalna dejavnost zagotavlja podrobne podatke v procesu določanja cilja. Ta proces zagotavlja njihovo učinkovito uporabo v napadalnih sistemih za ognjeno podporo.

2.3.3 Obveščevalni viri

Viri so opredeljeni s številnimi naslovi. V nadaljevanju je predstavljena opredelitev kratic s katerimi se opredeljujejo viri in njihove osnovne karakteristike (AJP-2: 26):

a. Pridobivanje obveščevalnih podatkov s pomočjo zvez. Pridobivanje obveščevalnih podatkov s pomočjo zvez (SIGINT) so obveščevalni podatki pridobljeni s prestrezanjem komunikacij (COMINT) in drugih elektronskih emisij (ELINT).

b. Pridobivanje obveščevalnih podatkov s pomočjo slikovnega materiala. Pridobivanje obveščevalnih podatkov s pomočjo slikovnega materiala (IMINT) pomeni »obveščevalne podatke pridobljene preko senzorjev, ki so lahko nameščeni na kopnem, morju in zraku oziroma so nameščeni na vesoljskih plovilih.«

c. Obveščevalna dejavnost s pomočjo človiških virov. Obveščevalna dejavnoat s pomočjo človeških virov (HUMINT) pomeni » Kategorijo obveščevalne dejavnosti, ki izhaja iz zbiranja in posredovanja informacij s pomočjo človeških virov.« HUMINT lahko dosežemo v prikritih (tajnih) ali v ne prikritih operacijah. Prikrite operacije izvajajo obveščevalne agencije. Sile v JOA na podlagi njihove nacionalne zakonodaje ponavadi izvajajo neprikrite operacije.

d. Pridobivanje obveščevalnih podatkov s pomočjo javnih virov. Pridobivanje podatkov s pomočjo javnih virov (OSINT) pomeni »Pridobivanje obveščevalnih podatkov iz

javno dostopnih informacij, kot tudi drugih informacij brez stopnje tajnosti, ki imajo omejeno javno distribucijo in dostopnost.

Te in druge kategorije obveščevalnih podatkov skupaj s povezanimi viri in agencijami so podrobneje opredeljene v AJP 2.1.

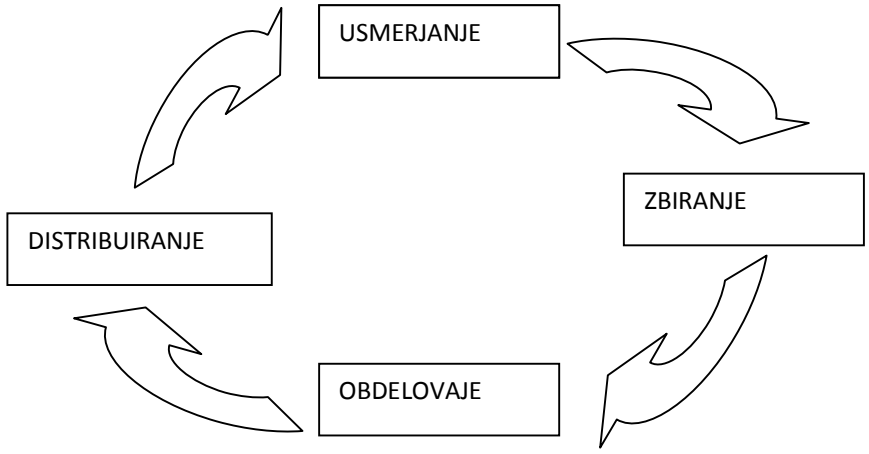
2.3.4 Krog obveščevalnih podatkov

V smislu obdelovanja vseh dostopnih informacij, opredelitve tistih, ki so pomembne ter iskanje tistih katere niso prisotne, obdelovanja ustreznih informacij v obveščevalne podatke, preden le te distribuiramo, zahtevajo strukturiran in sistematičen način izvajanja določenih postopkov. Krog obveščevalnih podatkov je okvir v katerega so vključene štiristopnje postopkov katerih izvajanje rezultira v distribuciji končnih produktov obveščevalnih podatkov. V osnovi se zahteva, da se postopki v krogu obveščevalnih podatkov stalno odvijajo in dopolnjujejo ter odgovarjajo na trenutne in ustrezne zahteve in potrebe poveljnika. Aktivnosti so ločene zato, ker informacije, ki pritekajo, se obdelajo in distribuirajo kot obveščevalni podatki. Aktivnosti se prikrivajo in sovpadajo tako, da se procesi izvajajo hkratno in nepretrgano in ne moremo govoriti o zaporednosti.

Aktivnosti so največkrat opisane kot stopnje ali koraki, ki jih opredeljuje spodaj prikazana shema št.2:

a. Usmerjanje.
b. Zbiranje.
c. Obdelovanje.
d. Distribuiranje.

Slika 4: Krog obveščevalnih podatkov



Vir: AJP-2: 27

a. Usmerjanje

Usmerjanje je prva stopnja v krogu obveščevalnih podatkov in vsebuje »Določanje zahtev za obveščevalne podatke, načrtovanje zbiranja, izdelovanje ukazov in zahtev ustreznim službam in zagotavljanje nepretrganega preverjanja učinkovitosti teh služb.

Obstajata dva vidika usmerjanja (AD70-1: 27):

- Usmerjanje, ki ga posreduje poveljnik svojemu obveščevalnemu osebju. Poveljnik mora usmerjati svoje obveščevalno osebje. On mora posredovati jasne zahteve, ki se navezujejo na informacije in obveščevalne podatke, ki jih potrebuje in če je le mogoče opredeli tudi rok za izvedbo naloge. Kot je le mogoče morajo biti njegove usmeritve vedno natančno opredeljene.Če je le mogoče mora zahtevane informacije ali obveščevalne zahteve opredeliti v prioritetnem redu.

- Usmeritve, ki jih posreduje obveščevalno osebje njihovim virom ali agencijam. To tvori osnovo načrta zbiranja in vsebuje:

1. Odločitev kako morajo biti sestavljeni odgovori na poveljnikova vprašanja in kakšne informacije in obveščevalni podatki so zahtevani za izvedbo naloge.
2. Posredovanje naloge ustreznim virom in agencijam, ki bodo zbrale potrebne informacije in obveščevalne podatke.
3. Izvajanje nadzora, da se prepričamo ali bodo zbrane ustrezne informacije.

b. Zbiranje

Zbiranje je druga faza v krogu obveščevalnih podatkov. Opredeljeno je kot:« Izkoriščanje virov s pomočjo služb za zbiranje in dobavo pridobljenih informacij v ustrezno procesno enoto za uporabo v pripravljanju obveščevalnih podatkov.« To je proces v katerem se zbirajo informacije in obveščevalni podatki zaradi zagotavljanja ustreznih odgovorov na povelnikove informacijske zahteve in zahteve po obveščevalnih podatkih, ki so opredeljene v fazi usmerjanja v krogu obveščevalnih podatkov.

