Anže Rode,
Lojze Pavič,
Rok Ravnak

DOI: 10.2478/cmc-2023-0003

# VOJAŠKA OBVEŠČEVALNA DEJAVNOST – POGLED V PRIHODNOST V LUČI VOJNE V UKRAJINI

# MILITARY INTELLIGENCE - A VIEW INTO THE FUTURE IN THE LIGHT OF THE WAR IN UKRAINE

**Povzetek** Vojaška obveščevalna dejavnost je eden izmed pomembnejših dejavnikov za uspešno izvajanje bojevanja na vseh ravneh. V današnjem kompleksnem in hitro spreminjajočem se varnostnem okolju je še toliko pomembnejša. Vojna v Ukrajini je znova pokazala, da je pravočasna in točna obveščevalna priprava odločilna za doseganje prevlade na bojišču, še posebej, če je razmerje sil med nasprotnikoma izrazito neenako. V prispevku sta predstavljena pomen te dejavnosti in pregled nekaterih tujih struktur na področju vojaške obveščevalne dejavnosti z namenom iskanja primernejše strukture v obrambnem sistemu Republike Slovenije.

**Ključne besede** ***Vojaška obveščevalna dejavnost, obveščevalna služba, obveščevalne zvrsti, proces štabnega dela.***

**Abstract** Military Intelligence is one of key factors that is needed for successful warfighting on all levels. It is even more important in modern complex and rapidly changing environment. Lessons learned from War in Ukraine show that timely and accurate intelligence preparation is key to achieve battlefield dominance, especially if ratio of fighting forces is fundamentally unequal. This article presents significance of military intelligence and offer insight in some foreign defense systems/ armed forces military intelligence structures in order to improve military intelligence structure in defense system of Republic of Slovenia.

**Key words** ***Military intelligence, intelligence services, intelligence disciplines, military decision making process.***

## Uvod

Varnostno okolje v svetu in Evropi se je v obdobju zadnjega leta izrazito spremenilo. Grožnje mednarodni varnosti (podnebne spremembe, terorizem, nelegalne migracije, epidemije itn.), ki so bile prisotne že prej, so ostale. Po desetletjih miru v Evropi se je z vojno v Ukrajini vrnila neposredna vojaška grožnja in ogrozila sedanjo svetovno ureditev. V mednarodnem okolju se kažejo tveganja za širjenje konflikta na druga območja, tako na območje Pacifika (Tajvan in Južnokitajsko morje) kot tudi do naše neposredne bližine (Zahodni Balkan). Svet prihodnosti bo vsaj srednjeročno prinesel več negotovosti in tveganj. Jedrske, tehnološke in ekološke grožnje ter ekonomske razmere bodo v luči geopolitičnih trenj povzročile razvoj veliko nevarnejšega sveta, kot smo ga vajeni v zadnjih desetletjih.[1]

Ker bodo ZDA svojo pozornost slej kot prej obrnile proti kitajski grožnji, bosta morali Evropa in tudi Slovenija svojo obrambo v prihodnosti še krepiti. Grožnja ekspanzijske politike avtoritarnih režimov (Rusija, Kitajska, Iran, Severna Koreja itn.) za svobodni svet je nedvomno globalna in jasno izražena, saj so tudi države, ki so bile prej zadržane pri opremljanju svojih oboroženih sil, kot sta na primer Japonska ali Nemčija, začele vlagati v prej zanemarjeno vojaško moč države (zato so tudi sprejele nove normativne podlage). Počasi in vztrajno krepijo zmogljivosti oborožitvene industrije, po kateri je veliko povpraševanje.

Čeprav Slovenija danes (še) ni neposredno vojaško ogrožena, si varnost deli z zavezniki in partnerji znotraj Evropske unije in Nata. Članstvo v Natu nam daje neprimerno večjo stopnjo varnosti, kot bi jo lahko zagotavljali sami, vendar v širši javnosti to ni prepoznano. Rusija kot aktualna kolektivna grožnja Zavezništvu zaenkrat še ne predstavlja neposredne vojaške grožnje Sloveniji, temveč neposredno ogroža partnerske in zavezniške države.

Čeprav smo del Zavezništva, smo za svojo varnost večinoma odgovorni sami. Le tako smo lahko njegov kredibilen partner (kredibilnost države poveča moč slovenske diplomacije, ki je pomemben steber obrambe majhnih držav, in posledično tudi zaupanje tujih vlagateljev v slovensko gospodarstvo). Treba se je zavedati, da ni nobene garancije, da bosta Nato in Evropska unija večna, in tako bomo morda morali nekoč za svojo varnost poskrbeti sami.

Slovenija kot majhna država ne more zagotoviti oboroženih sil z raznovrstnimi in velikimi zmogljivostmi, zato je vloga obveščevalne dejavnosti v današnji varnostni situaciji še toliko pomembnejša. Meja med mirom, izrednim stanjem in vojno je vedno bolj zabrisana, saj se hibridno vojskovanje začne izvajati že globoko v stanju (navideznega) miru, ko se proti oboroženim silam in civilnemu prebivalstvu deluje v kognitivni domeni.[2] Clark na primer navaja, da ruske oborožene sile

---

[1] *Vpogled v grožnje in tveganja je prikazan v poročilu* Eurasia Groups top risks for 2023*, natančnejši in podrobnejši vpogled pa najdemo na spletni strani WEF (World Economic Forum).*

[2] *Trenutno Nato prepoznava pet domen vojskovanja: kopno, morje, zrak, vesolje in kibernetski prostor. V literaturi se vedno bolj pojavljajo predlogi, da se doda še šesta, kognitivna domena. Kognitivno vojskovanje poskuša spremeniti dojemanje realnosti pri ljudeh, ki je temelj njihovega delovanja (Stratagem).*

hibridno vojno pojmujejo kot vojno, v kateri so vsi napori, vključno z vojaškimi operacijami, podrejeni informacijski kampanji. Zmago v taki vojni predstavlja uspešen prenos svojega svetovnega nazora in vrednot nasprotniku (Clark, 2020, str. 15).[3] Poenostavljeno to pomeni, da se s socialnimi omrežji, lažnimi novicami in usmerjenimi medijskimi prispevki poskuša spodkopati zaupanje nasprotnikovega prebivalstva v njegovo vodstvo in voljo prebivalstva do odpora.

Največje težave Slovenije pri zagotavljanju lastne obrambe se kažejo prav v kognitivni domeni. Tradicionalna dilema »masla in topov« je pri nas izrazito na strani »masla«. Slovenska javnost kljub bližini tradicionalno nestabilnega Zahodnega Balkana vojaške ogroženosti države ne zaznava in ima temu primeren odnos do svojih oboroženih sil. Če sodimo po raziskavi Eurobarometra, se zavedanje ogroženosti Slovenije kljub povečanim vojaškim grožnjam v svetu do danes ni bistveno spremenilo (Posebni Eurobarometer, 2022), saj vojaške grožnje še ni neposredno na naših mejah.[4] Vlečemo lahko vzporednice z begunsko krizo leta 2015, ko se je širša javnost grožnje zavedala šele, ko so slovenske meje prešle množice nelegalnih migrantov. Slovenska strateška kultura razumevanja oborožene sile izhaja iz izkušenj nekdanje Jugoslavije. Lahko rečemo, da se je tedanji odnos prebivalstva do Jugoslovanske ljudske armade in obveščevalnih služb prenesel tudi na Slovensko vojsko (SV) in obveščevalno dejavnost. Izogibanje vojaški službi je bilo že tedaj družbeno sprejemljivo in je tako ostalo tudi v neodvisni Sloveniji. Vojska še vedno ni prepoznana kot življenjsko pomemben družbeni podsistem,[5] ki družbi zagotavlja varnost in s tem povezano stabilnost, na podlagi katere je mogoče razvijati blagostanje vseh državljanov (Esih, 2020). Kar pa se tiče obveščevalne in varnostne dejavnosti, je ta v širši družbi deležna nezaupanja, saj je pogosto povezana z različnimi aferami.

