

## SMERNICE RAZVOJA OBVEŠČEVALNO- VARNOSTNE DEJAVNOSTI 21. STOLETJA

## GUIDELINES FOR THE DEVELOPMENT OF 21<sup>ST</sup> CENTURY INTELLIGENCE AND SECURITY ACTIVITIES

**Povzetek** Republika Slovenija in njena obveščevalno-varnostna dejavnost sta vpeti v mednarodno okolje. Spremembe v njenem strateškem in varnostnem okolju ter nalogah obrambnega sistema in zahteve po hitrem prenosu ter posredovanju informacij zahtevajo temeljito analizo procesov v obveščevalno-varnostni dejavnosti.

Obveščevalno-varnostna dejavnost na obrambnem področju ima pomembno mesto v vodenju vodilnih političnih struktur in vojaških oseb. S ciljem racionalne organizacije in posredovanja pravočasnih ter kakovostnih informacij podajamo smernice za njen nadaljnji razvoj.

Smernice za razvoj obveščevalno-varnostne dejavnosti temeljijo na podlagi zgodovinskorazvojnne, kvalitativne in primerjalne analize umestitve, delovanja in organiziranosti obveščevalno-varnostne dejavnosti v Natu in slovenskem obrambnem resorju.

V članku je analizirana obveščevalno-varnostna dejavnost v obdobju od osamosvojitvene vojne in začetka profesionalizacije Slovenske vojske do današnjih dni. Analizirani so pravne podlage in procesi dela na vseh ravneh.

**Ključne besede** *Obveščevalno-varnostna dejavnost, na učinkih temelječ pristop do operacij, celovit pristop, razvoj znanja, Slovenska vojska.*

**Abstract** The Republic of Slovenia and its intelligence and security activities are strongly connected to the international environment. The changes in strategic and security environment and defence system tasks, as well as the demands for high speed transmission and provision of information thus require a thorough analysis of intelligence and security processes.

Intelligence and security activities in the field of defence have an important place in the management of leading political structures and military personnel. We therefore offer guidelines for their future development so that rational organisation and provision of timely and quality information could be provided.

The guidelines for the development of intelligence and security activities are based on the historical development, qualitative and comparative analysis of the placement, functioning and organisation of intelligence and security activities in NATO and Slovenian defence sector as such.

The article provides the analysis of intelligence and security activities in the period between the War for Independence and the beginnings of Slovenian Armed Forces professionalization, and today, whereby all legal bases and work processes at all levels have been analysed.

**Key words** *Intelligence and security activities, effects-based approach to operations, comprehensive approach, knowledge development, Slovenian Armed Forces.*

**Uvod** Ustrezen odgovor na pojave asimetričnih groženj je oblikovanje enotnega in integriranega sistema, zato je bil v nekaterih državah in Natu sprejet koncept *na učinkih temelječ pristop do operacij* (angl. Effect Base Approach to Operations – EBAO), ki je prešel v *celovit pristop* (angl. Comprehensive Approach – CA), v katerem je posebno mesto namenjeno reorganizaciji obveščevalno-varnostne dejavnosti. Posebej so tega deležna operativna poveljstva, ki s svojo funkcijsko odgovornostjo in procesi vodijo najpomembnejše operacije zavezništva. Obveščevalno-varnostna dejavnost se iz klasične ozko štabno organizirane dejavnosti s konceptom *razvoja znanja* (angl. Knowledge development – KD) reorganizira v *centre znanja* (angl. Knowledge centre - KC), v katerih se vedenje in znanje zbirata, ob uporabi človeškega znanja in računalniških programskih orodij sistemsko analizirata ter posredujeta odločevalcem.

Glede na spremenjeno varnostno okolje obveščevalno-varnostna dejavnost gotovo pridobiva nove razsežnosti in pomen. Klasični elementi, vsebovani v obveščevalnih disciplinah, ostajajo, vendar se zaradi večrazsežnostnega in racionalnega pogleda poraja vprašanje o smotnosti, racionalizaciji procesov, upravičenosti umestitve in organiziranosti obveščevalno-varnostne dejavnosti. Ta se mora hitro prilagajati in prilagoditi Natovim usmeritvam oziroma varnostnim okoliščinam na globalni ravni.

Temeljni namen članka je analizirati delovanje obveščevalno-varnostne dejavnosti v Republiki Sloveniji na obrambnem področju in predlagati nekaj rešitev za racionalnejše in kakovostnejše opravljanje poslanstva, prilagojenega novim izzivom. Temeljna ideja je »v danih razmerah optimalna«.

Spremenjene grožnje in narava konfliktov v obdobju po hladni vojni ter projekcija prihodnjega varnostnega okolja zahtevajo od držav ter organizacij, na primer

OZN, EU, Nata itn., drugačen in predvsem učinkovitejši način spoprijemanja s tovrstnimi izzivi. Grožnje in izzivi imajo seveda pomembne implikacije in zahtevajo pomembne spremembe v varnostnih sistemih in oboroženih silah.

Resolucija o splošnem dolgoročnem programu razvoja in opremljanja Slovenske vojske do leta 2025 – ReSDPRO SV 2025 (2010, str. 7) navaja, da »se je v evroatlantskem prostoru močno zmanjšala verjetnost izbruha oboroženih meddržavnih spopadov. Vojaške grožnje se bodo pojavljale predvsem v obliki lokalnih in regionalnih nestabilnosti, ki lahko hitro prerastejo svoj okvir. Sodobne grožnje prevzemajo vse bolj hibridno obliko, njihov značaj pa zaradi močnih globalizacijskih vplivov postaja večplasten in mednaroden, takšni pa so tudi njihovi učinki. Bojišče prihodnosti bo poleg kopnega, morja in zraka obsegalo tudi kibernetški prostor in vesolje«.

Vrhovno poveljstvo zavezniških sil za Evropo (SHAPE) je dobilo poslanstvo in nalogo oblikovanja Natovih odzivnih sil, ki bodo zavezništvu omogočale nove vojaške zmogljivosti. Tako bo zavezništvo imelo pomembno vojaško zmogljivost – zmožnost proaktivnega delovanja. To predstavlja pomembno zgodovinsko spremembo v načinu odzivanja zavezništva, ki je v času hladne vojne delovalo reaktivno; takrat je bila določba 5. člena o kolektivni obrambi jasna, obrambni načrti so bili pripravljene vnaprej, številne vojaške enote so bile razmeščene vzdolž mej tedanjih držav članic zavezništva.

Proaktivnost v novem načinu zavezniškega razmišljanja pa ne pomeni takojšnje uporabe sile, temveč sposobnost preprečevanja konfliktov, reševanje kriz in njihovega pravočasnega odkrivanja. Na podlagi navedenega je v Natu izdelana študija in na podlagi te koncept EBAO ter pozneje model CA, po katerem se morajo poveljstva Nata reorganizirati (transformirati) iz funkcijsko usmerjenih v procesna, kar velja tudi za obveščevalno-varnostno dejavnost. Operativni poveljstvi Nata (angl. Joint Force Command), prvo v Brunsummu in drugo s sedežem v Neaplju, sta se organizirali leta 2009.

Na obrambnem področju, na katerem ne gre le za enega nosilca obveščevalno-varnostne dejavnosti, lahko govorimo o obrambni in vojaški obveščevalno-varnostni dejavnosti. V obeh primerih gre za dejavnosti, katerih namen so zbiranje in obdelava podatkov ter informacij na obrambnem področju, izdelava obveščevalno-varnostnih informacij ter posredovanje teh informacij naročnikom oziroma uporabnikom.

Vojaška obveščevalno-varnostna dejavnost v sodelovanju z obrambno s svojimi organizacijskimi in tehnološkimi rešitvami izpolnjuje nacionalne obrambne potrebe in delovanje oboroženih sil ter zavezništev. To se zagotavlja z angažiranjem vseh razpoložljivih virov, tudi s sodelovanjem s civilnimi in obrambnimi nosilci obveščevalno-varnostne dejavnosti, z vojaško obveščevalno-varnostno dejavnostjo oboroženih sil ter prek izmenjave informacij z drugimi pristojnimi resornimi organi države in s tujimi partnerskimi obveščevalno-varnostnimi službami.