V procesu zbiranja obstajata dva dela:

- Izraba virov s strani agnencij za zbiranje ter na drugi strani izraba virov in agencij s strani obveščevalnega osebja.

- Pravočasno posredovanje zbranih informacij s strani virov in agencij na naslednjo stopnjo v krogu obveščevalnih podatkov, kjer bodo le te obdelane v obveščevalne podatke.

c. Obdelovanje

Obdelava ali obdelovanje je del v krogu obveščevalnih podatkov, kjer se informacije, ki so bile zbrane kot odgovor na usmeritve poveljnika, predelujejo v obveščevalne podatke. Obdelovanje je strukturirano zaporedje aktivnosti, ki se lahko izvaja zaporedno ali pa tudi sočasno z drugimi procesi. Obdelava je opredeljena kot » Pretvarjanje informacij v obveščevalne podatke s primerjavo, ocenjevanjem, analizo, integracijo in razlago«.

Obdelava se izvaja v številnih točkah verige informacij in obveščevalnih podatkov. Vseeno pa sta najpomembnejši točki omenjenega procesa v strukturi, celica analize vseh virov in kombinirano poveljstvo sil za skupne naloge (CJTFHQ). Niz se lahko začne v začetnem

procesu obdelave, ki ga izvaja v okviru zbiranja agencija in največkrat vsebuje samo spreminjanje grobih podatkov v ustrezno obliko za kasnejše obdelovanje obveščevalnih podatkov. Le ti se pošljejo po liniji vodenja in poveljevanja na ustrezen strateški nivo. Vsak nov proces obdelave informacij ali obveščevalnih podatkov na višjem nivoju in z dopolnjevanjem dejstev ali podatkov, ki niso bili znani prejšnjemu nivoju, pomeni, da je nastal nov dopolnjen obveščevalni podatek.

Glavne točke v verigi obdelave podatkov (AJP-2: 31):

1.Razvrščanje v skupine. Razvrščanje v skupine je opredeljeno kot » Pri obveščevalnem delu, korak v obdelovalni fazi obveščevalnega kroga, ki z razvrščanjem med seboj povezanih elementov v skupine, zagotavlja zapis dogodkov in omogoča nadaljno obdelavo.« V praksi je sestavljeno iz postopkov prejemanja, grupiranja in snemanja vseh poročil, ki prihajajo v obveščevalno pisarno na katerem koli nivoju.

2.Ocena. Za namene obveščevalne dejavnsoti, korak v obdelavi kroga obveščevalne dejavnosti, ki opredeljuje ocenjevanje informacije z vidika zanesljivosti vira in verodostojnosti informacije. Ocena je ovrednotenje kako zanesliv je vir in kako verjetno je, da je informacija, ki prihaja od njega točna in zanesljiva. Pridobljeno informacijo ne smemo vzeti kot resnično samo po sebi. Za to obstaja veliko razlogov vključno z namernim zavajanjem, zakaj informacija lahko ni zanesljiva ali popolnoma točna. Proces ocenjevanja pomeni, da je vsak del informacije ali obveščevalnega podatka posebej opredeljen z alfanumeričnimi ocenami. Z njimi določamo stopnjo zaupanja, ki jo lahko prisodimo informaciji ali obveščevalnemu podatku.

Sprejeti standardi vrednosti za ocenjevanje stopenj zanesljivosti virov in kredibilnosti informacij so navedeni v spodnji razpredelnici.

Tabela 2: Vrednosti zanesljivosti in kredibilnosti

Zanesljivost vira		**Kredibilnost informacije**	
A	Popolnoma zanesljiva	1	Potrjena s strani drugega vira
B	Ponavadi zanesljiva	2	Verjetno resnična
C	Komaj zanesljiva	3	Morda resnična
D	Ne vedno zanesljiv	4	Dvomliva
E	Nezanesljiv	5	Neverjetna
F	Zanesljivosti ni mogoče oceniti	6	Resničnosti ni mogoče presoditi

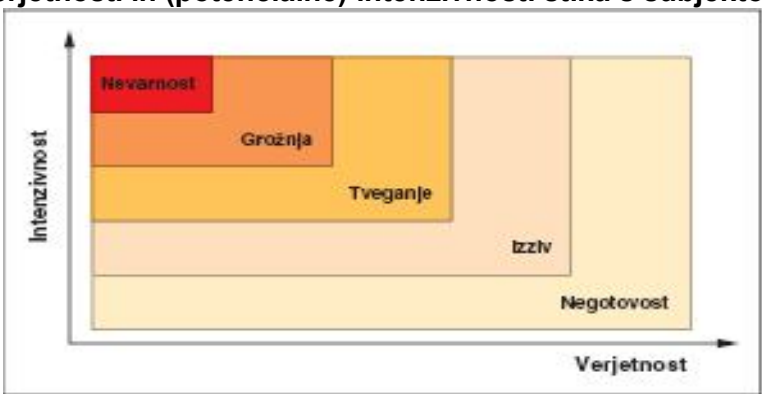
Vir: AJP-2: 31

3.Analiza in sinteza. Analiza in sinteza sta opredeljeni ločeno in pomenita v obveščanju, korak v fazi obdelave obveščevalnega kroga, kjer se produkti pregledujejo, da bi prepoznali pomembna dejstva in jih kasneje interpretirali. in v obveščevalni dejavnosti, korak procesne faze kroga obveščevalne dejavnosti, kjer se analizirane informacije in/ali obveščevalni podatki izbirajo in kombinirajo v vzorec v času nastajanja nadaljnih obveščevalnih podatkov.

V praksi sinteza sledi obliki analize brez presledka za vse namene se ta dva procesa obravnavata kot eden.

V fazi analize so informacije obdelane in ocenjene iz njih pa so izluščena pomembna dejstva. Ta pomembna dejstva se potem primerjajo z že znanimi dejstvi in se združijo v novo obliko. Sinteza se opravi skupaj z dedukcijo in identifikacijo iz njih pa se tvori obveščevalni podatek ali zaporedje dogodkov, ki tvorijo neko individualno sliko. Ta aspekt obdelave podatkov tvori ključno in kritično točko kroga obveščevalnih podatkov saj zaenkrat še niso našli zamenjavo za izkušnje in ocenjevalno zmožnost analitika(AJP-2: 33).