V takih okoliščinah je še toliko pomembnejše, da se obveščevalna, protiobveščevalna in varnostna zagotovitev v obrambnem sistemu postavi tako, da bo svoje naloge učinkovito opravljala in ne bo sama sebi namen. Za najboljši odziv države na grožnje potrebujemo široko družbeno zavedanje o njih in o pomenu svojih oboroženih sil. V doseganju tega zavedanja ima obveščevalna, protiobveščevalna in varnostna dejavnost pomembno vlogo. S pravočasnim in točnim opozarjanjem na grožnje omogoči strateškemu komuniciranju (StratCom)[6] pravočasno in ustrezno pripravo

---

[3] *Informacijska kampanja Kremlja je točka osredotočenja v ruskem pristopu k hibridnemu vojskovanju (Clark, 2020, str. 10).*

[4] *Po raziskavi Eurobarometer Slovence najbolj skrbijo naraščajoči življenjski stroški (88 %), sledijo podnebne spremembe (76 %) in grožnje revščine (74 %). Širjenje vojne v Ukrajini skrbi 72 % vprašanih, medtem ko je v Evropi kot celoti glede tega zaskrbljenih 81 % vprašanih.*

[5] *Slovenska javnost sicer izkazuje visoko zaupanje v vojsko kot institucijo. Po raziskavi Valicona Ogledalo Slovenije iz oktobra 2022 (Delo, 2022) je ta na visokem šestem mestu, vendar kljub temu ni naklonjena vlaganjem v vojsko. Nekatere stranke se celo strinjajo z omejitvijo vlaganj v vojaško opremo na zahtevo pobude Glas ljudstva. Razloge (»visoka varnostna nepismenost«) dobro pojasni izjava Dr. Vladimira Prebilića v članku Večjih vlaganj v opremo in oborožitev Slovenske vojske nismo imeli že desetletje (Esih, 2020).*

[6] *StratCom v Natu pomeni »usklajeno in primerno uporabo Natovih komunikacijskih dejavnosti in zmogljivosti v podporo zavezniških politik, operacij in aktivnosti z namenom doseganja ciljev« (*NATO Strategic Communications Centre of Excellence, 2023).

odziva za javnost ter tako krepi zavedanje resnične ogroženosti države v družbi in poveča javno podporo za izvedbo nujnih obrambnih ukrepov, ki so praviloma dragi in nepriljubljeni.

Dobra obveščevalna zagotovitev omogoča zgodnje opozarjanje na grožnje in njihovo globoko poznavanje, kar omogoči racionalnejšo izrabo omejenih virov (tako civilnih kot vojaških) majhne države, kot je Slovenija, ob zoperstavljanju agresiji v vseh fazah. Da pa tako vedenje/znanje dosežemo, potrebujemo integriran obveščevalni aparat, ki je sposoben učinkovitega zbiranja informacij, obdelave in pravočasnega posredovanja relevantnih obveščevalnih podatkov do odločevalcev, čeprav je njegov kadrovski obseg zaradi demografskih značilnosti in trendov v državi omejen.

V bližnji preteklosti smo se že srečali s kriznimi razmerami (begunska kriza 2015, izbruh covida-19 in vojna v Ukrajini), ki so povzročile občutne spremembe uveljavljenega načina življenja v Republiki Sloveniji. Ob tem se lahko vprašamo, ali je naša obveščevalna skupnost take dogodke napovedala in tako odločevalcem omogočila pravočasno in ustrezno ukrepanje. V kolikor te napovedi ni bilo oziroma je odločevalci niso upoštevali, je to jasen znak, da obveščevalno-varnostni sistem v Republiki Sloveniji potrebuje nujne spremembe, saj nas v prihodnosti čakajo še hujši izzivi v mednarodnem okolju.

Britovšek in Čretnik menita, da je bil obveščevalno-varnostni sistem v Republiki Sloveniji oblikovan na podlagi vedenja oziroma znanja, ki so ga snovalci imeli v devetdesetih letih prejšnjega stoletja (Britovšek, Čretnik, 2016). Zaradi zakonskih in organizacijskih omejitev, ki izhajajo od takrat, ne ustreza več sodobnim grožnjam in tudi ne demografskim trendom. Trenutno in prihodnje stanje v varnostnem okolju zahtevata bistvene spremembe in prilagoditve celotnega obrambno-varnostnega sistema države in tudi prilagoditev njegove obveščevalne ter varnostne komponente.[7]

## 1 METODOLOŠKI PRISTOP

V tem prispevku smo se osredotočili na vojaško obveščevalno dejavnost, ki je le del celotnega obveščevalno-varnostnega sistema države in je zaradi sedanje ureditve v obrambno-varnostnem sistemu Republike Slovenije kar nekoliko prezrta.

Pri preučevanju tematike smo uporabili različne raziskovalne metode. Osrednja za umestitev področja je bila metoda analize primarnih in sekundarnih pisnih virov. Deskriptivno analizo smo uporabili pri preučevanju področja v širšem smislu, primerjalno analizo pa na primeru petih držav, za katere ugotavljamo, da so z vidika našega raziskovanja zanimive. Uporabili smo tudi metodo opazovanja z lastno udeležbo, ki se izraža z večletnimi izkušnjami na področju dela obveščevalne, protiobveščevalne in varnostne dejavnosti na taktični, operativni in strateški ravni,

[7] *Resolucija o splošnem dolgoročnem programu razvoja in opremljanja Slovenske vojske do leta 2035, 2. poglavje. Ljubljana: 2022, str. 5–7.*

tudi v mednarodnem okolju. S problematiko zagotavljanja varnosti in sprejemanjem pravih odločitev ter ob podpori obveščevalno-varnostnega sistema smo se srečevali tudi kot poveljujoči v Republiki Sloveniji ter v mednarodnih operacijah in na misijah.

Pri pripravi prispevka se moramo zavedati omejitev, ki izhajajo predvsem iz obveze zagotavljanja tajnosti podatkov. Zato smo lahko uporabili samo javno dostopne vire.

## 2 VOJAŠKA OBVEŠČEVALNA DEJAVNOST

Vojaška obveščevalna dejavnost (angl. MI, Military Intelligence) je vojaška dejavnost, ki z zbiranjem in obdelavo podatkov pomaga poveljnikom na vseh ravneh pri sprejemanju odločitev. Ta cilj doseže z zbiranjem podatkov iz vseh virov, skladno z zahtevami za izvedbo naloge. Bojno delovanje usmerja tako, da uporabnikom zagotavlja obveščevalne podatke, ki ustrezajo njihovim potrebam in zahtevam. Te so specifične glede na raven (strateška, operativna, taktična) in nalogo. Angleški izraz intelligence se lahko nanaša tudi na obveščevalni podatek. Po spletnem angleško-angleškem slovarju Oxford Reference izraz Military Intelligence pomeni »obveščevalni podatek o vsem, kar se nanaša na tujo vojaško ali z vojsko povezano situacijo ali dejavnost, ki je pomembna za načrtovanje in izvajanje vojaških operacij in aktivnosti« (Oxford Reference, 2023).

Britovšek in Čretnik poudarjata: »Vojaške obveščevalne naloge so ožji pojem in se nanašajo na zbiranje in analiziranje podatkov, ki so primarno pomembni za vojaške poveljnike in poveljstva vojaških enot oziroma so pomembni za izvajanje nalog, ki jih opravljajo oborožene sile« (Britovšek, Čretnik, 2016, str. 330). Menita, da so obveščevalne naloge »širši pojem in predstavljajo zbiranje, analiziranje in ocenjevanje podatkov o razmerah in virih ogrožanja, ki izhajajo iz tujine« (Britovšek, Čretnik, 2016, str. 329).

Pri tem moramo ločiti ravni obveščevalne dejavnosti. Te so v Natu po AAP-06 navedene tako:

– Strateška obveščevalna dejavnost kot »obveščevalna dejavnost, potrebna za oblikovanje politike in vojaško načrtovanje ter zagotavljanje indikatorjev in opozoril[8] na nacionalni in/ali mednarodni ravni«. Osredotoča se na zagotavljanje obveščevalnih podatkov o grožnjah nacionalni varnosti in o zadevah nadnacionalnega pomena. Obsega vojaške, diplomatske, politične in ekonomske aspekte (AAP-06, 2021, str. 123).
– Operativna obveščevalna dejavnost je opredeljena kot »obveščevalna dejavnost, potrebna za načrtovanje in izvajanje kampanj na operativni ravni«. Uporabljajo jo poveljniki na operativni ravni in odločevalci s specifičnim območjem odgovornosti (AAP-06, 2021, str. 95).

[8] *Indikator je podatek, ki odraža namero ali zmožnost morebitnega sovražnika, da izvede predvideno varianto delovanja ali pa je ne izvede.*

– Taktična obveščevalna dejavnost je opredeljena kot »obveščevalna dejavnost, potrebna za načrtovanje in izvajanje operacij na taktični ravni«. Običajno podpira specifične aktivnosti poveljnikov in enot na taktični ravni (AAP-06, 2021, str. 127).