Ugotavljamo torej, da je »vojaška obveščevalna dejavnost celota funkcij, procesov, postopkov in ukrepov posameznikov, enot in poveljstev, s katerimi neprekinjeno

in celovito spremljajo, analizirajo in predvidevajo vojaško, vojaško-politično in varnostno situacijo ter delovanje sovražnika, *možnega sovražnika in druge vojaške ter varnostne grožnje, da lahko poveljnikom in drugim, ki odločajo o uporabi obo-roženih sil, omogočijo sprejem kakovostnih in pravočasnih odločitev na vseh ravneh poveljevanja*«. (Furlan et al, 2006, str. 3)

Zavezništvo se v svojih strateških načrtih prilagaja na nove izzive varnosti, s katerimi se srečuje pri vzpostavljanju miru v mednarodnih operacijah in na misijah (MOM). Iz precej ozkega pogleda na okolje, v katerem delujejo vojaki Nata, pri čemer je bila poglobljena informacija za poveljnike in druge odločevalce le stanje zemljišča, nasprotnika in vremena, prehajamo v celovit pristop, v katerem se za analiziranje, načrtovanje in realizacijo političnih in vojaških načrtov uporabljajo vsi viri ob tako imenovanem mavričnem okolju; za celovito obvladovanje situacije moramo poznati celovito okolje, s katerim se srečujemo v MOM.

## 1 METODOLOGIJA

Naše ugotovitve in smernice za razvoj obveščevalno-varnostne dejavnosti temeljijo na podlagi zgodovinskorazvojne, kvalitativne in primerjalne analize umestitve, delovanja in organiziranosti obveščevalno-varnostne dejavnosti v Natu in slovenskem obrambnem resorju.

Velik poudarek je na primerjalni metodi in kvalitativni analizi. Kvalitativno analizo smo uporabili za izbor najprimernejše oblike organiziranosti obveščevalno-varnostne dejavnosti. Za pomoč smo uporabili DEXi – program za pomoč pri odločanju, ki temelji na načelih večparametrskega modeliranja in je namenjen procesom odločanja.

Avtorji v tem prispevku govorimo o obveščevalno-varnostni dejavnosti na obrambnem področju, čeprav je poudarek predvsem na vojaški obveščevalno-varnostni dejavnosti. Obrambni sistem vidimo kot vsoto podsistemov z medsebojnim součinkovanjem, zato opisovanje vojaške obveščevalno-varnostne dejavnosti ne vidimo kot oviro; nasprotno, kot del sistema s svojimi učinki vpliva na celotni sistem kot sestavljeno celoto. Tudi Nato je obrambna organizacija, v kateri so vojaški vidiki najpomembnejši, novi koncepti pa izhajajo iz potreb večrazsežnostnega in racionalnega pogleda vojaške obveščevalno-varnostne dejavnosti, hkrati pa je to odraz izkušenj avtorjev. Naše izkušnje izhajajo iz obrambnih in vojaških izkušenj obveščevalno-varnostne dejavnosti v Republiki Sloveniji v MOM ter poveljstvih Nata.

V tem prispevku uporabljamo pojem obveščevalno-varnostna dejavnost, kot jo definira Vojaška doktrina (Furlan et al, 2006, str. 3).

Slovenska vojska (SV) je izdelala nekaj dokumentov, ki podrobneje usmerjajo poveljstva in enote v SV o organiziranju, pristojnostih in odgovornostih izvajanja obveščevalno-varnostne dejavnosti na vseh ravneh poveljevanja. Zaradi tajnosti vsebin dokumentov o njih ne moremo posebej razpravljati.

## 2 NATOV KONCEPT PROAKTIVNEGA OBVEŠČEVALNO-VARNOSTNEGA DELOVANJA

Odgovorni v Natu so iz izkušenj delovanja in izvajanja operacij ter hkratnega testiranja novih konceptov uvideli, da predvsem vojaška delovanja niso dovolj za doseganje ciljev v sodobnih, kompleksnih okoljih; za doseg celovitih političnih, civilnih in vojaških rešitev je potrebna vključitev preostalih akterjev (Cazamea, 2011).

Na podlagi pridobljenih izkušenj nekaterih držav članic Nata (ZDA in ZR Nemčije) iz operacij na Kosovu in v Afganistanu je očitno, da je uporaba celovitega pristopa ključna. Za doseganje tega je potrebna ozaveščenost, da klasično obveščevalno delo, pri katerem produkti opredeljujejo le nasprotnika v določenem času in prostoru, nadomešča celovit pristop, ki zahteva celovite podatke in znanje (angl. knowledge) o sposobnostih, zmožnostih, povezavah in vplivanju na vse akterje na območju delovanja operacije (Kuehtreiber-Fritz, 2011).

Proaktivnost v novem načinu zavezniškega razmišljanja ne pomeni takojšnje uporabe sile, temveč sposobnost preprečevanja konfliktov, reševanje kriz in njihovega pravočasnega odkrivanja. Uveden je koncept EBAO, ki so ga uvedle ZDA v prvi zalivski vojni in se navezuje na uvajanje vojaških in nevojaških metod delovanja za doseg čim boljših uspehov ob minimalni kolateralni škodi (Batschlet, 2002, 3,20).

Koncept je bil več let testiran in ob tem deležen številnih kritik, saj ni upošteval vseh akterjev v prostoru nastajanja (reševanja) krize, pri tem celo zavrnil uveljavljene doktrine ter po nepotrebnem zapravljaj energijo (Vego, 2006, str. 52–56) in vnašal zmedo med visokimi poveljniki, ki se zaradi napak koncepta niso mogli resnično posvetiti reševanju operativnih izzivov (Riper, 2009, str. 84–85). Prav tako je zaradi nepravilnega interpretiranja informacij vzbujal odločevalcem nepravilno dojemanje okolja (Mattis, 2008, str. 22). Uspešen je bil na taktični ravni, za odločevalce na operativni in strateški ravni pa ni bil zadosten.

Po končanju študije in koncepta EBAO leta 2009 je bil ob upoštevanju ugotovitev in zahtev Nata po vrhu 2009 koncept preimenovan v celovit pristop. V osnovi sledi študiji EBAO, upošteva pa dodatne zahteve po sodelovanju s civilnimi institucijami (Zuna, 2010, str. 5–18).

### 2.1 Koncept razvoja znanja – (r)evolucija obveščevalno-varnostne dejavnosti

Koncept razvoja znanja predstavlja osnovo delovanja Nata v prihodnjem obdobju, ki lahko kljubuje sodobnim izzivom. Po njem se morajo poveljstva Nata reorganizirati oziroma preoblikovati iz funkcijsko usmerjenih v procesna, kar velja tudi za obveščevalno-varnostno dejavnost.

Ključnega pomena je celovito združevanje vseh podatkov in informacij v znanje in procese, ki bodo odločevalcem - poveljnikom v procesu sprejemanja odločitev

na voljo čim prej in celovito (holistično). Bistvo tako posredovanega znanja je razumevanje celovitosti varnostnih razmer, pri čemer interdisciplinarni strokovnjaki poveljujočim posredujejo analizirane informacije v obliki odgovorov. Uspešnost odgovorov na celovitost temelji na sistemskem pristopu, ki upošteva dojemanje okolja kot nedeljive celote, pri čemer je pri vsakem posegu v kateri koli del treba opazovati relacije v celotnem sistemu. Posredovano znanje vključuje vse možne posledice in odzive ob različnih odločitvah. Hkrati napoveduje možne izhode ob različnih ravnanjih (Håkon, 2006, str. 1–3).

Zaradi narave sodobnih konfliktov, v katerih niso vključene le vojaške oborožene sile, obstaja zahteva po »povezavah« z viri informacij zunaj tradicionalno vojaških področij ali organizacije (mednarodne organizacije, nevladne organizacije, univerze, itn.), da bi se razširilo razumevanje specifičnega okolja in prostora. Znanje ustvarjajo ljudje in vključuje izobraževanje, izkušnje, razmišljanje, sprejemanje odločitev in vse druge sposobnosti za ustvarjanje možnosti in ukrepanja. Ustvarjeno znanje mora biti sistematično shranjeno in obdelano z uporabo standardiziranih metod ter informacijskih sistemov, s katerimi ustvarimo organizacijsko bazo znanja in ki so v veliko pomoč pri operativnem načrtovanju. Pridobljeno znanje v doktrini celovitega pristopa je namenjeno ne le poznavanju klasičnih vojaških elementov (sile, zemljišče, oprema, logistika in infrastruktura), temveč tudi ravnanju nasprotnika (Midan, 2009, str. 41).