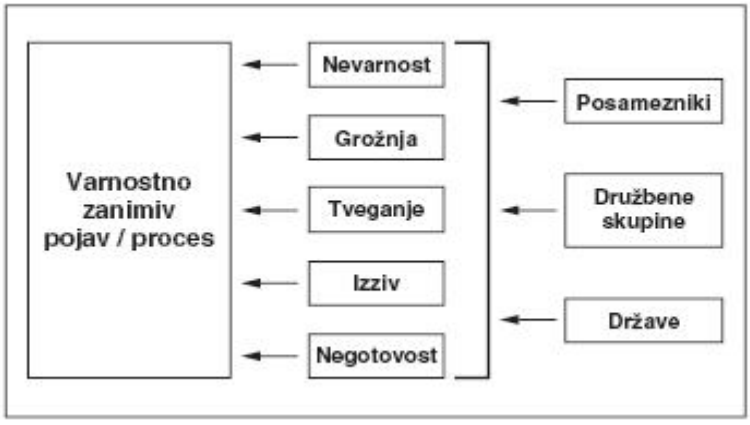
Slika 4: Kategorizacija varnostno zanimivih pojavov/procesov v odvisnosti od verjetnosti in (potencialne) intenzivnosti stika s subjektom



Vir: Kotnik (2001/2001: 216).

4.Razlaga je opredeljena kot končni korak v procesni fazi kroga obveščevalnih podatkov v kateri poteka presoja pomena informacij in/ali obveščevalnih podatkov glede na obstoječe znanje. To je zadnja faza v procesu obdelave, kjer se informacije, ki so bile zbrane, ocenjene in integrirane končno vključujejo in dopolnjujejo proces pretvarjanja informacij v obveščevalne podatke.

Slika 5: Odnos različnih subjektov do istega varnostno zanimivega pojava/procesa



Vir: Kotnik (2001/2001: 216).

5.Povzetek. Sistematična obdelava informacij in obveščevalnih podatkov je izvedena iz zbiranja, ocenjevanja, analize, integracije in interpretacije ter združena s sprejemanjem

informacij ter njihovim snemanjem. Na vse to vpliva izvajanje logičnih metod miselnega procesa, ki pretvarjajo informacije v obveščevalne podatke. Sam mentalni proces je odvisen od širokega znanja o nasprotnikovi taktiki, opremi, organizaciji ter je odvisen od taktične izkušenosti analitika. Na ustrezno izdelavo ocen vpliva tudi velik del zdrave logike, ki je povezan z zmožnostjo izdelati logične zaključke.

6.Razum in intuicija. Zmožnost osebe, da izdeluje logične ocene in zaključke ter njegova intuicijska sposobnost predvidevanja je zelo pomembna za uspešno izvedbo operacij v anlitičnem procesu, ki je srce obdelave informacij. Te sposobnosti se težko naučijo in se lahko prodobijo kot rezultat prakse in izkušenj analitika skozi opravljanje poklicnih dolžnosti na tem področju. Te sposobnosti so kluč do pravilnega napovedovanja obveščevalnih podatkov.

d. Posredovanje

Posredovanje je opredeljeno kot pravočasno pošiljanje obveščevalnih podatkov v ustrezni obliki in na primeren način vsem tistim, ki takšne podatke rabijo. Ključni komponenti tega procesa sta (AJP-2: 33):

a. Pravočasnost. Obstajata dva vidika pravočasnosti. Prvi je, da so obveščevalni podatki, ki dosežejo nameravano lokacijo prepozno, neuporabni. Drugi pa je, da je večina obveščevalnih podatkov na operativnem in taktičnem nivoju zaradi dinamike dogajanja, ter časa, ki ga porabimo za pošiljanje izgubi večji del svoje vrednosti. Oba vidika nas vodita do zaključka, da je potrebno obveščevalne podatke dostaviti do uporabnika v čim krajšem možnem času. Ko je potreba proces obdelave skrajšati zato, da bi se doseglo določen rok, je to potrebno v ustreznih opombah uporabnika na to tudi opozoriti in sicer tako, da ima uporabnik možnost ravnati s podatki glede na stopnjo zanesljivosti.

b. Primernost. Nima smisla posredovati obveščevalne podatke, ki ne odgovarjajo uporabnikovim zahtevami, so za njega nerazumljivi ali pa se pošiljajo preko takšnih sistemov do katerih uporabnik nima dostopa. Obveščevalni podatki morajo biti v obliki, ki je skladna z uporabnikovimi zahtevami. Obveščevalni podatki morajo odgovarjati na zahteve uporabnika, morajo biti napisane v razumljivem jeziku in se morajo pošiljati po komunikacijskem sistemu katerega uporabljata pošiljatelj in prejemnik. Če ni izpolnjena kateri od navedenih parametrov bo zapozneli obveščevalni podatek brez vrednosti.

Pomembnost vseh prej naštetih postopkov zbiranja obveščevalnih podatkov se kaže v tem, da vsaka napaka, nedoslednost, napačna presoja ali ocena lahko bistveno vplivajo na ukrepe v zvezi z zmanjšanjem ali nevtralizacije nevarnosti, tveganja ali grožnje in posledično povzročijo nepopravljivo škodo.

Obveščevalna struktura mora povezati zbiralce, obdelovalce in uporabnike informacij v ustrezno mrežo. Obveščevalna struktura in usmerjanje obveščevalne dejavnosti mora vključevati tudi izvajanje procesa CCIRM ter optimatizirati vsa obveščevalna opravila na vseh nivojih svojih sil ali formacij. Obogočati mora ustrezen časovni pretok informacij in obveščevalnih podatkov vertikalno in horizontalno, kakor tudi znotraj in zunaj enot in svojih formacij.

3 VPLIV NA DELOVANJE SV GLEDE NA OCENO OGROŽANJA

3.1 ZOPERSTAVLJANJE GROŽNJAM IN UPRAVLJANJE S TVEGANJIM

Upravljanje s tveganjem je premišljen proces, ki nam omogoča varno izvajanje aktivnosti, brez ogrožanja varnosti lastnih sil na eni strani ter brez ogrožanja doseganja ciljev, torej poslanstva enote, na drugi strani. Poveljniki morajo neprestano ocenjevati tveganja glede razmer, v katerih se usposabljanje izvaja, da bi preprečili nepotrebne izgube in uničenje opreme. Stopnja tveganja se spreminja z razmerami, ki so odvisne tudi od trajanja usposabljanja, predvsem pa od stopnje usposobljenosti moštva. Na primer: ali je enota že izvajala usposabljanje tovrstnih postopkov? Ali se je usposabljanje že izvajalo ponoči? Ali je moštvo izčrpano? …
S kvalitetno načrtovanim, pravilno vodenim in dobro izvedenim usposabljanjem se izognemo nezgodam. V dobro usposobljenih enotah tako posledično prihaja do manjšega števila nezgod. Večina nezgod je posledica nepravilno usposobljenega, slabo nadziranega, nemotiviranega ali nezadovoljnega moštva (Priročnik za usp.poveljstev in enot, 2011: 24).