Naša normativna ureditev v Zakonu o obrambi (*Zakon o obrambi, 2004, 2015, 2020)* v 1. odstavku 32. člena opredeljuje obveščevalne in protiobveščevalne naloge tako:

»Obveščevalne in protiobveščevalne naloge obsegajo zbiranje, dokumentiranje in analiziranje informacij ter podatkov, ki so pomembni za obrambne interese države oziroma varovanje takih podatkov, zlasti pa:

– ugotavljanje in ocenjevanje vojaških in politično varnostnih razmer ter vojaških zmogljivosti zunaj države, ki so posebnega pomena za varnost države;
– zbiranje in ocenjevanje podatkov o razmerah na območjih, na katerih med izpolnjevanjem obveznosti, prevzetih v mednarodnih organizacijah, oziroma pri opravljanju vojaške službe delujejo tudi pripadniki Slovenske vojske;
– odkrivanje in preprečevanje dejavnosti obveščevalnih služb vojaških organizacij ter drugih organov in organizacij, ki ogrožajo obrambne interese države, Slovensko vojsko ali ministrstvo« (*Zakon o obrambi, 2004, 2015, 2020).*

V 3. odstavku določa, da:

»Obveščevalne in protiobveščevalne ter varnostne naloge na obrambnem področju opravlja obveščevalno-varnostna služba ministrstva« (*Zakon o obrambi, 2004, 2015, 2020).*

Kot vidimo, zakon ne razlikuje med vojaškimi obveščevalnimi nalogami in obveščevalnimi nalogami oziroma dejavnostjo ter za opravljanje teh nalog na obrambnem področju določa obveščevalno-varnostno službo ministrstva. V 2. odstavku 33. člena zakona je sicer zapisano: »Podatki in informacije, zbrane pri opravljanju obveščevalnih in protiobveščevalnih ter varnostnih nalog, so podlaga za analitične in operativne ocene, opravljanje štabnih varnostnih nalog v vojski, izdelavo načrtov uporabe vojske in drugih obrambnih priprav ter za načrtovanje in izvajanje obrambnih ukrepov. S pomembnejšimi ugotovitvami obveščevalno--varnostna služba ministrstva seznanja ministra, načelnika generalštaba, predsednika vlade, predsednika republike in po odločitvi predsednika vlade druge organe« (*Zakon o obrambi, 2004, 2015, 2020).*

Če izhajamo iz pomena sistemske urejenosti in skladnosti z zakoni, potem na primer načelnik štaba generalštaba ne more neposredno razpolagati z obveščevalnimi podatki, potrebnimi za vojaško odločanje znotraj štabnega procesa dela. Te podatke pa nujno potrebuje, da bi podprl načelnika generalštaba pri sprejemanju odločitev. Taka ureditev povzroča, da se poiščejo obvodi, s čimer pa se izgublja dragocen čas za

sprejem optimalnih in pravočasnih odločitev. To potem še bolj velja za odločevalce na nižjih ravneh.

Pri tem vloga vojaških obveščevalnih organov ni ustrezno opredeljena. Ti so v resnici omejeni le na uporabo izdelkov obveščevalnovarnostne službe ministrstva (v nadaljevanju OVS), do katerih morda strogo gledano niso upravičeni (predvsem na operativni in taktični ravni), saj je v skladu z 2. odstavkom 33. člena služba dolžna seznanjati s pomembnejšimi ugotovitvami v Slovenski vojski le načelnika generalštaba (*Zakon o obrambi, 2004, 2015, 2020)*.

Iz navedenega lahko sklepamo, da zakon ne razlikuje med strateško, operativno in taktično obveščevalno dejavnostjo, kar posledično omejuje vojaško obveščevalno dejavnost zlasti na taktični in tudi operativni ravni. Britovšek in Čretnik sicer navajata, da »OVS tako opravlja obveščevalne in vojaške obveščevalne naloge, vendar se nekatere vojaške obveščevalne naloge dejansko ne izvajajo v OVS, ampak v Slovenski vojski (obveščevalni in varnostni organi t. i. J/G/S-2[9] ter obveščevalno--izvidniške enote)« (Britovšek, Čretnik, 2016, str. 331). To vsekakor nakazuje na funkcionalne pomanjkljivosti sedanje zakonske ureditve vojaškega obveščevalnega področja v okviru obrambnega sistema.

Učinkovito opravljanje vojaških obveščevalnih nalog lahko namreč izvajajo le vojaške osebe, ki na podlagi svojega znanja in izkušenj razumejo, kaj je pomembno za vojaškega poveljnika. Civilne osebe, ki delujejo v obveščevalnih agencijah in službah, sicer zbirajo in obdelujejo podatke, pomembne za obrambo države, vendar niso osredotočene na konkretne obveščevalne zahteve in potrebe oboroženih sil oziroma praviloma niso usposobljene in tudi nimajo ustreznih izkušenj za zagotavljanje ustrezno interpretiranih obveščevalnih podatkov, ki bi lahko neposredno podprli poveljnike na terenu na vseh ravneh poveljevanja. Tako bo na primer analitik, ki je civilist brez vojaških izkušenj, lahko potrdil, da je most čez široko reko podrt, ne bo pa znal interpretirati, kaj to pomeni za situacijo na bojišču in kako to dejstvo izrabiti oziroma upoštevati v nadaljnjem delovanju enote. Analitik mora razumeti potrebe po informacijah, ki jih zahteva vojaški poveljnik. Te se razlikujejo od potreb političnih odločevalcev. Sicer so produkti bolj značaja »dobro je vedeti« (angl. nice to know) namesto »treba je vedeti« (angl. need to know). Zato imajo številne oborožene sile po svetu pogosto organizirane vojaške obveščevalne organe ali službe, ki neposredno podpirajo vrhovno poveljstvo oboroženih sil (generalštab ali obrambni štab) in tudi podrejene poveljnike, ki jih pretežno sestavlja vojaško osebje in jih vodijo visoki častniki ravni generala.

---

[9] *J/G/S-2 je poimenovanje za vojaški obveščevalni, protiobveščevalni in varnostni sektor štaba na različnih ravneh: S – taktična raven (bataljon in brigada), G – taktična ali operativna raven (v ZDA npr. od ravni divizije), J – operativna ali strateška raven. Od leta 2013 se v Slovenski vojski uporabljata le S-2 (taktična raven) in J-2 (operativna in strateška raven, J pomeni združevanje, npr. različnih zvrsti oboroženih sil).*

# 3 PRIMERJAVA TUJIH VOJAŠKIH OBVEŠČEVALNIH ORGANOV

## 3.1 Velika Britanija

Zelo dober primer organizacije vojaške obveščevalne službe je britanska Obrambna obveščevalna služba (angl. Defence Intelligence – DI), katere dejavnost se osredotoča na zbiranje in obdelavo obveščevalnih podatkov vojaške narave (Defence Intelligence, 2023). Njena primarna naloga je analiza obveščevalnih podatkov, pridobljenih iz različnih zvrsti (angl. all source). Njeno osebje sestavljajo tako vojaki (okoli dve tretjini osebja) kot tudi civilisti, zagotavlja pa podatke za odločevalce na ministrstvu za obrambo, oborožene sile in tudi druge vladne ustanove. To vključuje nasvete in pravočasne obveščevalne ocene, ki podpirajo odločitve o politikah, vojaške operacije in obrambne raziskave ter programe opremljanja. Od drugih britanskih obveščevalnih in varnostnih služb se razlikuje v tem, da je v sestavi vladnega organa – obrambnega ministrstva, in ni samostojna organizacija, ter da ni osredotočena na samo eno obveščevalno zvrst (kot so MI5, MI6 in GCHQ).[10] S svojimi produkti podpira tudi organe zunaj ministrstva za obrambo in mednarodne partnerje.

Načelnik obrambne obveščevalne službe (CDI – glej shemo) je praviloma general s tremi zvezdicami ali izjemoma visok civilni uradnik.[11]

Namestnik načelnika obrambne obveščevalne službe (DCDI) je po direktoratih odgovoren za obveščevalne analize in produkcijo. Zagotavlja obveščevalne ocene in strateška opozorila na več področjih (obveščevalna podpora operacij, proliferacija in nadzor oborožitve, konvencionalne vojaške zmogljivosti in tehnično vrednotenje oborožitvenih sistemov). Te ocene temeljijo na stopnjevanih podatkih, ki jih dobijo iz različnih virov (od drugih obveščevalnih agencij, vojaških zmogljivosti ISTAR, diplomatskih poročil ter različnih odprtih virov).