Da bi se lažje spoprijeli z izzivi in celovitostjo sodobnega bojevališča, je koncept razvoja znanja razširil ciljne skupine, s katerimi se odgovorni v obveščevalno-varnostni dejavnosti ukvarjajo. Iz nekoč le ene razsežnosti (nasprotnika) se zdaj v vseh postopkih obveščevalnega cikla sistemsko analizirajo politični, vojaški, ekonomski in socialni dejavniki, infrastruktura ter informatika (angl. Political, Military, Social, Infrastructure and Information – PMESII). Dejavniki, vključeni na območju delovanja oziroma interesa, so tako imenovane mavrične (angl. rainbow) interesne skupine: lastne sile, sovražnik, vladne in nevladne organizacije. Končni produkti predstavljajo večjo količino informacij, pri čemer predstavlja najpomembnejši del predvidevanje (Mitchel, 2008, str. 14).

Razvoj znanja podpira načrtovanje, izvajanje in ocenjevanje z zagotavljanjem celostnega razumevanja prostora. V osnovi se postopki v procesu ne razlikujejo med klasičnim obveščevalnim ciklusom, večje spremembe so vidne v izvajanju procesov, predvsem v analiziranju (diagram 1).

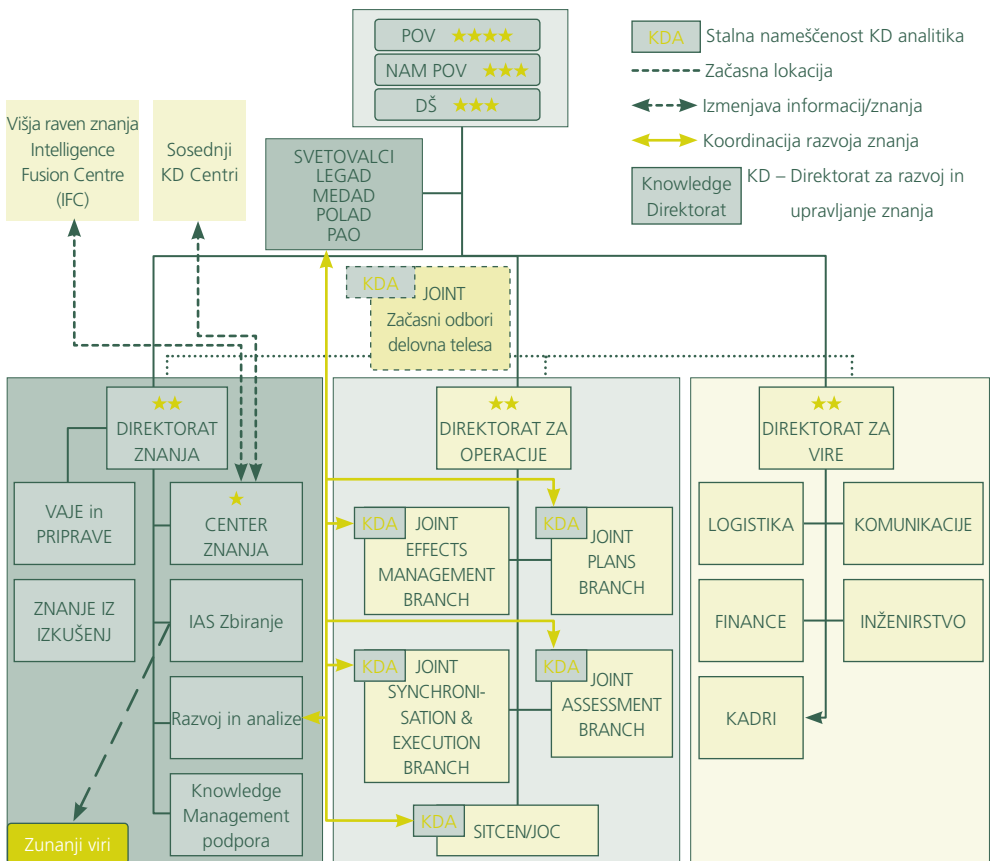
## 2.2 Organiziranost razvoja znanja v Natu

Na strateški ravni SHAPE ohranja najpomembnejšo vlogo v Natovi obveščevalno-varnostni dejavnosti. Pri razvoju znanja ima najpomembnejšo vlogo pri organizaciji in menedžmentu *Obveščevalni center za združevanje podatkov* (angl. Intelligence Fusion Centre – IFC v Molesworthu v Veliki Britaniji, saj z novim konceptom dobiva glavno vlogo v »razvijanju« in produkciji obveščevalnih produktov. IFC predstavljajo regijske centre, v katerih se za potrebe odgovornosti, na primer za Isaf,

informacije dodatno analizirajo in posredujejo podrejenim taktičnim poveljstvom ter poveljstvu operacije.

Da bi EBAO lahko zaživel na operativni ravni, sta bila JFC Brunssum in JFC Neapelj 2009 reorganizirana. Iz klasične štabne organiziranosti dela sta prešla v procesno naravnost, pri čemer so načrtovalci v upanju po ustreznem razmerju med kakovostjo in količino kadra število zaposlenih zmanjšali za 50 odstotkov. Na novo so vzpostavljeni trije direktorati: direktorat za vire, direktorat za operacije in direktorat znanja. V slednjem najboljše deli predstavlja center znanja, sestavljen iz treh sektorjev. Za razvoj in končne produkte je odgovoren sektor za razvoj in analize (diagram 1), ki ob izvajanju systemske analize (angl. System of Systems – SOSA), sodelovanju analitikov v direktoratu za operacije in ob izdatni podpori analitičnih računalniških orodij, razvitih posebej za analiziranje in sintetiziranje podatkov, skrbi za pravočasne, natančne in celovite informacije (Kuehntreiber-Fritz, 2011).

**Diagram 1:**  
Razvoj znanja v operativnem poveljstvu Nata  
Vir: Henigman, 2012, prirejeno po BI-Sc Command Knowledge Development, 2010.





### 3 OBVEŠČEVALNO-VARNOSTNA DEJAVNOST NA MINISTRSTVU ZA OBRAMBO REPUBLIKE SLOVENIJE

Zakon o obrambi (ZOBR) RS določa, da obveščevalno-varnostno dejavnost na obrambnem področju v obliki izvajanja obveščevalno-varnostnih nalog izvaja Obveščevalno varnostna služba ministrstva<sup>1</sup> (OVS). OVS je organizirana kot organizacijska enota ministrstva, ki ima lahko svoje izpostave v SV. Zakonodajalec je z Uredbo o obveščevalno varnostni službi Ministrstva za obrambo Republike Slovenije (MO RS) podrobneje uredil njeno delovanje in organizacijo.

Od leta 1991 do 1994 je bila obveščevalno-varnostna dejavnost delno vezana na obveščevalne organe v Teritorialni obrambi (TO), večji del nalog pa so izvajali varnostni organi Ministrstva za obrambo (VOMO), ki so bili močno vpeti v delo štabov TO. Z novim ZOBR leta 1995 je VOMO prešel v OVS, ki je do svoje reorganizacije imela »aktivne« izpostave v SV. Po reorganizaciji leta 2000 so del teh nalog prevzeli novoorganizirani vojaški obveščevalno-varnostni organi J/G/S-2 v SV. Njihove naloge in odgovornost je minister za obrambo določil z Odredbo o izvajanju nalog organa, pristojnega za obveščevalno podporo poveljevanju in vodenju ter za izvajanje štabno varnostnih nalog v SV. Naloge izključujejo izvajanje tajnih ukrepov in preiskovalnih dejanj, saj vojaški obveščevalno-varnostni organi takih pooblastil nimajo oziroma jih **še vedno imajo le** nekateri pripadniki OVS. Z novo reorganizacijo je SV dobila širšo strukturo obveščevalno-varnostnih organov, s pomočjo katerih je lažje izvajala vojaško obveščevalno-varnostno dejavnost.