Grožnjam se zoperstavlja z upoštevanjem naslednjega (AJP-2: 27):

- Izvajanje ustreznih predhodnih podlag za postavitev varnostnih ukrepov in sicer v najbolj zgodnih fazah načrtovanja, predvsem pri izgradnji vladnih in drugih zgradb državnih organov in kompleksov. S tem lahko prihranimo ogromne stroške, ki bi se nam lahko pojavljali v kasnejšem časovnem obdobju.
- Koncentracijo pomembnih stvari, ki jih je potrebno varovati v čim manjša varnostna območja.
- Ustanovitev večjih varnostnih ukrepov v globini našega sistema.
- Uveljavitev skupnih minimalnih standardov na področju fizične varnosti.
- Izdajanje in uveljavljanje varnostnih navodil, ki so smiselna in praktična.
- Izobraževanje vsega osebja na področju varnosti.
- Usposabljanje osebja, ki je direktno odgovorno za varnost. Še posebno pa v zoperstavljanju subverzivnega delovanja in ideološkim napadom ter jim zagotoviti ustrezne informacije in osnovno znanje s tega področja.
- Uveljavitev principov potrebe po vedenju »need to know« in potrebe po hranjenju »need to hold«.
- Izvajanje stalnih varnostnih nadzorov, pregledov in inšpekcij.
- Zagotoviti uporabo in angažiranost vseh varnostnih specialistov.
- Sodelovanje s protiobveščevalnim (ci) in varnostnim štabom in osebjem ter zahtevati in sprejemati njihove nasvete.

3.1.1 Sistemska zaščita

Zaščita je cilj spreminjanja resnosti in verjetnosti tveganj, ki pripadajo vsem človeškim dejavnostim, na najnižjo, še sprejemljivo stopnjo. Zaščita pomeni predvsem odsotnost nevarnosti oz. ogroženosti in stanje, ko nismo podvrženi tveganju poškodbe.
Največ definicijam sistemske zaščite je skupno ugotavljanje, kako dosegati optimalno stopnjo zaščite znotraj omejitev določenega sistema, ki jih lahko predstavljajo operativna učinkovitost, čas in stroški.

Anžič (2002: 455) pravi, da je sistemska zaščita načrten in sistematično organiziran preventivni pristop, ki temelji na oblikovanju in odzivanju varnostnih mehanizmov, še preden

pride do ogrožanj. Za njegovo uresničevanje pa je predvideno dvoje: predvidevanja in analiza ogrožanj. Ta koncept vključuje poleg omenjenega tudi oceno škode oz. izgub. Njegov osnovni cilj je identificirati vire ogrožanj (grožnje), sledi analiza teh groženj, nadaljuje se z nevtralizacijo škodljivih učinkov in končno doseči ravnovesje med tveganjem in nadzorom.

V preteklosti je bil pristop k ogrožanjem znotraj sistema usmerjen predvsem k ugotavljanju in analizi vzrokov nesreč in iskanju ter uvajanju ukrepov za njihovo preprečevanje, po tem, ko je že prišlo do njih, koncept sistemske zaščite pa predstavlja preventivni pristop, ki je načrtovan in sistematično organiziran ter vsebuje metodo identifikacije, analize in nadzora varnosti.

3.1.2 Preventivni ukrepi in zaščita sil pred potencionalno grožnjo v SV

V vseh oblikah organizacij obstajajo tveganja in potencialne nevarnosti, ki so odvisne od okolja v katerem le-ta deluje, od dejavnosti, ki jo organizacija opravlja in od njenih članov. SV je organizacija, ki je v slovenskem merilu po številu pripadnikov velika organizacija. Njena osnovna naloga je obramba republike Slovenije in njene ozemeljske celovitosti. Okolje v katerem deluje pa je zelo raznoliko. SV večina dejavnosti opravlja v Republiki Sloveniji. V tujini pa SV sodeluje oz je sodelovala:

- v mednarodnih misijah in operacijah (Bosna in Hercegovina, Kosovo, Afganistan, Libanon, Ciper, Čad…),
- izobraževanja v tujini (ZDA, Anglija, Nemčija, Slovaška, Kanada, Irska, Hrvaška, Romunija…)
- mednarodne vaje in usposabljanja (Nemčija, Avstrija, Italija, Turčija, Francija, ZDA, Makedonija, Ukrajina, Francija…)

Iz zgoraj opisanega je razvidno, da pripadnike SV delujejo v zelo raznolikem okolju, ki se med seboj zelo razlikuje po geografskih, vremenskih, kulturnih, nacionalnih, rasnih in drugih značilnosti, ki vse bolj ali manj vlivajo na tveganja, grožnje in potencialne nevarnosti zoper SV in njene pripadnike.

V tej fazi bojnega in nebojnega delovanja SV nastopi t.i. zaščita sil. V Vojaški doktrini SV bg. Furlan opisuje zaščito sil kot aktivnosti, ki se izvajajo za zmanjševanje ranljivosti moštva, opreme, objektov in delovanj pred vsemi grožnjami v vseh situacijah (Furlan in drugi, 2006: 108).

Zaščita sil z vidika obveščevalne podpore pomeni zaščito sil pred konvencionalnimi in nekonvencionalnimi grožnjami. Konvencionalne grožnje so tiste, s katerimi se sile običajno soočajo med delovanjem, nekonvencionalne pa so vohunjenje, terorizem, sabotaže, diverzije in kriminalna dejavnost. Naloga vojaške obveščevalne dejavnosti za podporo zaščite sil je zagotoviti obveščevalne podatke o varnostnih grožnjah in oceno nekonvencionalnih groženj. Oboje je podlaga za načrtovanje elementov zaščite sil, kot so varnost moštva, varnost objektov, informacij, informacijske tehnologije ter varnosti organizacije (GŠSV 2010, 4-16).

V AJP-2 je zaščita sil 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«.

Sami obveščevalni podatki zbrani v zvezi s konvencionalnimi, kakor tudi nekonvencionalnimi grožnjami nimajo nobenega pomena, v kolikor se na njih ne odzovemo s preventivnimi ali kurativnimi protiukrepi.