Vodja za kibernetsko obveščevalno dejavnost in informacijsko upravljanje (DCI3) je odgovoren za zagotavljanje specializirane obveščevalne, slikovne in geoprostorske podpore ter za usposabljanje na obveščevalnem in varnostnem področju za pripadnike oboroženih sil. Odgovoren je za dva oddelka znotraj obrambne obveščevalne službe (DI), in sicer za Združeno vojaško obveščevalno skupino (JFIG) ter za Združeno vojaško obveščevalno skupino za usposabljanje (JITG). JFIG je največja podenota v DI in je odgovorna za podporo pri zbiranju obveščevalnih podatkov v

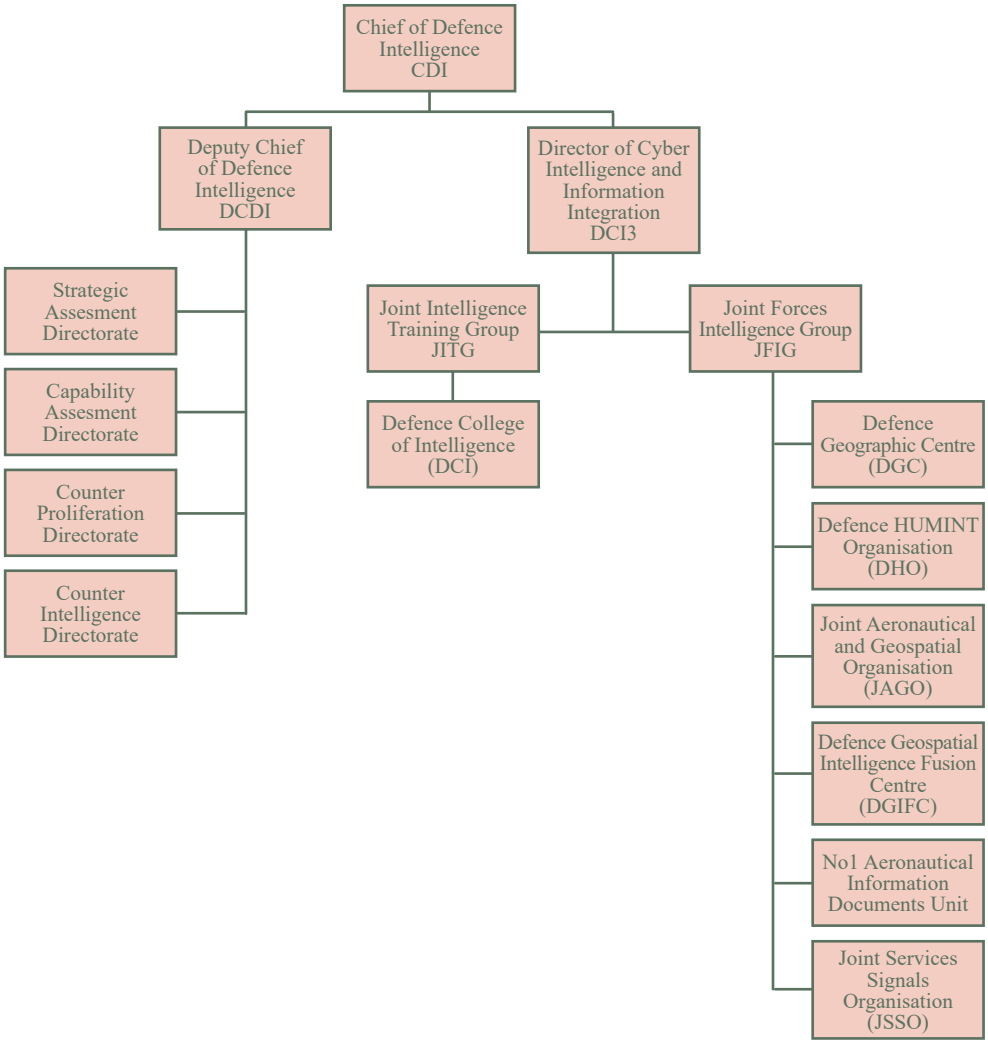
---

[10] *MI-5 – protiobveščevalna služba, MI-6 – obveščevalna služba, GCHQ – služba za obveščevalno in varnostno delovanje v elektronskem spektru in kibernetskem prostoru.*

[11] *Danes je DI umeščena v strateško poveljstvo (Strategic Command) oboroženih sil. Trenutno je o strukturi DI malo znanega v javnosti. Javno dostopni podatki so v nasprotju s tistimi izpred leta 2014 precej skopi. Opis strukture izhaja iz uradnih strani iz leta 2012, ki od leta 2014 niso več ažurirane (*https://www.gov.uk/guidance/defence-intelligence-services*). Trenutno je direktor civilni uradnik Adrian Bird, ki je prvi civilni direktor od začetka delovanja službe leta 1964 (tedaj znana kot DIS – Defence Intelligence Staff). Današnja umeščenost DI v obrambno ministrstvo je razvidna iz How Defence Works, Version 6.0, sep. 2020, notranja struktura pa ni več javno objavljena. Domnevamo, da se osnovne funkcije niso bistveno spremenile. Leta 2021 so Britanci ustanovili National Cyber Force (NCF), v katerem DI sodeluje z GCHQ. Po poročilu ISC (angl. Intelligence and Security Committee of Parliament) Annual Report 2021–2022 je NFC izvajal tudi ofenzivne kibernetske operacije. O tem tudi v Devanny, Stevens (2021).*

obveščevalnih zvrsteh HUMINT, SIGINT, GEOINT, IMINT in MASINT.[12] Deli se na več enot oziroma centrov, specializiranih za posamezne obveščevalne zvrsti (Defence Intelligence: roles, 2023). JITG zagotavlja enotno usposabljanje na področju obveščevalnih in varnostnih zadev, jezikov in fotografiranja. V njegovi sestavi je Obrambna obveščevalna akademija (Defence College of Intelligence), ki izvaja usposabljanja za pripadnike oboroženih sil, policijo, javno upravo in tudi za mednarodne partnerje (Defence Intelligence: roles, 2023).

**Slika 1:** Struktura DI pred letom 2014 (povzeto po: Defence Intelligence: roles, 2023)




[12] *Obveščevalne zvrsti delimo na HUMINT – Human Intelligence, SIGINT – Signal Intelligence, GEOINT – Geospatial Intelligence, IMINT – Imaging Intelligence in MASINT – Measurement Intelligence. Pomembna zvrst je tudi OSINT – Open Source Intelligence. V britanskem primeru sta Mi-5 in Mi-6 osredotočeni na HUMINT, GCHQ pa na SIGINT.*

Britanski model odlikuje izrazit poudarek na vojaški obveščevalni dejavnosti in temu primerna je umeščenost znotraj ministrstva za obrambo. Podatke za analize pridobiva iz »vseh virov«, tudi od drugih domačih in zavezniških obveščevalnih služb, sam pa čez JFIG usmerja zbiranje podatkov po različnih obveščevalnih zvrsteh. Vse zvrsti oboroženih sil imajo še svoje obveščevalne organe na operativni in taktični ravni. V primerjavi s slovensko OVS[13] je pri DI vojaška obveščevalna dejavnost izrazitejša, temu primerna pa je tudi sestava kadra, ki ga pretežno sestavlja vojaško osebje.

DI je v času pred začetkom vojne v Ukrajini spadala med obveščevalne službe, ki so pravilno napovedale potek dogodkov in tudi tekoče objavljale obveščevalne podatke z namenom onemogočanja ruske manipulacije javnega mnenja na Zahodu (Adam, 2022, in Bealle, 2022). Danes njihove obveščevalne ocene vojne, ki jih redno objavljajo, veljajo za zelo natančne.

## 3.2 Švica

Za vojaško obveščevalno dejavnost v švicarskih oboroženih silah se uporablja izraz vojaška obveščevalna skupnost (nem. Nachrichtendienst der Armee – NDA), ki povzema vse enote in štabne funkcije, ki izvajajo obveščevalne naloge. Strokovno jedro vojaške obveščevalne skupnosti na ravni poveljstva oboroženih sil predstavlja Vojaška obveščevalna služba (Militärischer Nachrichtendienst – MND),[14] ki je v sestavi poveljstva sil (Kommando Operationen). V strukturo spada tudi Služba za protiobveščevalno in varnostno zaščito oboroženih sil (Dienst für präventiven Schutz der Armee – DPSA),[15] zato je njihovo celotno poimenovanje Vojaška obveščevalna služba in Služba za protiobveščevalno in varnostno zaščito oboroženih sil (MND&DPSA), načelnik združene službe pa je častnik s činom brigadnega generala.