Strateška obrambna pregleda (SOPr 2005–2010 in 2007–2012) določata integracijo J-2 GŠSV in OVS, da bi se racionalizirala uporaba virov in procesov ter da bi se dosegla višja stopnja učinkovitosti na področju obrambne obveščevalno-varnostne dejavnosti. V letih 2004–2005 je bil tako ustanovljen Oddelek za obveščevalne analize GŠSV (OOA2) in umeščen v strukturo OVS. Cilj je bil doseganje višje stopnje racionalizacije, usklajenosti in dopolnjevanja z obveščevalno analitiko OVS. Oblika dela je temeljila na skupnem delu pripadnikov SV in OVS. Kljub začetnim težavam je bila to dobra oblika integracije vojaškega in upravnega dela MO.

Po končani kadrovski konsolidaciji SV leta 2010 se je OOA ukinil, pripadniki SV pa so bili prerazporejeni na druge dolžnosti v SV (Grozde, 2011, str. 6).

#### 3.1 Obveščevalno-varnostna dejavnost v Slovenski vojski

V SV se v okviru obveščevalno-varnostne dejavnosti izvajajo obveščevalna, protiobveščevalna in varnostna dejavnost ter sistematično opazovanje in pridobivanje podatkov o ciljih. Izvajajo se v miru in vojni.

<sup>1</sup> 3. odstavek 32. člena Zakona o obrambi RS.

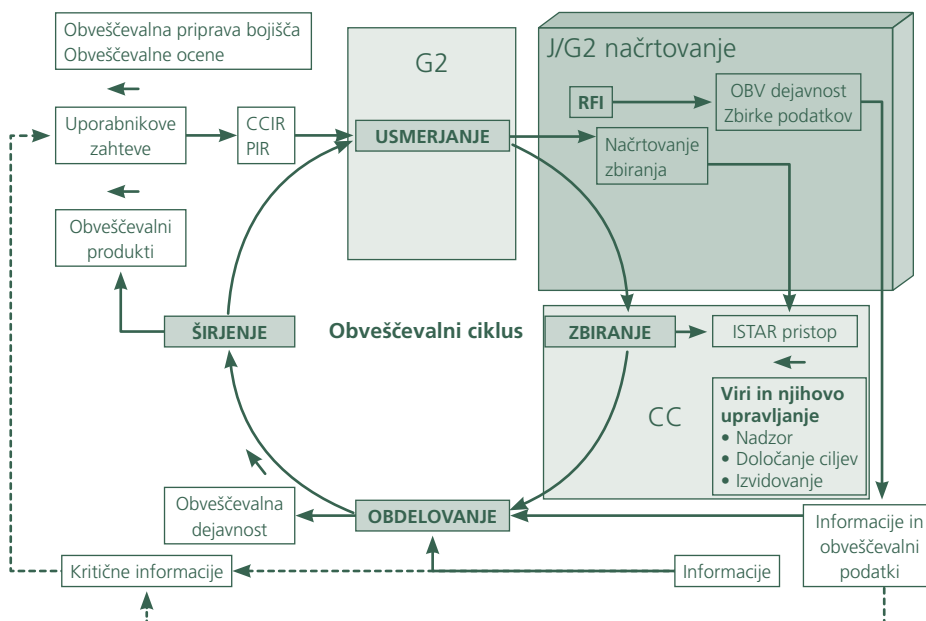
<sup>2</sup> OOA je bil ustanovljen za povezovanje obveščevalnih procesov med OVS in SV. Fizično je bil v OVS, po poveljniški liniji pa je bil vezan na NGŠSV (in J-2).



Viri obveščevalno-varnostne dejavnosti so človeški viri, slikovna in pisna gradiva, tehnična sredstva, sredstva zvez, radarji, javni viri in zaplenjena tehnična sredstva ter oprema. Osnova učinkovite obveščevalne dejavnosti je obveščevalni cikel, ki obsega opredelitev obveščevalnih zahtev in načrtovanje, zbiranje in obdelavo obveščevalnih informacij ter njihovo posredovanje uporabnikom. Del obveščevalne dejavnosti je elektronsko izvidovanje, ki se v Slovenski vojski izvaja centralizirano.

ZOBR v svojem delu o izvajanju obveščevalno-varnostne dejavnosti posebej omenja obveščevalne, protiobveščevalne in varnostne naloge na obrambnem področju, ki jih opravlja OVS (1., 2. in 3. odstavek 32. člena ZOBR). SV pa izvaja preventivne naloge protiobveščevalne zaščite. Štabni varnostni organi v sestavi J/G/S-2 opravljajo 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 OVS. Štabni varnostni organ GŠSV strokovno vodi in usmerja delovanje podrejenih štabnih varnostnih organov ter sodeluje z OVS (5. odstavek 32. člena ZOBR).

Slika 1: Procesi ISTAR in obveščevalni cikel  
Vir: Henigman, Rode, 2010, prirejeno po AJP-2.0, STANAG 2190, 2003.



Obveščevalno-varnostna dejavnost z aktivnim delovanjem in usmerjanjem ISTAR<sup>3</sup> podpira delovanje SV v MOM (slika 1). ISTAR predstavlja »sistem sistemov«, ki vključuje izdelke senzorjev v stopnjah zbiranja, usmerjanja in obdelave v obveščevalnem ciklusu ter procesu *določanja ciljev* (angl. targeting). Zagotavlja infor-

<sup>3</sup> Intelligence, Surveillance, Target Acquisition, and Reconnaissance.

**Tabela 1:**  
Izvajanje obveščevalno-varnostnih procesov in nalog na različnih ravneh  
Vir: Henigman, 2012, prirejeno po AJP-2.0, STANAG 2190, 2003.

PROCES	IZHAJAJOČE NALOGE		RAVEN IZVAJANJA		
			STR	OP	TKT
USMERJANJE	CCIR, PIR	DL	X	X	-
	Izdelava krovnih dokumentov	DL	X	X	-
	Izdajanje strokovnih usmeritev	DA	X	X	-
	Nadzor nad izvajanjem nalog	DA	X	X	-
	Nudenje strokovne pomoči	DL	X	X	-
NAČRTOVANJE	Načrtovanje izvidniških nalog	DL	-	X	X
	Načrtovanje obveščevalnih nalog	DL	X	X	X
	Načrtovanje drugih nalog	DL	X	X	X
ZBIRANJE	Zbiranje obveščevalnih informacij:	DA	X	X	X
	– javni viri	DA	X	X	X
	– človeški viri	DA	-	X	X
	– prestrazanje signalov	DA	X	X	X
	– slikovni podatki	DL	X	X	X
	Izmenjava	DL	X	X	X
ANALIZIRANJE	Ocenjevanje podatkov in informacij	DA	X	X	X
	Analiziranje podatkov	DA	X	X	X
POSREDOVANJE	Posredovanje obveščevalnih produktov uporabnikom SV	DA	X	X	X
	Posredovanje obv. produktov OVS	DL	X	X	X
USPOSABLJANJE	Osnovna vojaška usposabljanja J/G/S-2	DL	X	X	X
	Specialistična usposabljanja J/G/S-2	DL	X	X	-
	Usposabljanja za tuji jezik J/G/S-2	DL	X	-	-
	Usposabljanje prip. SV	DL	X	X	X
	Usposabljanje prip. SV za zagotavljanje funkcij	DL	X	X	X
	Usposabljanje prip. SV – ob odhodih v tujino	DA	X	X	X
RAZVOJ IN OPREMLJANJE	Izdelava študij	NE	X	X	-
	Opremljanje s sodobno opremo	DL	X	X	X
	Upravljanje kadrov	DL	X	X	X

Legenda: STR – Strateška raven, OPT – Operativna raven, TKT – Taktična raven

NE – se ne izvaja

DA – se v celoti izvaja

DL – se delno izvaja

macije za uresničitev *kritičnih informacijskih zahtev* (angl. Commander's Critical Information Requirement - CCIR) in *prednostnih obveščevalnih zahtev* (angl. Priority Information Requirements - PIR) ter podpira bojno delovanje.

V asimetričnem bojišču to v praksi navadno pomeni, da se poveljniki enot osredotočajo predvsem na cilje, za katere imajo kakovostne in zadostne obveščevalne informacije<sup>4</sup>.