Zbiranje in obdelava podatkov in izdelava ocen groženj in tveganj so podlaga za načrtovanje in izvajanje ukrepov zaščite sil. Na podlagi izdelanih ocenj ogroženosti, se izdelajo akti poveljevanja, ki opredeljujejo ukrepe zaščite sil (GŠSV, 2011: 3).

3.1.2.1 Ocena ogroženosti

Obveščevalna podpora zaščiti sil se začne z izdelavo ocene groženj, ki opredelijo nasprotnika in druge grožnje za elemente sil zveze NATO. Ta ocena groženj je ponavadi dopolnjena in tvori osnovo za izvajanje zaščitnih ukrepov. Zaščita sil generira lastne poveljnikove zahteve po kritičnih informacijah in prioritetne zahteve po obveščevalnih podatkih, ki so del normalnega delovanja sistema koordinacije zbiranja in usmerjanja zahtev po informacijah (CCIRM). V nadaljevanju se dragoceni obveščevalni podatki, ki so potrebni za zaščito sil pridobijo z obveščevalnim delovanjem, nadzornimi sistemi, določitvijo ciljev in izvidovanjem z ISTAR komponentami.

Podatki se pridobijo s (AJP-2: 37):

- Človeškimi viri na območju operacij, ki jih izvajajo NATO ali nacionalni HUMINT elementi (obveščevalne enote, protiobveščevalne enote (CI), vojaška policija (MP)).

- Lokalni javni viri.

- Nacionalne obveščevalne in protiobveščevalne službe.

Na podlagi zbranih obveščevalnih podatkov, njihove obdelave in analize, je osnova za sistemsko zaščito pripadnikov in enot SV ocena ogroženosti, ki jo za SV izdeluje OVS. Na podlagi ocene ogroženosti se izdela načrt ukrepov, ki s preventivnimi ukrepi odpravlja potencialno grožnjo oziroma nevarnost. Ocena ogroženosti se izdeluje za objekte, kakor tudi za aktivnosti SV.

Ocena ogroženosti je podlaga za izdelavo načrtov varovanj in drugih ukrepov z namenom maksimalnega zmanjšanja potencialne grožnje in tveganj.

Izdelava ocene ogroženosti je zelo pomemben ukrep, ki mora biti izdelan v smislu zoperstavljanja grožnjam. Vsebovati mora naslednje (GŠSV, 2011: 27):

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

Najbolj pregledno se izdela opis po naslednjih točkah (AJP 2.1: 14):

1. Situacija (opišemo trenutno stanje entitet – stvari in bitij in iz njih definiramo cilje, ki bodo najbolj verjetne tarče);
2. Grožnje (opišemo katere grožnje pretijo entitetam – najpomembnejšim ciljem);

3. Ocena tveganja (opišemo verjetnost za uresničitev grožnje posamezni entiteti – pomembnem cilju).
4. Ukrepi (Opišemo varnostne ukrepe, ki zmanjšajo verjetnost uresničitve groženj posamezni entiteti – pomembnem cilju)

3.1.2.2 Ocena tveganja

Ocena tveganja (Priloga 1) za izvajanje aktivnosti SV se izdela na podlagi več parametrov. Osnova za izdelavo ocene tveganja je ocena ogroženosti, ki pa se dopolnjuje še z ostalimi parametri, kot so:

- vrsta aktivnosti,
- izkušnje iz preteklih podobnih aktivnosti,
- dodatne informacije in podatki,
- število in sestava pripadnikov, ki sodelujejo,
- čas trajanja aktivnosti,
- vreme,
- geografske značilnosti področja, kjer se aktivnost izvaja,
- čas izvajanje (noč/dan),
- nacionalnost in število pripadnikov tujih armad, ki sodelujejo pri aktivnosti,
- vrsta in število MTS, ki se na aktivnosti uporablja...

Glavno orodje za upravljanje s tveganjem je matrika, katera je namenjena določitvi stopnje tveganja. Le-to določimo na podlagi dveh kriterijev, in sicer teže nezgode oz. njenih vplivov in verjetnosti, da bo do nezgode prišlo.

S pomočjo Matrike za upravljanje s tveganjem izpolnimo Obrazec za upravljanje s tveganjem, ki je namenjen (GŠSV, 2011: 26):

- identifikaciji tveganja,
- določitvi ukrepov za zmanjšanje tveganja,
- določitvi odgovornih za izvajanje ukrepov za zmanjšanje tveganja,
- opredelitvi zmanjšane stopnje tveganja in
- odobritvi predvidene stopnje tveganja na ustreznem nivoju.

Tabela 3 : Matrika za upravljanje s tveganjem

		Verjetnost				
Vplivi		Pogosto	Verjetno	Občasno	Redko	Malo verjetno
		A	B	C	D	E
Ekstremno	I	I	I	V	V	Z
Kritično	II	I	V	V	Z	N
Obrobno	III	V	Z	Z	N	N
Zanemarljivo	IV	Z	N	N	N	N

	STOPNJA TVEGANJA:	NOSILCI ODLOČITVE:
I	Izjemno visoka	PSSV
V	Visoka	poveljnik brigade
Z	Zmerna	poveljnik bataljona
N	Nizka	poveljnike čete

Vir: GŠSV, 2011: 27

1. Vplivi

Vplive oziroma težo nezgode razvrščamo v naslednje štiri (4) kategorije (GŠSV, 2011:27):

- Ekstremno,
- Kritično,
- Postransko,
- Zanemarljivo.

EKSTREMNO (I)
Izguba sposobnosti za izvedbo naloge ali neuspešno izvedena naloga. Primer nezgodne smrti ali trajne popolne invalidnosti (v primeru nesreče). Izguba glavnih ali za izvedbo naloge ključnih sistemov ali materialnih sredstev. Velika premoženjska (materialna) škoda (na zmogljivostih in objektih). Huda okoljska škoda. Varnostna napaka, zaradi katere ni mogoče uspešno izvesti naloge. Nesprejemljiva stranska škoda.

KRITIČNO (II)
Bistveno (močno) zmanjšana zmogljivost za izvedbo naloge ali pripravljenost enote. Trajna delna invalidnost ali začasna popolna invalidnost v trajanju več kot tri (3) mesece (v primeru nesreče). Obsežna (velika) škoda na materialnih sredstvih ali sistemih. Znatna premoženjska ali okoljska škoda. Varnostna napaka. Velika stranska škoda.

POSTRANSKO (III)
Zmanjšana zmogljivost za izvedbo naloge ali pripravljenost enote. Manjša škoda na materialnih sredstvih ali sistemih, na premoženju ali v okolju. Izgubljeni delovni dnevi zaradi poškodbe ali bolezni, v trajanju do treh (3) mesecev (v primeru nesreče). Manjša premoženjska ali okoljska škoda.