Če se osredotočimo na Vojaško obveščevalno službo – MND, ta izvaja funkcije in naloge:

– funkcija nacionalne vojaške obveščevalne službe;
– popolnjuje obveščevalne celice na operativni ravni (J-2);
– vodi vojaške obveščevalne naloge po zvrsteh oboroženih sil.

Zakonsko predpisano poslanstvo Vojaške obveščevalne skupnosti – NDA je zbiranje in vrednotenje za oborožene sile pomembnih obveščevalnih podatkov o tujini, s posebnim poudarkom na obrambi države in mirovnih operacijah v tujini.

---

[13] *Glej Britovšek, Čretnik, 2016. Avtorja na strani 335 v vseh modelih predlagata krepitev obveščevalnega sektorja Slovenske vojske, ki bi v celoti prevzel vojaške obveščevalne naloge, iz česar lahko sklepamo, da OVS ni optimalno zastavljen za izvajanje vojaške obveščevalne dejavnosti.*

[14] *V francoščini Renseignement militaire (RM), v italijanščini Servizio informazioni militare (SIM).*

[15] *V francoščini Service pour la protection preventive de l'armee (SPPA), v italijanščini Servizio per la protezione preventiva dell'esercito (SPPEs).*

Naloge Vojaške obveščevalne skupnosti obsegajo:

– pridobivanje informacij o tujini, pomembnih za oborožene sile;
– podporo vojaškemu vodstvu pri načrtovanju in vodenju operacij z informacijami o grožnjah in okolju;
– spremljanje razvoja tujih oboroženih sil in podobnih organizacij;
– ugotavljanje spoznanj, ki so pomembna za nadaljnji razvoj in usposabljanje oboroženih sil kot tudi usmerjanje temeljne pripravljenosti;
– razvoj in uveljavljanje obveščevalne doktrine oboroženih sil ter sodelovanje pri razvoju novih obveščevalnih sistemov.

Pri nalogah, ki se izvajajo na ozemlju države, Vojaška obveščevalna skupnost predstavlja del švicarske obveščevalne skupnosti, ki jo vodi Zvezna obveščevalna služba (nem. Nachrichtendienst des Bundes – NDB). Vojaška obveščevalna skupnost pri teh nalogah tesno sodeluje z zveznimi in kantonalnimi agencijami in organi, po potrebi pa tudi z mednarodnimi organi in poveljstvi (Schweitzer Armee, 2023).

Švicarska Vojaška obveščevalna služba in Služba za protiobveščevalno in varnostno zaščito oboroženih sil (MND & DPSA) sta kljub drugačni umeščenosti (v operativno poveljstvo) primerljivi z našim Sektorjem za vojaško obveščevalno, protiobveščevalno in varnostno dejavnost (SVOPVD J-2), vendar imata širša pooblastila zlasti na področju vojaške obveščevalne dejavnosti. Hkrati sta močneje vpeti v celotno obveščevalno skupnost (imata funkcijo nacionalne vojaške obveščevalne službe), ki ju usmerja in vodi nacionalna Zvezna obveščevalna služba – NDB.

## 3.3 Španija

Španske oborožene sile imajo vzpostavljen Obveščevalni center oboroženih sil (šp. El Centro de Inteligencia de las Fuerzas Armadas – CIFAS), ki z načelnikom obrambnega štaba podpira ministra za obrambo z obveščevalnimi podatki, potrebnimi za zgodnje opozarjanje o mednarodnih razmerah, ki lahko povzročijo krizo in bi lahko ogrozile nacionalno varnost. Hkrati zagotavlja obveščevalno podporo za vodenje vojaških operacij španskih oboroženih sil. Poveljnikom zvrsti svetuje pri protiobveščevalnih in varnostnih zadevah ter prispeva k svetovanju načelniku obrambnega štaba na strateški ravni vodenja vojaških operacij. Direktor Obveščevalnega centra oboroženih sil je generalmajor, ki je hkrati tudi vodja varnosti v obrambnem štabu.

Naloge:

– usmerjanje in usklajevanje zmogljivosti JISR[16] in usklajevanje obdelave informacij, pridobljenih s specifičnimi ISR-sistemi z ustreznimi službami;

[16] *Joint Intelligence, Surveillance and Reconaissance – združena obveščevalno-izvidniška dejavnost.*

– zagotovitev obveščevalnih podatkov, nujnih za razvoj aktivnosti, in ki zagotavljajo pripravljenost sil, za načelnike štabov mornarice in kopenske vojske po načelniku obrambnega štaba;
– odgovarjanje na zahtevke za informacije (ZZI) organov ministrstva za obrambo, v skladu s svojimi zmožnostmi in pooblastili;
– načrtovanje, usmerjanje in, kadar je mogoče, izvajanje geoprostorske informacijske dejavnosti na področju obrambe za potrebe vojaških operacij v sodelovanju z operativnim poveljstvom. Ustrezna organa kopenske vojske in mornarice na tem področju sta funkcijsko podrejena Obveščevalnemu centru oboroženih sil;
– v sodelovanju z Združenim štabom in združenim poveljstvom za kibernetski prostor določanje operativne zahteve za sisteme za opazovanje zemlje za optimalno učinkovitost zmogljivosti IMINT (Ministerio de Defensa, 2023).

Španski model omogoča centralizirano upravljanje vojaške obveščevalne dejavnosti v vseh zvrsteh oboroženih sil in z vojaškimi obveščevalnimi produkti podpira načelnika obrambnega štaba ter ministra kot tudi podrejene enote po operativnih poveljstvih zvrsti.

## 3.4 Irska

V Republiki Irski Direktorat za vojaško obveščevalno dejavnost (angl. Directorate of Military Intelligence – D INT ali alternativno D J2) izvaja tudi naloge nacionalne obveščevalne službe in je torej osrednja obveščevalna služba države v sestavi generalštaba obrambnih sil, in sicer v odseku za operacije (Operations Division). Načeluje mu namestnik načelnika generalštaba (Irish Defence Forces, 2023). Najpomembnejša funkcija direktorata je zgodnje opozarjanje na zunanje in notranje grožnje varnosti države in varnosti oboroženih sil (Safeguarding and Enhancing, 2023, str. 13). Njegovo osebje se rekrutira iz vseh zvrsti oboroženih sil in redno sodeluje ter se usposablja skupaj z vladnimi in nevladnimi organizacijami ter tujimi partnerskimi obveščevalnimi službami (Clonan, 2006). Službo vodi direktor (Director of Military Intelligence), ki je častnik s činom polkovnika, zaposluje pa izključno častnike in podčastnike. Direktor zagotavlja redna obveščevalna poročila pomembnim osebam, enkrat na mesec pa osebno poroča ministru za obrambo (Spyscape, 2023). Čeprav je osebje vojaško, lahko naloge opravlja tudi v civilnih oblačilih.

Služba se deli na Obrambni obveščevalni odsek (Defence Intelligence Section – DI) in Nacionalno-varnostni obveščevalni odsek (National Security Intelligence Section – NSIS).

Obrambni obveščevalni odsek zagotavlja obveščevalno podporo obrambnim silam. Spremlja politično, ekonomsko, socialno in vojaško situacijo v svetu in pripravlja obveščevalna poročila ter strateške študije za podporo operacijam. Osebje tudi poroča celotni strukturi obrambnega ministrstva. V sodelovanju z Nacionalnim policijskim uradom za varnostna preverjanja (Garda National Veting Bureau – GNVB) izvaja varnostna preverjanja pripadnikov obrambnih sil. Pomembno vlogo v

zagotavljanju obveščevalnih podatkov na misijah v tujini imajo Specialne sile (Army Ranger Wing – ARW), ki zagotavljajo prisotnost moštva iz svoje obveščevalne sekcije na operacijah. Specialne sile tudi izvajajo naloge po usmeritvah Obrambnega obveščevalnega odseka (Spyscape, 2023).

Nacionalno-varnostni obveščevalni odsek spremlja grožnje državi in obrambnim silam na področjih vohunstva, terorizma in organiziranega kriminala. Velik del njihovih nalog obsega protiobveščevalno delovanje, ukvarjajo pa se še s fizično varnostjo kritične infrastrukture. Tesno sodelujejo s Policijo (Garda Siochana), zlasti s Specialno kriminalistično policijo (Special Detective Unit – SDU) in Državno nadzorno enoto (National Surveillance Unit – NSU) pri odkrivanju potencialnih groženj varnosti državi (O'Keefffe, 2022). V Republiki Irski je sicer varnostna dejavnost prednostno v domeni policije (Garda Siochana, 2023), medtem ko vojska izvaja obveščevalno dejavnost.