Pri analiziranju procesov dela obveščevalno-varnostne dejavnosti na obrambnem področju zasledimo za obveščevalno-varnostno dejavnost specifično sistematičnost dela v okviru obveščevalnega ciklusa. Po večini gre vedno za usmerjanje tako imenovanih naročnikov, na podlagi česar se začeta izvajati načrtovanje in zbiranje vseh ustreznih podatkov in informacij, vezanih na zahtevo, poznejše obdelovanje ali analiziranje ter posredovanje uporabnih podatkov (tabela 1).

Na podlagi procesov dela obveščevalno-varnostne dejavnosti smo opredelili izvajanje izhajajočih nalog na vseh ravneh, pri čemer smo dodatno vključili procese usposabljanja ter razvoja in opremljanja (tabela 1).

#### 4 ANALIZA DELOVANJA OBVEŠČEVALNO-VARNOSTNE DEJAVNOSTI

V naši analizi smo najprej izvedli kvalitativno analizo načinov delovanja obveščevalno-varnostne dejavnosti<sup>5</sup>. S pomočjo strokovnjakov smo določili merila, jih ovrednotili in upoštevali vse do zdaj navedene elemente za delovanje obveščevalno-varnostne dejavnosti v različnih organizacijskih oblikah za izvajanje vseh procesov v dejavnosti v realnem času.

Najpomembnejše oziroma najbolj zelene lastnosti obveščevalno-varnostne dejavnosti so po pričakovanju strokovnjakov učinkovito poveljevanje in kontrola (PINK) ter zakonska urejenost, saj je ta dejavnost ves čas pod nadzorom notranjih in zunanjih, torej civilnih, nadzornikov in jo spremljata laična in strokovna javnost. Sem spadajo še učinkovito delovanje v najzahtevnejših razmerah (MOM), ustrezni in razpoložljivi kadrovski viri ter sistemska povezanost (SOSA) *centrov znanja*.

Merila za primerjavo različic, skupaj s kriteriji, ki so jih posredovali strokovnjaki, pokažejo najpomembnejše lastnosti in zahteve do modelov obveščevalno-varnostne dejavnosti.

Strokovnjake smo izbrali med pripadniki Slovenske vojske, pa tudi zavezniških sil. Vsi imajo izkušnje iz dela na obveščevalno-varnostnem področju, iz dela v enotah, poveljstvih oboroženih sil ter MOM.

Posebno pozornost smo namenili usklajenemu delovanju in odzivnosti, pri čemer smo upoštevali značilnosti in prednosti, pomembne za posamezno različico (tabela 2, slika 2).

<sup>4</sup> *Menimo sicer, da je lahko tovrsten način pri tako imenovanih "anti head" operacijah, če je izveden površno, sporen in kontraproduktiven, saj lahko še bolj podžge uporniško delovanje. To se vidi tudi na primeru prenosa strategije generala Petrausa iz Iraka v Afganistan, kjer ni dosegla zelenih učinkov (glej tudi Svete, Guštin, Črnčec, 2011).*

<sup>5</sup> *Celotno poročilo o izvedeni kvalitativni analizi je zaradi obsega na voljo v arhivu avtorjev.*

S kvalitativno analizo smo med seboj primerjali in analizirali štiri izbrane različice. Posamezna različica pomeni način organiziranja in izvajanja procesov obveščevalno-varnostne dejavnosti. Tako smo poimenovali tudi posamezne različice oziroma modele.

Prvi model, poimenovan EBAO, pomeni, da je obveščevalno-varnostna dejavnost organizirana tako, da predvsem podpira operacije, ki temeljijo na učinkih. Model omogoča zelo dobro vključevanje značilnih nevojaških struktur (civilne institucije, nevladne organizacije, UN), kar je s stališča poveljevanja in kontrole (PINK) slabo. Poveljujoči in drugi kritiki tega modela poudarjajo predvsem nerešeno vprašanje usklajevanja in nadzora med vojaškimi in civilnimi organizacijami.

Drugi model je model, ki je začel delovati leta 1991 in je v RS prevladoval do leta 2000. Pripadniki VOMO v poveljstvih TO in po novem ZOBR od leta 1995 pripadniki OVS v poveljstvih SV so skupaj z obveščevalnimi pripadniki SV predstavljali celovit sistem obveščevalno-varnostne dejavnosti. Ta je omogočal centralizirano vodenje in decentralizirano podporo. Za tedanje razmere je sistem ustrezno podpiral obveščevalno-varnostno dejavnost. Imel je nekaj izredno pozitivnih rezultatov v obliki hitrosti prenosa pomembnih informacij, ni pa omogočal celovitega vodenja, saj so razen obveščevalnega osebja v TO oziroma SV drugi pripadniki pripadali VOMO oziroma OVS. Pomanjkljivost sta pomenila poveljevanje in kontrola, ker poveljniki niso imeli popolnega nadzora nad obveščevalno-varnostnim osebjem in so bili omejeni pri zahtevah kritičnih informacijskih zahtev in prednostnih obveščevalnih zahtev. Tedanji sistem se je tudi sicer zaradi osamosvojitve leta 1991 in vojne v Republiki Hrvaški ter Bosni in Hercegovini bolj posvečal varnostni in protiobveščevalni dejavnosti.

Tretji model, poimenovan celovit pristop, se trenutno uporablja v strateških in operativnih poveljstvih Nata. Pri tem modelu je obveščevalno-varnostna dejavnost v stebru razvoja znanja (KD). Klasične vojaške strukture s funkcijskimi področji (S/G/J) ni. Po dveletnem testiranju je prav zaradi združevanja informacij v celovito znanje, posredovano poveljujočim, koncept prešel v doktrino razvoja znanja. Razpršenost obveščevalno-varnostne dejavnosti med razvojem znanja in operativnim delom v posameznih primerih pomeni težavo pri PINK, predvsem pa pri usklajevanju končnih informacij<sup>6</sup>.

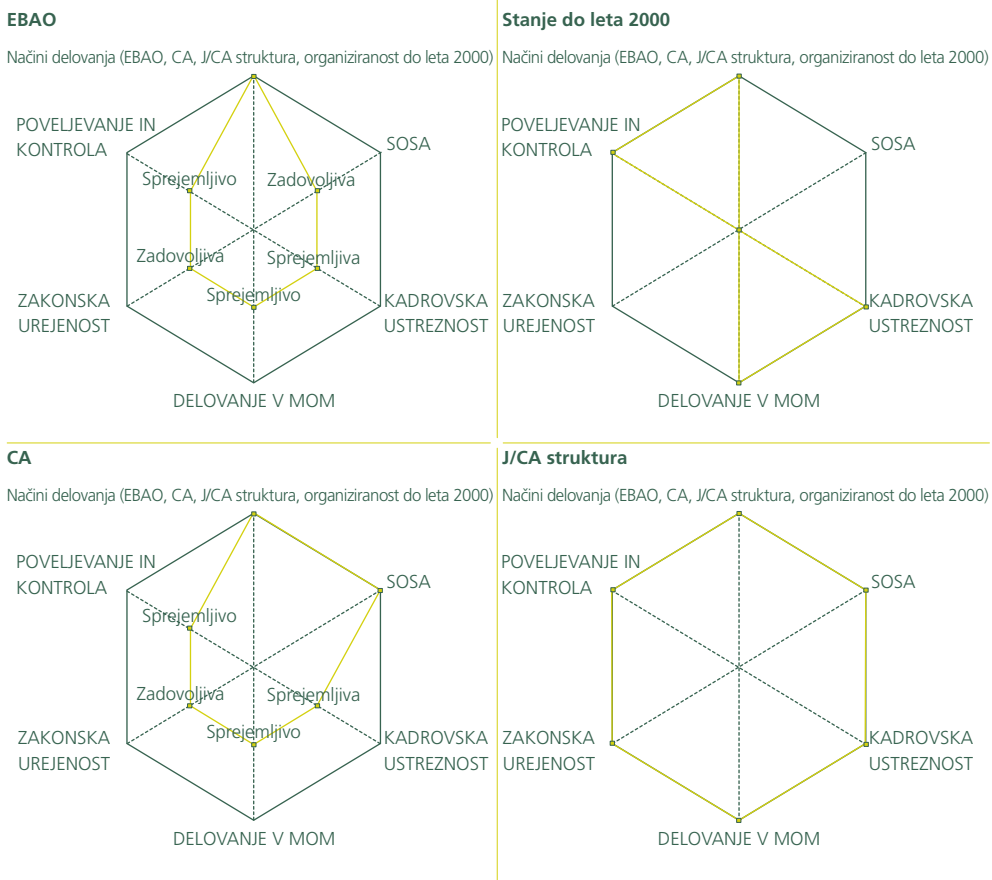
Četrti model, ki je poimenovan J-struktura, uporablja in upošteva vse prednosti celovitega pristopa. To je model, ki se »ponovno« vpeljuje v operativnih poveljstvih Nata, v katerih se uveljavlja štabno procesno naravnana struktura s funkcijskimi področji (J), ki vključuje vsa nova spoznanja razvoja znanja in jih nadgrajuje z upravljanjem znanja (angl. knowledge management – KM).