ZANEMARLJIVO (IV)
Malo ali nič negativnega vpliva na zmogljivost za izvedbo naloge. Nudenje prve pomoči ali manj zahtevna zdravstvena oskrba (v primeru nesreče). Neznatna škoda na materialnih sredstvih ali sistemih, ki ostajajo popolnoma funkcionalni in uporabni. Malo ali nič premoženjske ali okoljske škode.

2. Verjetnost

Verjetnost, da bo do dogodka prišlo razvrščamo v naslednjih pet (5) kategorij (GŠSV, 2011: 27):

- Pogosto,
- Verjetno,
- Občasno,
- Redko,
- Malo verjetno.

POGOSTO (A); Dogodi se pogosto, dogaja se redno:
Pri posameznem kosu opreme: Zgodi se zelo pogosto v življenjski dobi. Najverjetneje se bo večkrat zgodilo v času trajanja določene naloge ali operacije. Pri celotni opremi (inventarju): Dogaja se redno med določeno nalogo ali operacijo, ali v času življenjske dobe. Pri posameznem vojaku: Zgodi se zelo pogosto v karieri. Najverjetneje se bo večkrat zgodilo med opravljanjem določene naloge ali operacije. Pri vseh vojakih, ki so izpostavljeni tveganju: Dogaja se redno med opravljanjem določene naloge ali operacije.

VERJETNO (B); Zgodi se večkrat:
Pri posameznem kosu opreme: Zgodi se večkrat v življenjski dobi. Najverjetneje se bo zgodilo v času trajanja določene naloge ali operacije. Pri celotni opremi (inventarju): Dogaja se zelo pogosto, vendar v časovnih presledkih (na splošno pogosti in redni časovni presledki). Pri posameznem vojaku: Zgodi se večkrat v karieri. Najverjetneje se bo zgodilo med opravljanjem določene naloge ali operacije. Pri vseh vojakih, ki so izpostavljeni tveganju: Dogaja se zelo pogosto, vendar v časovnih presledkih.

OBČASNO (C); Dogaja se občasno:
Pri posameznem kosu opreme: Zgodi se enkrat v življenjski dobi. Obstaja približno 50-odstotna verjetnost, da se bo zgodilo med določeno nalogo ali operacijo. Pri celotni opremi (inventarju): Zgodi se večkrat v življenjski dobi. Pri posameznem vojaku: Zgodi se enkrat v karieri. Lahko se zgodi med opravljanjem določene naloge ali operacije, vendar ne pogosto. Pri vseh vojakih, ki so izpostavljeni tveganju: Dogaja se občasno (neredno, redko, včasih).

REDKO (D); Malo verjetno, lahko se zgodi:
Pri posameznem kosu opreme: Lahko se zgodi v času življenjske dobe, vendar je to le malo verjetno. Najverjetneje se ne bo zgodilo v času trajanja določene naloge ali operacije. Pri celotni opremi (inventarju): Pojavljajo se osamljeni primeri. Lahko se zgodi v času življenjske dobe, vendar redko. Do dogodka največkrat ne pride. Pri posameznem vojaku: Pojavi se kot osamljen primer v času kariere. Obstaja majhna verjetnost, da do dogodka pride, vendar najverjetneje ne med opravljanjem določene naloge ali operacije. Pri vseh vojakih, ki so izpostavljeni tveganju: Zgodi se le redko, in sicer kot osamljen primer.

MALO VERJETNO (E); Do dogodka najverjetneje ne bo prišlo, vendar to ni nemogoče:
Pri posameznem kosu opreme: Dogodek ni nemogoč, vendar v življenjski dobi opreme do njega skoraj nikoli ne pride. Do dogodka najverjetneje ne bo prišlo v času trajanja določene naloge ali operacije. Pri celotni opremi (inventarju): Zgodi se zelo redko (skoraj nikoli ali zelo malo verjetno). Možno je, da do dogodka pride v času življenjske dobe. Pri posameznem vojaku: Dogodek ni nemogoč, vendar v času kariere ali med opravljanjem določene naloge ali operacije do njega najverjetneje ne bo prišlo. Pri vseh vojakih, ki so izpostavljeni tveganju: Zgodi se zelo redko, vendar ni nemogoče.

3.1.2.3 Načrt varnostnih ukrepov

»Načrt varnostnih ukrepov« (Priloga 2) je dokument, ki se izdela kot priloga ukaza za izvedbo konkretne aktivnosti SV. Podlaga za izdelavo tega dokumenta je »Obrazec za upravljanjem s tveganji«, ki predvidi vsa tveganja in oceno njihove potencialne nevarnosti. V načrtu varnostnih ukrepov se predvidijo vsa možna tveganja in grožnje in protiukrepi z namenom nevtralizacije ali maksimalnega zmanjšanja nevarnosti za moštvo, MTS in aktivnost. V načrtu varnostih ukrepov se določijo vsi varnosti ukrepi v fazi priprav in med samim izvajanjem aktivnosti, kakor tudi v fazi konsolidacije.

Pri določanju varnostnih ukrepov izhajamo iz rezultatov oziroma ocen, ki so bile določene v »Obrazcu za upravljanje s tveganji«. Glede na določene parametre se določijo tudi varnostni ukrepi.

Primer: če gre za aktivnost, v kateri se bo opravilo veliko prevoženih kilometrov z motornimi vozili po slabših voznih površinah in v slabših vremenskih pogojih, bomo posvetili veliko pozornost predvsem:

- psihofizičnim sposobnostim voznikov (dovolj počitka, nastanitev za njih...),
- brezhibnosti vozil,

- primernosti vozil in njihovi opremi...

Pomembno je, da predvidimo vse varnostne ukrepe glede na oceno tveganja in v sorazmerju s stopnjo tveganja.

Zaključek

Ocenjevanje groženj ima v sodobnem svetu velik pomen. To velja za globalno, kakor tudi za lokalno raven. Nepravilna ocena ima pogosto katastrofalne posledice. Podcenjevanje grožnje privede do opuščanje ali zmanjšievanje varnostnih ukrepov, kar lahko privede do nepopravljive škode. Precenjevanje groženj pa privede do pretiranih ali nepotrebnih varnostnih okrepov, kar ima za posledico:

- Velike finančne stroške,
- Nepotrebno angažiranje človeških resursov,
- Neracionalno razporejanje moštva in MTS,
- Opuščanje varnostnih ukrepov na drugih ravneh...