Letalstvo in mornarica imata še svoji obveščevalni celici, ki zagotavljata obveščevalno podporo zvrstem. Brigade kopenske vojske imajo regionalne obveščevalne funkcijske organe (G-2), ki poročajo v obveščevalne funkcijske organe strateške ravni – J2.

Irski primer je zanimiv, ker je organiziran zelo racionalno[17] za potrebe oboroženih sil, po velikosti in zmogljivostih precej primerljive s slovenskimi (verjetno celo manj zmogljive – ob upoštevanju, da gre za nevtralno državo), ob tem pa še služi kot osrednja obveščevalna služba v državi. Po navedbah Murthaga naj bi v taki ureditvi težavo predstavljala predvsem odsotnost nadrejene povezovalne funkcije med obveščevalno varnostno strukturo policije (Garda) in J-2 na ravni vlade (Murtagh, 2017). Obveščevalna dejavnost v smislu zgodnjega opozarjanja na grožnje na Irskem velja za prvo linijo obrambe države (Safeguarding and Enhancing …, 2023, str. 13). Pri tem je obveščevalni aparat sestavljen iz izključno vojaškega osebja, ki lahko deluje tudi v civilu. Nekdaj poimenovana G-2 je med hladno vojno in krizo v Severni Irski (obdobje, poimenovano v angl. tudi The Troubles) pridobila sloves učinkovite obveščevalne službe, zlasti v sodelovanju s CIA pri spremljanju sovjetske obveščevalne dejavnosti[18] in pri samostojnem spremljanju subverzivne aktivnosti obeh sprtih strani v severnoirskem konfliktu, ta sloves pa je kljub nekaterim spodrsljajem do neke mere ohranila tudi v obdobju globalnega boja proti terorizmu (Irish Echo, 2011, in Clonan, 2006). Danes velja za eno najbolj skrivnostnih obveščevalnih služb v Evropi, jo pa trenutno verjetno kot celoten irski obrambni sistem pestita pomanjkanje sredstev in splošen občutek zanemarjanja pomena obrambe in varnosti v državi.[19]

---

[17] *Obseg je minimalen glede na potrebe (glej Safeguarding and Enhancing the Critical Capabilities of the Defence Forces Intelligence function in Ireland's National Security in the 21st century).*

[18] *Tudi v začetku vojne v Ukrajini so spremljali rusko obveščevalno dejavnost (predvsem GRU), ki ima center na ruskem veleposlaništvu v Dublinu (Gallagher, 2021).*

[19] *Zadnji primer Irke Marine Sologub, ki ji je Avstralija odpovedala vizo zaradi tveganja stikov z ruskimi obveščevalnimi službami, čeprav je prej delala v irskem parlamentu in pozneje v Irskem nacionalnem vesoljskem centru, naj bi kazal na odsotnost varnostnih protokolov in strategij v državi (Lally, Carswell, 2023, in Fitsanakis, 2023).*

### 3.5 Avstrija

Republika Avstrija ima v sestavi ministrstva za obrambo ločena Vojaški obveščevalni urad (nem. Heeresnachrichtenamt – HNaA) in Protiobveščevalni urad (Abwehramt – AbwA).

Vojaški obveščevalni urad je opredeljen kot hibridna strateška obveščevalna služba za spremljanje tujine in služi najvišjemu vojaškemu in političnemu vrhu. Hibridnost razumejo kot pokrivanje strateške obveščevalne in vojaške obveščevalne dejavnosti po eni strani in vojaške obveščevalne dejavnosti na operativni in taktični ravni na drugi strani. Urad je odgovoren za zgodnje opozarjanje na grožnje in razvoj varnostnih političnih tveganj v tujini. Njegovo interesno območje obsega celoten svet in deluje tudi tam, kjer diplomatski kanali v krizni situaciji ne delujejo več (Bundesheer, 2023). Urad torej ne služi zgolj obrambnemu ministrstvu ali oboroženim silam, temveč na državni ravni predstavlja obveščevalno službo, ki spremlja tujino (podobno kot na Irskem), medtem ko je domače razmere spremljal Zvezni urad za zaščito ustave in zoperstavljanje terorizmu (nem. Bundesamt für Verfassungsschutz und Terrorismusbekämpfung – BVT), ki spada k notranjemu ministrstvu. Po terorističnem napadu na Dunaju novembra 2020 ga je z reorganizacijo zamenjala Direkcija za zaščito države in obveščevalno dejavnost (nem. Direktion fur Staatschutz und Nachrichtendienst – DSN), ki danes opravlja naloge zaščite ustave (Bundesministerium Inneres, 2023).

Na čelu službe je častnik s činom generalmajorja ali brigadirja, ki je nameščen na ministrstvu za obrambo.

Vsem prej navedenim državam dodajmo še primer Hrvaške. Vojaška varnostna obveščevalna agencija (hrv. Vojna sigurnosno-obavještajna agencija – VSOA) je v Republiki Hrvaški sicer organizirana v sestavi ministrstva, podobno kot Obveščevalno varnostna služba na Ministrstvu za obrambo v Republiki Sloveniji, vendar je na čelu častnik s činom brigadnega generala, podpira pa tako ministrstvo za obrambo kot tudi oborožene sile (Ministarstvo obrane Republike Hrvatske, 2023).

## 4 VLOGA VOJAŠKE OBVEŠČEVALNE DEJAVNOSTI V SLOVENSKI VOJSKI

Praksa v obravnavanih državah kaže, da se oborožene sile zanašajo na obveščevalno zagotovitev, ki jo dobijo od služb ali agencij, ki primarno izvajajo vojaško obveščevalno dejavnost. Poveljniki na vseh ravneh potrebujejo podatke, pridobljene od ustrezno kvalificiranega osebja ob uporabi razpoložljivih virov.

Pri tem je treba poudariti, da je delovanje primerjanih vojaških obveščevalnih služb, direktoratov, oddelkov in agencij v sozvočju z demokratično ureditvijo držav, tudi kar se tiče uporabe posebnih metod in sredstev. Te službe ne ogrožajo demokratične

ureditve, temveč jo ščitijo.[20] Funkcija prisile je v naštetih državah v rokah policije, in ne oboroženih sil, kot to velja za vsako demokratično državo.

Vojaške obveščevalne službe sicer izmenjujejo podatke z drugimi obveščevalnimi službami v državi, vendar izvajajo analize in pripravljajo poročila predvsem s poudarkom na vojaškem vidiku, česar civilne obveščevalne službe praviloma ne zmorejo zagotoviti v enaki meri, saj zagotavljajo analize za politične odločevalce (izvajajo obveščevalne naloge).

Vojaški način delovanja je predpisan in najučinkovitejši v okviru štabnega procesa dela (Pravila za štabno delo, Zvezek 1). Štab ima svoje sektorje/oddelke, ki morajo v procesu vojaškega odločanja prispevati svoj delež za pravilno odločanje poveljnika. Vojaška obveščevalna dejavnost ima pri tem pomembno vlogo. Doktrina AJP-5[21] (Allied joint doctrine for the planning of operations) v točki 3.3 navaja, da je razumevanje okolja delovanja (angl. Operating Enviroment) kritičen pogoj za vse načrtovalne dejavnosti, še posebej za zasnovo delovanj (angl. Operations design). Ta določa glavni pristop v operaciji, iz njega pa izhajajo dejavnosti sil. Pri tem združena obveščevalna priprava okolja delovanja (angl. Joint Intelligence Preparation of Operating Enviroment – JIPOE), ki jo izvaja vojaško obveščevalno osebje, z opisom glavnih značilnosti operativnega okolja omogoči štabu oceno potencialnih učinkov tega okolja na izvedbo poslanstva. Združena obveščevalna priprava okolja delovanja podpre sprejem odločitve poveljnika, saj mu omogoči, da si predstavlja obseg problema in način, kako oblikovati in spreminjati okolje delovanja sebi v prid (AJP-5, 2019, str. 3–5).