<sup>6</sup> *Zelo podoben model je bil vzpostavljen v sistemu vodenja operacije Združeni zaščitnik (angl. Unified Protection). Prav zaradi težav pri PINK so zaradi nujnosti posredovanja ključnih informacij, predvsem zaradi zaščite civilnega prebivalstva, namensko kršili linijo PINK (razgovor z generalpodpolkovnikom Charles Bouchardom, oktober 2011).*

**Tabela 2:**  
Kvalitativna  
analiza  
delovanja  
obveščevalno-  
varnostne  
dejavnosti  
Vir: Henigman,  
Rode, metoda  
DEXI, 2012.

Različica	EBAO	Stanje do leta 2000	CA	J/CA struktura
Hitrost delovanja PINK	Zadovoljiva	Hitra	Zadovoljiva	Hitra
Učinkovitost PINK	Zadovoljiva	Dobra	Zadovoljiva	Dobra
Sprejemljivost PINK	Nesprejemljiv	Delno sprejemljiv	Delno sprejemljiv	Sprejemljiv
Nacionalna zakonodaja	Podpira z omejitvami	Podpira	Podpira z omejitvami	Podpira
STANAG-i	Podpirajo	Ne podpirajo	Podpirajo	Podpirajo
Bojno delovanje (FSO)	Možno z omejitvami	Možno delovanje	Možno z omejitvami	Možno delovanje
Delovanje v SASO	Možno delovanje	Možno z omejitvami	Možno delovanje	Možno z omejitvami
Usposobljenost	Sprejemljiva	Dobra	Sprejemljiva	Dobra
Razpoložljivost	Sprejemljiva	Dobra	Sprejemljiva	Dobra
Motiviranost	Dobra	Dobra	Dobra	Dobra
SOSA	Zadovoljiva	Nezadovoljiva	Dobra	Dobra

**Slika 2:**  
Primerjava  
ustreznosti  
načina delovanja  
obveščevalno-  
varnostne  
dejavnosti  
Vir: Henigman,  
Rode, metoda  
DEXI, 2012.



## 5 RAZPRAVA

V našem raziskovanju govorimo o obveščevalno-varnostni dejavnosti na obrambnem področju, na katerem prednost izhaja iz pravočasnih, točnih in natančnih informacij, ki jih potrebujejo vlada, minister za obrambo in poveljujoči. Na obrambnem področju je ta prednost še posebno pomembna, saj so tu vložki zelo visoki – navadno človeška življenja. Bistvo je torej v organiziranju za pravočasno posredovanje ključnih uporabnih podatkov, saj ti lahko postanejo pomembne informacije za odločanje (Podbregar, Mulej, Pečan, Podbregar, Ivanuša, 2010).

Konkurenčnosti tu sicer ni, saj so zakonsko določene pristojnosti jasno razmejene, čeprav se med seboj v posameznih elementih dotikajo in celo dopolnjujejo. Čeprav so temeljne značilnosti delovanja vseh organizacij kakovost in izboljšave – v obveščevalno-varnostni dejavnosti to predstavlja načrtovanje izboljšav, izvajanje ukrepov, spremljanje učinkov in analizo.

Proaktivnost, sposobnost predvidevanja dogodkov in razvoja posameznih dejanj ter celovito obveščanje poveljujočih so za take nosilce ključni.

Lahko rečemo, da so postavljanje kritičnih informacijskih zahtev in prednostnih obveščevalnih zahtev poveljujočih ter v zvezi s tem ustrezno načrtovanje obveščevalno-varnostne dejavnosti, strokovnost in usposobljenost kadra ter posredovanje in dostopnost do informacij najnujnejši, zato bomo tem področjem namenili največ pozornosti<sup>7</sup>.

Načrtovanje in izvajanje obveščevalnih aktivnosti, nadzora in izvidovanja (angl. Intelligence, surveillance and reconnaissance – ISR) sta ključna elementa uspešnega zagotavljanja obveščevalno-varnostne dejavnosti. Če poveljujoči postavijo ustrezne kritične informacijske zahteve in prednostne obveščevalne zahteve, se načrtovalci obveščevalno-varnostne dejavnosti lažje osredotočijo na načrtovanje angažiranja zmogljivosti. Na obveščevalnem področju to pomeni predvsem angažiranje obveščevalnih disciplin z izvidniškim delovanjem (angl. Reconnaissance & Surveillance) s človeškimi viri (angl. Human Intelligence – HUMINT), iz javno dostopnih virov (angl. Open Source Intelligence – OSINT), iz slikovnih virov (angl. Imaginary Intelligence) in s prestrezanjem signalov (angl. Signal Intelligence (SIGINT)). Le redke izmed držav Nata premorejo zmogljivosti za angažiranje (in neprestano delovanje) vseh teh obveščevalnih disciplin, saj je to zelo zahtevno.

Obveščevalno-varnostna dejavnost je posebno področje, na katerem je stopnja pričakovanja vodilnih političnih in vojaških poveljnikov izredno visoka. Posredovane informacije jim služijo kot glavno izhodišče pred načrtovanjem in izvajanjem kakršnih koli aktivnosti. Izredno redki so primeri, ko je osnovni podatek že lahko uporabna

<sup>7</sup> *NATO Military Authorities Intelligence Coordination Group (NMAICG) je Natovo telo, ki določa pomanjkljivosti oz. prioriteto v obveščevalno-varnostni dejavnosti. V letih 2011 in 2012 določa ta odbor načrtovanju zbiranja, kadrom in interoperabilnosti (povezljivosti) sistemov obveščevalno-varnostne dejavnosti najvišjo prioriteto.*

informacija; velika večina predstavlja surove podatke brez posebne vrednosti, dokler jih analitiki s profesionalnim znanjem ne proučijo, analizirajo in posredujejo v uporabno informacijo. To pa zahteva čas ter profesionalno in strokovno osebje. Prav osebje predstavlja svojevrsten izziv, saj večina sistemov potrebuje izredno veliko časa za vzpostavitev takih zmogljivosti. Razvoj informatike z računalniškimi analitičnimi aplikacijami in drugimi orodji delo obveščevalno-varnostne dejavnosti močno olajšuje, vendar človekove vloge in pomena ne more zamenjati.

Obrambni sistemi držav imajo različne oblike ureditve delovanja obveščevalno-varnostne dejavnosti; nekeje je bolj usmerjeno v vojaški del, drugje bolj v upravni – navadno je to odvisno od zgodovinske organiziranosti in angažiranja držav v MOM ter aktivne vloge v Natu. Slovenski sistem obveščevalno-varnostne dejavnosti je določen v ZOBR, v katerem je nedvoumno zapisano, da je Obveščevalno varnostna služba nosilec obveščevalno-varnostne dejavnosti, razen za izvajanje štabno varnostnih nalog in dela usmerjanja vojaške policije, kjer je to z novelo ZOBR iz 2004 prepuščeno štabnovarnostnim organov v SV. Morda je zgodovinsko dejstvo organiziranosti te dejavnosti pred letom 1991, ko so bili nosilci obveščevalno-varnostne dejavnosti umeščeni v vojaški del, pomenilo odklonilni odnos pri graditvi nove tovrstne dejavnosti. Čeprav se je sistem izrazito pozitivno uveljavil v obdobju slovenskih osamosvojitvenih procesov in pozneje, bi ga morali ob novih izzivih RS izboljšati.