Teza 1: *Ocena ogroženosti ima velik vpliv na delo protiobveščevalnih in varnostnih organov SV. Vendar protiobveščevalni in varnostni organi v SV pri varnostni zagotovitvi kot osnovo ne uporabljajo le ocene ogroženosti ampak je potrebno le-to nadgraditi še z izkušnjami, trenutno situacijo, vrsto aktivnosti in strukturo ter številom udeleženih pri aktivnosti.*
To tezo lahko v celoti potrdim.

Kot je razvidno iz naloge, ima ocenjevanje groženj velik vpliv na delo obveščevalnih, protiobveščevalnih in varnostnih organov SV. Njihovo delo je mozaki v sestavljanju celotne varnostne zagotovitve od zbiranja informacij, njihovih obdelav, pa do ocene ogroženosti in kasneje izdelave načrta varnostne zagotovitve aktivnosti poveljstevv in enot SV.
Na delo obveščevalnih, protiobveščevalnih in varnostnih organov SV pa ne vpliva le ocenjevanje groženj, ampak tudi izkušnje iz preteklosti oziroma učenje iz izkušenj. Izdelava načrta varnostne zagotovitve le na podlagi ocene ogroženosti oziroma ocene tveganj bi bila toga in pomanjkljiva. Izdelovala bi se zgolj formalna oblika na podlagi togih ocen iz ocene tveganja. Dejansko bi bil to le birokratski postopek primerjave kategorij tveganj in stopnje tveganj in tem primerno določanje varnostnih aktivnosti.

Naloga obveščevalnih, protiobveščevalnih in varnostnih organov SV pa se tu še zdaleč ne konča. Prav v tem delu nastopi njihov del naloge. S svojimi izkušnjami, pridobljenimi v preteklem času in s svojimi dodatnimi informacijami neposredno iz enot in morajo v tem koraku varnostne zagotovitve oplemenititi obstoječe ocene ogrožanja in tveganj. Obveščevalnih, protiobveščevalnih in varnostnih organov SV imajo možnost dodatne varnostne in protiobveščevalne oskrbljenosti zlasti zaradi naslednjih dejstev:

- Ocena ogroženosti se praviloma izdeluje 1x letno za objekte in pred večjimi aktivnostmi. Določena dejstva so se lahko od izdelave ocene ogroženosti že spremenila,
- Ocena je izdelana splošno in načeloma ne predvideva posameznih podrobnosti, ki pri njeni izdelavi niso znane. Primer: sestava moštva, ki bo v aktivnosti sodelovalo (ljudje, ki predstavljajo varnostno tveganje),
- V samem zaključku priprav na aktivnost lahko pride do sprememb, ki jih ocena tveganja ni predvidela. Naloga obveščevalnih, protiobveščevalnih in varnostnih organov SV je, da v tem trenutku k spremembam aktivnosti prilagodijo tudi celotno varnostno zagotovitev,
- Med samim izvajanjem aktivnosti lahko pride do devinentnih pojavov ali aktivnosti, ki zahtevajo spremembe načrtovanih aktivnosti varnostne zagotovitve. To je naloga obveščevalnih, protiobveščevalnih in varnostnih organov SV,

V fazi analize celotne aktivnosti od načrtovanja, izvedbe pa do kosolidacije je naloga obveščevalnih, protiobveščevalnih in varnostnih organov SV, da podrobno preučijo vse segmente varnostne zagotovitve in učinkovitosti le-te na dogodke in obratno. Ta faza je po mojem mnenju zelo pomembna, ne le za enoto, ki je aktivnost izvajala, temveč je pomemben FEET-BACK za izdelovalce ocene ogroženosti. Na ta način bodo neposredno seznanjeni z informacijami in podatki, ki so in kako so vplivali na samo izvedbo. V tem delu se kaže tudi pomembna vloga obveščevalnih, protiobveščevalnih in varnostnih organov SV v krogu obveščevalnih podatkov tudi izven SV.

Teza 2: *Tok obveščevalnih podatkov poteka tudi iz nižjih taktičnih ravni do obveščevalnih struktur na strateški ravni v MORS in so sestavni del pri izdelavi ocene ogroženosti.*
To tezo lahko potrdim le delno!

Kot sem v tezi 2 te naloge navedel, da bom skušal dokazati pomembnost tudi obratnega toka obveščevalnih iz taktičnega in operativnega nivoja protiobveščevalnih in varnostnih organov SV nazaj na strateško raven varnostnih struktur SV, pa tudi RS, lahko to tezo sicer potrdim, vendar z določenimi omejitvami:

- Obraten tok informacij in obveščevalnih podatkov sicer obstaja, a bi lahko bil intenzivnejši,
- Analiza dilevantnih dogodkov na taktični ravni bi lahko bila podrobnejša z namenom zbiranja informacij za bodoče preventivno varnostno delovanje,
- Po vseh večjih aktivnostih SV in ob koncu nekega časovnega obdobja (polleta, eno leto...) bi bilo smoterno na taktičnih nivojih SV izdelati ne le poročilo, ampak analizo, ki bi jo bilo smoterno izmenjevati na taktičnem nivoju med enotami, ne le pošiljati na višje nivoje,
- Zbirniki poročil in analiz bi bilo potrebno v obratnem toku posredovati nazaj v enote, ki bi s tem dobile vpogled v sistem (večkrat se izkaše, da en dogodek ne kaže predznaka varnostnega zanimivega dogodka. Ko pa se v analizi združi več takšnih dogodkov iz različnega okolja, se večkrat izkažejo povezave med dogodki, večkrat tudi za organizirano delovanje),
- Povezovanje protiobveščevalnih in varnostnih organov SV in MORS mora poleg formalnih povezavah potekati tudi na neformalnih vezeh, ki omogočajo hitrejšo in ažurnejšo izmenjavo podatkov in informacij, ter s tem skrajšati čas od zaznavanja grožnje in tveganja do protiukrepov in preventivnega delovanja.