Pri tem moramo upoštevati, da se je struktura groženj v obdobju zadnjih nekaj let bistveno spremenila. Iz poudarka na terorizmu smo prešli na klasične in celo natančno opredeljene vojaške grožnje. Tako je na primer Rusija v strateškem konceptu Nata iz leta 2022 opredeljena kot grožnja (NATO 2022 Strategic Concept, 2022), medtem ko je bila v istem dokumentu leta 2010 opredeljena kot partnerica (NATO 2010 Strategic Concept, 2010). Pojavili sta se tudi novi domeni, vesolje in kibernetski prostor, in vedno izrazitejša je težnja po uvedbi kognitivne domene. Civilne obveščevalne agencije lahko uspešno pokrivajo terorizem, ki je v bistvu težava notranje varnosti in se mu praviloma zoperstavlja policija, težje pa zagotavljajo obveščevalne podatke in predvsem obveščevalne analize o klasični vojaški grožnji sovražnih držav ali držav tekmic.

---

[20] *Kot primer lahko navedemo britansko DI, pri kateri že na njeni predstavitveni spletni strani navajajo usklajenost službe z zakonodajnimi akti in parlamentarni nadzor nad dejavnostjo agencije. Irska J-2 pogosto uporablja skladno z zakonom sredstva za prisluh po odobritvi pristojnih sodišč, kadar je lahko ogrožena varnost države* (O'Keefffe, 2022).

[21] *Za načrtovanje na strateški in operativni ravni uporablja Nato zavezniško združeno doktrino AJP-5, v kateri je kot osnovno orodje za načrtovanje opredeljena Comprehensive Operation Planning Directive (COPD). Ta je tudi temeljno orodje za načrtovanje v Slovenski vojski na ravni Generalštaba SV, Poveljstva sil SV in Centra vojaških šol (Pravila za štabno delo, Zvezek 1, str. 14).*

Nove domene zahtevajo interdisciplinaren pristop, ki predvideva tesno sodelovanje vojaških in civilnih organov. Tudi prehod med mirom, krizo in vojno je v današnjem varnostnem okolju vedno bolj zabrisan, predvsem zaradi hibridnega pristopa k vojskovanju (Gilles, 2020), ki ga med drugim opisuje tudi t. i. doktrina Gerasimova.[22] Če bi si dovolili bistveno drugačen pristop med delovanjem v miru in v vojni, se izpostavljamo velikemu tveganju. Clark navaja, da »morajo ZDA in zavezniki razumeti kremeljski koncept hibridnih vojn, da bi se lahko zoperstavili sredstvom, ki so vpletena v te vojne, ali pa Zahod tvega, da bo zmagoval v posameznih bitkah in izgubil vojno, ki se je sploh ne bo zavedal« (Clark, 2020, str. 13). Ves trud je treba ciljno naravnati v smeri preprostega prehoda iz delovanja v miru v delovanje v vojni.

Kot primer dobre prakse prehoda iz miru v krizo lahko navedemo migrantsko krizo leta 2015, ko se je Slovenska vojska skoraj čez noč, kljub vsem izzivom okoli 37.a člena Zakona o obrambi, morala organizirati za nalogo varovanja državne meje. Zaradi vojaškega načina delovanja ter organizacije in štabnega procesa dela (ki je povezljiv z Natom) je Slovenska vojska hitro vzpostavila nadzor nad situacijo (prešla iz mirnodobnega v krizno stanje) in kljub takratnemu materialnemu pomanjkanju uspešno opravila svojo nalogo. Policija take obsežne in kompleksne situacije sama ni zmogla obvladovati, med drugim tudi zaradi drugačnega načina dela.

Za vojsko velja, da se v miru usposablja podobno, kot bo delovala v vojni. Vojaška obveščevalna dejavnost mora potekati neprekinjeno v miru in vojni. V miru iščemo potencialne grožnje, zbiramo in obdelujemo podatke o njih, vse z namenom, da bi poznali sovražnika, če bi prišlo do vojne ali konflikta. Danes je pogosto težko določiti stanje med vojno in mirom. Hibridno vojskovanje se namreč začne že precej pred začetkom kinetičnega delovanja, zato je treba budno spremljati faze[23] in temu

---

[22] *Nekateri avtorji sicer dvomijo, da je doktrina Gerasimova zares enaka zahodnemu razumevanju hibridnega vojskovanja, predvsem zaradi razlik v svetovnem nazoru med Rusijo in Zahodom (glej Gilles, Alexander, 2020: Valery Gerasimov's Doctrine, from Soviet armor officer to strategic mastermind?).*

[23] *Faze hibridnega vojskovanja (po rusko »vojne nove generacije«) povzete po ruskih avtorjih (Čekinov in Bogdanov, 2013):*

- *1. faza: nevojaško asimetrično vojskovanje – preplet informacijskih, psiholoških, ideoloških in gospodarskih ukrepov v sklopu enotnega načrta z namenom doseči ugodne politične, ekonomske in vojaške razmere.*
- *2. faza: zavajanje nasprotnikovega vodstva z usklajenimi ukrepi diplomacije, medijev in vladnih agencij.*
- *3. faza: zastraševanje, zavajanje in podkupovanje vladnih uradnikov in častnikov z namenom, da bi opustili svoje dolžnosti.*
- *4. faza: povečevanje nezadovoljstva med prebivalstvom s propagando, napotitev paravojaških enot in eskalacija subverzije.*
- *5. faza: vzpostavitev prepovedi letenja, blokad in uporaba zasebnih vojaških podjetij v sodelovanju z oboroženo opozicijo.*
- *6. faza: začetek vojaških operacij, pred katerimi so izvedeni obsežno izvidovanje in subverzivne operacije. Uporaba vseh sredstev in sil.*
- *7. faza: kombinacija ciljanih informacijskih operacij, elektronskega vojskovanja, zračnih operacij in preciznih orožij ter orožij, temelječih na novih principih delovanja (mikrovalovi, nesmrtonosna orožja, biološko orožje…).*
- *8. faza: uničenje preostalih točk odpora s specialnimi enotami in artilerijo, izvedba zračnodesantnih napadov in čiščenje ozemlja s kopenskimi silami.*

*Vsaka od navedenih faz pripravi ugodne pogoje za naslednjo. Če ti niso doseženi, vojna ne more preiti v naslednjo fazo. Avtorja posebej poudarjata pomen informacijske in psihološke prevlade nad nasprotnikom ter vlogo napredne tehnologije (npr. robotov) v prihodnjih vojnah.*

ustrezno prilagoditi svoje postopke, saj se bomo v nasprotnem primeru neustrezno odzvali – na primer bomo že v vojni, izvajali pa bomo mirnodobne postopke z vsemi omejitvami. Vzpostaviti moramo jasno zavedanje, v kateri fazi morebitnega hibridnega vojskovanja smo in tudi primerno prilagoditi postopke. Ti postopki pa morajo ustrezati normativnim ureditvam.

Naši postopki morajo sovražnika prehiteti. Predvidevati moramo njegove korake, namesto da se odzivamo na že opravljena dejstva. Zaradi naštetega ne moremo več strogo ločiti izvajanja obveščevalne in vojaške obveščevalne dejavnosti, saj zaradi prepletenih groženj potrebujemo tudi prepleteno sodelovanje obeh dejavnosti. To je izrazito pri izvajanju t. i. PMESII-analize[24] v okviru procesa združene obveščevalne priprave okolja.[25] V luči novih groženj je treba okrepiti sodelovanje vojaške obveščevalne, protiobveščevalne in varnostne dejavnosti (VOPVD) z OVS, v katerem vsak sodelujoči pokriva svoje področje, izdelki obeh pa se združijo v produkte, ki ustrezno podprejo tako vojaške kot civilne odločevalce pri njihovih odločitvah.

Tudi tradicionalne razmejitve med strateško, operativno in taktično ravnjo bojevanja so vedno bolj zabrisane, zato potrebujemo usklajeno delovanje strokovnega obveščevalnega osebja na vseh omenjenih ravneh in jasno razmejitev nalog med civilnimi (SOVA), obrambnimi (OVS) in vojaškimi obveščevalnimi organi (J/S-2).

Glede na to, da bi v vojni delovali v okviru Zavezništva bodisi kot del morebitne koalicije ali pa kot posamezniki znotraj mednarodnih enot in poveljstev, morajo biti naši postopki skladni z Natovimi standardi (primer AJP 2.0[26] in podrejene doktrine). Ne smemo si privoščiti »dvojnih standardov«, torej da bi pri delovanju doma uporabljali drugačne postopke kot pri delovanju v Zavezništvu. Zavezništvo svoje postopke in standarde nenehno izpopolnjuje in spreminja, mi pa jim moramo skozi proces standardizacije slediti in jih tudi uporabljati, saj bomo le tako lahko uspešno delovali v kompleksnem in hitro spreminjajočem se mednarodnem okolju. Zelo verjetno se bomo tudi v morebitni vojni ali spopadu na ozemlju Slovenije bojevali skupaj z zavezniki. Tudi v tem primeru sta interoperabilnost in integracija zelo pomembni.