Leta 2008 je bil pripravljen predlog akta o integraciji obveščevalno-varnostnega sistema Ministrstva za obrambo, ki je predvidel integracijo posameznih procesov obveščevalne, protiobveščevalne ter varnostne dejavnosti v OVS in SV. Oddelek za obveščevalne analize, ki je začel aktivno delovati v letih 2004/2005, je bil prvi integracijski element na MO in v SV in je po mnenju tedanjih vodij kljub začetnim izzivom izrazito pozitivno prispeval h končnim produktom. Bil je prvi uspešen poskus skupnega integrativnega delovanja pripadnikov SV in OVS. Z novim vodstvom na MO in v SV predlog nadaljevanja integracije ni bil sprejet. Z ukinitvijo Oddelka za obveščevalne analize leta 2010 je bilo vzpostavljeno stanje pred letom 2004 (Grozde, 2011, str. 8).

Zaposleni v obveščevalno-varnostni dejavnosti so v svojem delu vedno specifični. Predvsem bojazen, da bo nekdo zlorabil informacije ali da bo prišlo do njihove odtujitve, največkrat pripelje odgovorne, da produktom določajo nesorazmerno visoke stopnje tajnosti, zaradi česar je njihova uporaba omejena in časovno pozna, kar jih uvršča v neuporabne (zastarele) podatke. V okviru celovitega pristopa je prav zaradi holističnega pristopa ključno, da se celovite informacije čim prej posredujejo končnim uporabnikom.

Razvoj znanja predstavlja revolucionarno miselnost v delu, ki določa potrebe obveščevalno-varnostne dejavnosti po hitrih spremembah v mišljenju. Ustrezni procesi, informacije in podatki že obstajajo v številnih primerih, ki podpirajo ustrezne odločitve. Težava je z »izoliranimi informacijami«, ki so na različnih mestih in niso ustrezno zbrane ter ovrednotene na enem mestu. *»Imamo več kot 100.000 ljudi, ki odlično razumejo situacijo, toda če tega ne zmoremo deliti z drugimi, je*



*delo brezpredmetno.*» (David Rodriquez, generalpodpolkovnik, poveljnik ISAF Združenega poveljstva, 2010). Pogosto je končni uporabnik, navadno poveljnik, prepuščen trenutno razpoložljivim podatkom in informacijam pri sprejemanju odločitev. Razvoj znanja z novim načinom in sistemom ne nadomešča uveljavljenih odločitev podpornih procesov in mehanizmov, jih pa z novim načinom razmišljanja in skupnega povezovanja močno izboljšuje.

V okviru načrtovanja obveščevalno-varnostne dejavnosti je treba posebno pozornost nameniti morebitnim krizam in pripraviti realne scenarije razvoja kriz, načrtovanja in izdelave modelov. Treba je prepoznavati in analizirati tveganja ter nevarnosti, proučevati modele, po katerih so se določene krizne situacije zgodile, in poznati razmere o drugih državah.

### Sklep in priporočila

Obveščevalno-varnostna dejavnost je temelj za učinkovito uresničevanje poslanstva SV. Zagotavlja ključne informacije za načrtovanje, odločanje in delovanje SV. Obsega ukrepe, postopke in aktivnosti, ki se izvajajo, da bi poznali in razumeli sovražnikove dejavnosti, zmogljivosti in namere ter zemljišče in vreme. Zaradi potreb po prilagajanju za obveščevalno-varnostno dejavnost to pomeni stalno spremljanje stanja ter načrtovanje izboljšane, kakovostnejšega pridobivanja, analiziranja, obdelave in posredovanja podatkov.

Obveščevalno-varnostna dejavnost s ciljnim pridobivanjem podatkov po končanem analitičnem procesu zagotavlja poveljujočim ključno podporo načrtovanja nadaljnjih aktivnosti in tako izpolnjuje svoje poslanstvo: posredovanje predvidevanja za kritično ukrepanje. Seveda nihče ne pozna prihodnosti, lahko pa na podlagi preverjenih in novih metod, upoštevanja zadostne in potrebne celovitosti ter systemskega razmišljanja dvignemo napovedno moč oziroma predvidevanje na višjo raven.

Organizacijska struktura obveščevalno-varnostne dejavnosti mora zagotavljati sprotno prilagajanje na nastale krize. Sistem mora biti dovolj kadrovsko podprt za realizacijo vseh zahtevanih procesov. Sistemizacija delovnih mest (angl. peace establishment) mora predvideti dovolj osebja za zmožnost interdisciplinarnega delovanja, ki se bo ob nastalih situacijah lahko sproti prilagajal pripravi in izdelavi najbolj zahtevnih produktov.

Iz opisa poslovnih procesov na posameznem področju obveščevalno-varnostne dejavnosti kot tudi iz opisa del in nalog posameznih dolžnosti mora biti razvidno, kateri osnovno ter specialistično znanje mora oseba na taki dolžnosti izpolnjevati. Ključno je, da menedžment poskrbi za profesionalni razvoj zaposlenih v obveščevalno-varnostni dejavnosti.

Naloge obveščevalno-varnostne dejavnosti niso opredeljene na enem mestu (več različnih pravnih norm), normativni dokumenti so zastareli in niso prilagojeni spremembam v predpisih in doktrinarnih dokumentih.

Razvoj in graditev zmogljivosti sistema obveščevalno-varnostne dejavnosti SV morata potekati s postopnim tehnološkim opremljanjem in sistematičnim usposabljanjem kadrov ter učinkovito in racionalno uporabo razpoložljivih virov.

Zavezanost boju proti terorizmu, delovanje v Natovih operacijah in dosedanje izkušnje določajo, da obveščevalno-varnostna dejavnost s svojimi produkti ostaja na osrednjem mestu.

Profesionalni izziv sodobne obveščevalno-varnostne dejavnosti je v znanosti, razvoju kadra, izobraževanju in usposabljanju, sistemski analizi ob uporabi umetne inteligence, integraciji procesov ter izmenjavi podatkov in informacij.

Najustreznejša sta »klasična« štabna organiziranost in način dela z ustrezno integracijo procesov ob upoštevanju vseh domen PMESII in izdatni podpori analitičnih orodij pri sistemski analizi. Obveščevalno-varnostna dejavnost mora biti elastična predvsem v proaktivnem smislu. Večjo pozornost smo namenili predvsem operacijam, v katerih so strokovnjaki dali veliko težo učinkovitosti delovanja v najtežjih razmerah, to je krizi (vojni) oziroma delovanju v celotnem spektru.

Naša priporočila se navezujejo na sistemski del organizacije oziroma zakonodaje, kadrov in izobraževanja, dostopanja do informacij in graditve dodatnih zmogljivosti.

Obveščevalno-varnostno dejavnost na obrambnem področju bi bilo treba preoblikovati. Iz klasične štabno funkcijske organiziranosti mora preiti v procesno organiziranost, ki bo v novi informacijski dobi omogočala prilagajanje nastalim razmeram, z odzivnostjo in elastičnostjo. Obveščevalno-varnostna dejavnost bi se morala organizirati tako, da bi lahko sledila zahtevam izvajanja obveščevalnega ciklusa od začetka do konca. Jasno bi bilo treba določiti vsa delovna mesta, ki podpirajo posamezne procese dela obveščevalno-varnostne dejavnosti.