Spisek uporabljene literature

1. Anžič, Andrej (2001) Mednarodni terorizem – sistemski globalni in nacionalno-varnostni pristop. V Milan Pagon (ur.) Varstvoslovje, 254-261. Ljubljana: VPVŠ,
2. Arnejčič, Beno (1999) Nevojaške oblike varnostnih tveganj in groženj. *Revija Slovenska vojska* 177(6), 14-15;
3. Boc, Špela (2007) Soočanje z grožnjami varnosti in stabilnosti v 21. Stoletju – študija primera Slovenija, Kranj
4. Branimir Furlan, Davorin Rečnik, Rudi Vrabič, Vasilije Maraš, Janez Cerkovnik, Branko Špur, Miloš Šonc, Marjan Tušak, Marijan Ivanuša, Boris Gorjup, Martin Kojadin, Kamil Lasič in Marko Unger. 2006. Doktrina vojaške obrambe, Ljubljana: PDRIU,
5. Grizold, Anton (1999) Varnost malih držav v okviru novega evropskega varnostnega okolja. V Kramberger Anton (ur.) *Slovenska država, družba in javnost,* 65-74. Ljubljana: FDV.
6. GŠSV 2010, Direktiva o zaščiti sil v SV, Ljubljana, GŠSV,
7. GŠSV 2011, Priročnik za usposabljanje poveljstev in enot SV, GŠSV
8. GŠSV, 2010, Obveščevalnovarnostna doktrina SV, Ljubljana: GŠSV,
9. Jelušič, Ljubica (2002) Globalnost varnostnih interesov in groženj, *Teorija in praksa*, 39 (4), 613-620.
10. Kotnik, Dvojmoč, Igor (2000/2001) Varnostna tveganja in grožnje v sodobnem svetu. *Ujma*, 14/15, 215-223.
11. Malešič, Marjan (2005) Nekatera teoretična izhodišča preučevanja krize. V Marjan Malešič (ur.) *Krizno upravljanje in vodenje v Sloveniji-izzivi in priložnosti,* 11-26. Ljubljana: FDV.
12. Prezelj, Iztok (2000) Varnost sodobne družbe kot večdimenzionalni pojav (oblikovanje metodološkega modela proučevanja ogrožanja varnosti). Ljubljana: FDV.
13. Prezelj, Iztok (2001a) Nujnost medorganizacijskega sodelovanja pri zagotavljanju nacionalne in mednarodne varnosti. V Milan Pagon (ur.) *Dnevi varstvoslovja*, 809-818, Ljubljana: VPVŠ.
14. Prezelj, Iztok (2006b) Modeliranje celovitega ocenjevanja ogrožanja nacionalne varnosti Republike Slovenije. V Milan Pagon (ur.) *Dnevi varstvoslovja,* 31-40, Ljubljana: VPVŠ.
15. Priročnik OS ZDA, FM 3-100.12 "Risk Management" (MORS, št. 604-16/2006-2 z dne 27. 1. 2006)

Viri:

- Beat Habegger (2006): 3rd Zurich Roundtable on Comprehensive Risk Analysis and Management: How to detect Emerging Risks: http://www.crn.ethz.ch/publications/crn-team/detail.cfm?lng=en?id=27222 (15.12.2006)
- Susan, Strange (2005) »Reference Curriculum: Globalization and Security: "Old" and "New Threats,http://www.isn.ethz.ch/wgcd/Ref_curricula/rc_security_challenges_dr_2005_04_27.doc, (12. 2. 2007),
- Marisc Lunker, http://in.linkedin.com/in/drmanishlunker, (14.10.2008),
- Marish Lunker, http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN005846.pdf
- Resolucija o strategiji nacionalne varnosti Republike Slovenije (Ur.l. RS, št. 92/07),
- Zakon o varstvu pred naravnimi in drugimi nesrečami (Ur.l. RS, št. 64/94),

Seznam slik in tabel

Seznam uporabljenih kratic in okrajšav

AJP - »Alide joint publication«,
GŠSV - Generalštab Slovenske vojske,
INFOSEC- »Information security« Informacijska varnost,
MTS - Materialni tehnična sredstva,
RS - Republika Slovenija,
SV - Slovenska vojska,
Ur. l. - Uradni list,

Priloga 1: Obrazec za upravljanje s tveganjem

OBRAZEC ZA UPRAVLJANJE S TVEGANJEM					
AKTIVNOST: ime vaje *(če je aplikativno)* vrsta aktivnosti *(OBVEZNO)* številka ukaza *(če je aplikativno)* materialno sredstvo ali sistem *(s katerim se bo aktivnost izvajala, npr. helikopter Bell 412)*	**ENOTA:** npr.1/1. četa 10. MOTB	**DATUM:** 12DEC10	**IZDELAL:** čin, ime in priimek položaj, enota		**Št. strani** 1 od 1

TVEGANJE	verjetnost dogodka	vplivi	stopnja tveganja	UKREPI ZA ZMANJŠANJE TVEGANJA (ali VARNOSTNI UKREPI)	IZVAJALEC	zmanjšana verjetnost dogodka	zmanjšani vplivi	zmanjšana stopnja tveganja
PRIMER: Poškodbe med taktičnim premikom peš (vod)	C	III	Z	1. Da bi preprečili padce, poškodbe kolen in gležnjev ter poškodbe oči zaradi nizkega vejevja zagotovite, da se moštvo giblje počasi in pazljivo. 2. Pri načrtovanju in izvedbi premika na določeni smeri se izogibajte možnim oviram (vodne ovire, prepadne stene, …). 3. Ko se oviram na načrtovani smeri premika ni mogoče izogniti zagotovite, da ima enota, ki izvaja premik potrebna materialna sredstva za prečkanje ovire, in da je usposobljena za izvedbo prečkanja. Zagotovite, da enota v procesu priprav na izvedbo premika izvede urjenje postopkov prečkanja pričakovane ovire. 4. Med izvedbo aktivnosti vzdržujte situacijsko pozornost moštva na visoki stopnji.	- poveljniki skupin, - poveljniki oddelkov, - vodni podčastnik, - ocenjevalci.	D	III	N

SKUPNA STOPNJA TVEGANJA PO IZVEDBI UKREPOV ZA ZAMANJŠANJE (ali VARNOSTNIH UKREPOV) (glede na najvišjo zmanjšano stopnjo tveganja)				ODGOVORNA OSEBA (podpis):
IZJEMNO VISOKA	VISOKA	ZMERNA	**NIZKA**	čin, ime in priimek položaj, enota

Priloga 2: Obrazec za načrt varnostnih ukrepov

(obr. F-O/2)

PRILOGA O/J/2

NAČRT VARNOSTNIH UKREPOV

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							
II. V ČASU IZVAJANJA AKTIVNOSTI							

....

IZJAVA O AVTORSTVU ZAKLJUČNE NALOGE

Kandidat (ka) / Slušatelj (ica) (čin ime in priimek) **stotnik Branko Poklič** izjavljam, da sem avtor/ica zaključne naloge z naslovom »**Pomen ocenjevanja groženj pri izvajanju protiobveščevalne in varnostne dejavnosti v SV«**, ki sem jo napisal/a pod mentorstvom **majorja Jožeta Grbec**.

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 **4. Junij 2012** Podpis: _____