Nadaljevati bi bilo treba z integracijo procesov obveščevalno-varnostne dejavnosti, ki bo omogočala učinkovito obveščevalno, protiobveščevalno in varnostno dejavnost na strateški, operativni in taktični ravni v realnem času. Treba bi bilo spremeniti in dopolniti ZOBR, ki bi kot ključni normativni akt določal nosilca obveščevalno-varnostne dejavnosti tudi v SV, ki bi postala Obrambno vojaška obveščevalna služba – OVOS. OVS in obveščevalno-varnostni sektor na GŠSV bi se pri tem integrirala. Integracija bi morala vsebovati sistemski in procesni del. Bilo bi sicer logično, da nekateri deli, kot so tajni in prikriti ukrepi iz protiobveščevalne ter varnostne dejavnosti, kot tudi posebne metode dela iz obveščevalne dejavnosti ostanejo izključno v OVS. Ne bi pa smelo biti nobenih ovir pri integraciji na področju analitičnih, vojaških varnostnih in protiobveščevalnih zadev. Zaradi transparentnosti in hkratnega nadzora nad izvajanjem zakonsko določenih tajnih in prikritih metod dela bi takšno integrirano službo še vedno vodil generalni direktor kot civilna oseba, njegov namestnik, pa bi moral biti visok častnik ali celo general. Tako bi bila vključena obrambni in vojaški del, obrambni sistem pa bi dobil sistem

obveščevalno-varnostne dejavnosti, ki bi poleg vseh zahtevanih pogojev izpolnjevala tudi racionalizacijo in optimizacijo kadrovskih virov.

Težiti je treba k dodatnemu interdisciplinarnemu znanju z ustrezno podporo in uporabo informacijske tehnologije, zato bi se morali organizirati specifično specialistično izobraževanje in izpopolnjevanje. Glede na procese dela in opise del in nalog posameznih dolžnosti bi morali pripraviti standardizacijo usposabljanj v obveščevalno-varnostni dejavnosti. Menedžment bi pripravil načrt usposabljanj in izobraževanj za pripadnike OVS in SV za različne ravni in dolžnosti.

Za enotno vodenje integrirane obveščevalno-varnostne dejavnosti bi morali izdelati skupno doktrino, taktično-tehnične postopke in standardne operativne postopke, da bi se poenotilo delovanje integrirane obrambne obveščevalno-varnostne dejavnosti.

Tehnične rešitve, ki podpirajo sodelovanje in izmenjavo ter lahek dostop do informacij, morajo slediti novim zahtevam. Razvoj in uporabnost specifičnih orodij za uporabo v obveščevalno-varnostni dejavnosti bi morala ostati bistvena cilja za pripravo celovitih produktov v prihodnjem obdobju, analizirane in pripravljene informacije pa morajo kot produkt znanja biti dostopne upravičenim uporabnikom.

Vzpostaviti bi bilo treba tak sistem posredovanja informacij (angl. info sharing), da bi bile po sistemu potrebe po vedenju (angl. need to know) obveščevalno-varnostne informacije vidne (angl. visible), dostopne (angl. accessible), razumljive (angl. understandable) in z izraženim koeficientom verjetnosti (angl. trustable) kot enim bistvenih elementov obveščevalno-varnostne dejavnosti oziroma napovedovanja. Dostopnost do informacij bi se morala dodatno zagotoviti z ustreznimi elementi dostopanja in varovanja, in sicer s pristopnim nadzorom (angl. access control), identifikacijo (angl. identifying management), privilegiranim položajem (angl. privilege management), združevanjem in povezovanjem (angl. credential management). S takim sistemom bi dosegli poenotenje, celovitost, dostopnost in širjenje informacij.

Nadaljevati bi bilo treba začete projekte graditve zmogljivosti IMINT za zagotovitev taktičnih obveščevalno-varnostnih podatkov v realnem času. Kljub trenutno ne najboljšim časom take zmogljivosti maksimalno pripomorejo k varovanju življenj naših vojakov v MOM, hkrati pa bi jih lahko uporabljali tudi kot pomoč ob naravnih nesrečah, kot so požar, potres in poplave v RS.

## Literatura

1. *AJP-2.0, Skupna zavezniška obveščevalna, protiobveščevalna in varnostna doktrina, STANAG 2190, 2003, Bruselj, Nato Standardisation Agency.*
2. *Batschelet, A. W., 2002. Effects-Based Operations: A New Operational Model? Strategy Research Project, U.S. Army War College.*
3. *Bi-Strategic Command Knowledge Development (Pre-Doctrinal Handbook, Final Draft, November 2010. Allied Command for Transformation, SHAPE.*
4. *Cazamea, J., 2010. Challenges and Effects from Knowledge Management (briefing). SHAPE.*

5. Furlan, B., Rečnik D., Vrabič, R., Maraš, V., Cerkovnik, J., Špur, B., Šonc, M., Tušak, M., Ivanuša, M., Gorjup, B., Kojadin, M., Lasič, K., Unger, M., 2006. *Vojaška doktrina. Poveljstvo za doktrino, razvoj, izobraževanje in usposabljanje*. Ljubljana, Defensor d. o. o.
6. Grozde, J., 2011. *Reorganizacija obrambne obveščevalno-varnostne dejavnosti MO RS 2000–2010, Seminarska naloga pri predmetu nacionalna varnost, Generalštabni tečaj, Maribor*.
7. Håkon, T., 2006. *A State Space Formulation for Effects Based Operations*. Nato C3 Agency, Haag, Netherlands.
8. Henigman, Ž., Rode, A., 2010. *ISTAR – Slovenska vojska in zoperstavljanje terorizmu: [predavanje na mednarodni regionalni konferenci Izzivi zoperstavljanja terorizmu v regiji jugovzhodne Evrope, Maribor]*.
9. Ivanuša, T., Podbregar, I., Pečan, S., Mulej, M., Tičar, B., Ivanuša, T. (ur.), Podbregar, I. (ur.), 2009. *Pandemija: upravljanje in obvladovanje omejitve gibanja: učbenik*. Ljubljana: Zavod za varnostne strategije pri Univerzi Maribor.
10. Kuehreiber-Fritz, F., 2011. *Knowledge management within Comprehensive Approach (briefing)*. Joint Force Command Brunssum.
11. Mattis, J. N., 2008. *USJFCOM Commander's Guidance for Effects-based Operations. Parameters, Vol. XXXVIII, Spring 2008. pp. 18–25*.
12. Midan, Christophe, *Implementation of NATO EBAO Doctrine and its effects on operational Staff's structure and functions. Strategic Impact 4/2009, pages 39–54*.
13. Mitchel, W., 2008. *Comprehensive Approach Capacity Building: Implementing the Effects Based Approach to Military Operations, Institute for Leadership and Organisation, Faculty of Military Psychology, Leadership and Pedagogy, Royal Danish Defence College, Copenhagen*.
14. *Odredba o izvajanju nalog organa, pristojnega za obveščevalno podporo poveljevanju in vodenju ter za izvajanje štabno varnostnih nalog v Slovenski vojski (št. 017-06-10/2000-2, z dne 8. 9. 2000)*.
15. Podbregar, I., Mulej, M., Pečan, S., Podbregar, N. in Ivanuša, T., 2010. *Informacije kot "bojna" podpora kriznemu odločanju, krizni komunikaciji in delovanju*. Zavod za varnostne strategije pri Univerzi Maribor. Ljubljana.
16. Vego, N. M., 2006. *Effects-Based Operations: A Critique. Joint Force Quaterly Issue 41, str. 51–75*.
17. Ripier, K. P., 2009. *EBO There Was No Baby in the Bathwater. Joint Force Quaterly Issue 52, str. 82–85*.
18. *Resolucija o splošnem dolgoročnem programu razvoja in opremljanja Slovenske vojske do leta 2025 (ReSDPRO SV 2025), 2010. Uradni list Republike Slovenije, številka 99/2010, z dne 7. 12. 2010*.
19. *Srednjeročni obrambni program 2005–2010, MO RS, šifra 802-00-1/2004-69, z dne 22. 6. 2005*.
20. *Srednjeročni obrambni program 2007–2012, MO RS, šifra 803-2/2006-58, z dne 27. 11. 2006*.
21. Svete, U., Guštin, D., Črnčec, D., 2011. *Asimetrija in nacionalna varnost: od zgodovinskih izkušenj do sodobnih izzivov*. Knjižnica Jurija Vege. Ljubljana: Defensor.
22. *Uredba o obveščevalno-varnostni službi Ministrstva za obrambo, Uradni list RS, št. 89/04*.
23. *Zakon o obrambi – ZOb, Zakon o spremembah in dopolnitvah Zakona o obrambi – ZObr-D (Uradni list RS, št. 40/04, z dne 20. 4. 2004)*.
24. Zuna, J., 2010. *Perspectives of EBO/EBAO and its relationship to comprehensive approach. Defence & Strategy, University of Defence Czech Republic*.