Danes se operacije poganjajo z informacijami (razširjen angl. izraz – »intel driven« oziroma »J2 run ops«), kar pomeni, da informacije iz vseh virov neposredno vplivajo in usmerjajo operacije oboroženih sil. Tak aktiven pristop omogoča, da lahko grožnje prehitimo in smo vedno korak pred njimi. Kot primer: če pravočasno ugotovimo, da je recimo medijska kampanja ali širjenje lažnih novic po socialnih omrežjih uvodna faza hibridnega delovanja, lahko sprejmemo ukrepe, ki bodo

---

[24] *S PMESII-analizo opišemo operativno okolje na podlagi šestih med seboj povezanih faktorjev: political (P), military (M), economic (E), social (S), informational (I) in infrastructural (I).*

[25] *Joint Intelligence Preparation of Operational Enviroment – analitični proces, ki zagotovi obveščevalno oceno in druge produkte poveljniku za podporo odločanja in načrtovanja (AAP-06, 2022).*

[26] *AJP-Allied Joint Publication, AJP 2.0, je Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security.*

ustavili nadaljnje hibridno delovanje in mogoče tudi prehod v kinetično fazo. Za hibridno vojno namreč velja, da poteka po korakih in je za prehod v naslednji korak potrebna izpolnitev predhodnega, sicer obstane. V kolikor pa tega ne zaznamo (ob spremljanju indikatorjev in opozoril – angl. Indicators and Warnings – I&W), lahko delovanje nemoteno poteka v kognitivni in pozneje kibernetski domeni. Ko pa se začne kinetična faza, smo prepozni za ukrepanje in vojna je že izgubljena.

V prihodnosti lahko pričakujemo še več sprememb. Vedno večji bo pomen umetne inteligence in naprednih komunikacijskih 5G-povezav.[27] Kibernetski prostor bo vse pomembnejši, zato je treba krepiti zmogljivosti v kibernetski domeni in jih centralizirati ter poenotiti. V Sloveniji je več subjektov kibernetske varnosti, ki zagotavljajo varovanje informacijske infrastrukture na različnih ravneh, v zasebnem in javnem sektorju. Kibernetski napad z jasnim vojaškim ozadjem (torej prepoznana udeležba oboroženih sil neke države v napadu na vojaško informacijsko omrežje) se v Sloveniji še ni zgodil, bi pa v tem primeru morala obrambo in tudi odgovor na tak napad zagotoviti Slovenska vojska, ki po drugem odstavku 3. člena Zakona o obrambi izvaja vojaško obrambo države samostojno ali v Zavezništvu na podlagi mednarodnih pogodb. Če razumemo, da se ustrezen odgovor in obramba izvajata v okviru Zavezništva, potem je treba tudi na vajah sodelovati z istim osebjem in postopki kot v vojni. To osebje mora biti povezljivo z Zavezništvom, torej obvladovati angleški jezik in poznati Natove standarde in doktrine na svojem področju. Ne smemo pozabiti, da je temeljni namen oboroženih sil delovati v vojni, kar mora veljati za vse njihove podsisteme in bojne funkcije, tudi za vojaško obveščevalno dejavnost.

Britovšek in Čretnik sta v svojem članku že leta 2016 predlagala tri modele reorganizacije obveščevalno-varnostnega sistema v Republiki Sloveniji, pri čemer vsi modeli predvidevajo okrepitev obveščevalnega sektorja znotraj Generalštaba Slovenske vojske. Po njunem mnenju bi moralo biti tako: »Obveščevalni sektor SV bi v celoti prevzel vojaške obveščevalne naloge (spremljanje vojaških groženj, razmer v mednarodnih operacijah in na misijah, bojiščih ter kriznih žariščih) in bi s svojimi ocenami ter ugotovitvami redno podpiral enote, poveljnike in poveljstva SV ter druge organe Ministrstva za obrambo. Za optimalno opravljanje nalog bi obveščevalni sektor SV moral okrepiti analitični del ter izkoristiti obveščevalne zmogljivosti, ki jih premore SV« (Britovšek, Čretnik, 2016, str. 335).

Če povzamemo predzadnjo oceno pripravljenosti Slovenske vojske iz leta 2022, je po besedah tedanjega vrhovnega poveljnika, predsednika republike Boruta Pahorja, »SV naredila viden napredek, ni pa ta napredek še dovolj za celovito delovanje v vojnih razmerah« (Dnevnik, 2022). Tudi zadnje poročilo vrhovni poveljnici, predsednici republike Pirc Musar, po poročanju načelnika Generalštaba Slovenske vojske kaže na odstopanja od zahtevanih standardov, predvsem na področjih zmogljivosti in sposobnosti za delovanje (A. K., 2023). Če je v tej oceni mogoče

[27] *Tehnološki standard za peto generacijo širokopasovnih mobilnih omrežij. Omrežja 5G odlikujejo visoke hitrosti (do 10Gbit/s) in večja pasovna širina, ki omogoča povezavo več naprav hkrati kot dosedanje povezave do 4G. Pripravlja se že 6G, ki bo imel še zmogljivejšo tehnologijo.*

prepoznati tudi vojaško obveščevalno dejavnost, potem lahko sklepamo, da mora poleg celotne Slovenske vojske tudi obveščevalno-varnostna struktura na področju obrambe napredovati, tako da bo lahko v času miru poleg svojih osnovnih nalog ustrezno usposabljala moštvo in pripravljala postopke za vojno stanje. Le tako bodo ti primerni ali vsaj dovolj dobri za celovito delovanje v vojnih razmerah.

## 5 IZKUŠNJE VOJAŠKE OBVEŠČEVALNE DEJAVNOSTI MED VOJNO V UKRAJINI

V zgodovini je celovita obveščevalna zagotovitev že mnogokrat prihranila žrtve in omogočila zmago, medtem ko je nezadostna ali površna povzročila poraze sicer močnejših sil, ki sovražnika niso dobro poznale in so ga posledično podcenjevale. Dogodki med vojno v Ukrajini potrjujejo pomen dobre obveščevalne zagotovitve. Miller in Benton navajata, da so ruske oborožene sile napad začele s slabo izvedeno obveščevalno pripravo (FSB),[28] ki je povsem podcenila ukrajinsko voljo do odpora in vrhovnemu poveljniku postregla z informacijami, ki jih je želel slišati, ne pa z resničnim stanjem (Miller in Belton, 2022). Posledično so v Ukrajino vdrli s premalo silami, ki so bile logistično pomanjkljivo oskrbljene in popolnoma nepripravljene na intenzivnost in trajanje spopadov, ki so jih čakali. Ta napaka se je odrazila v na tisoče žrtvah in ogromnih izgubah v tehniki. Nasprotno ima Ukrajina ustreznejšo obveščevalno podporo, predvsem podprto z zmogljivostmi partnerjev. Zato so na bojišču večkrat premagali močnejše ruske sile. S pravočasnimi in natančnimi obveščevalnimi podatki o ciljih so lahko tudi z raketnimi sistemi HIMARS uspešno uničevali ruska poveljniška mesta in oskrbovalne točke ter tako spremenili potek vojne. Nasprotno ruske oborožene sile s svojimi raketnimi napadi na vojaške cilje niso dosegle uspeha, saj je njihova obveščevalna podpora pri iskanju premičnih ciljev pomanjkljiva in predvsem prepočasna. Cilji, ki so jih napadali, so bili pogosto že daleč stran od zadnje lokacije, ki je bila ruski strani znana. Ocenjevanje bojne škode je bilo zaradi tehničnih omejitev zelo slabo (Zabrodsky, Watling, Danylyuk, Reynolds, 2023), saj ne izvajajo dinamičnega ciljenja (angl. Dynamic targeting). Zato so se preusmerili k uničevanju civilne infrastrukture, kar lahko predstavlja tudi kršitev mednarodnega vojnega prava in vojni zločin.

Uspehi in neuspehi obveščevalne zagotovitve v tej vojni so zaznamovale tudi osebne usode odgovornih. Tako je bil ukrajinski vodja glavnega direktorata za obveščevalne zadeve ministrstva za obrambo (GUR) Kirilo Budanov, ki je pravilno napovedal ruski napad, predčasno povišan iz brigadirja v generalmajorja, hkrati pa je pridobil velik vpliv (pojavil se je tudi kot kandidat za obrambnega ministra), medtem ko je na primer direktor francoskega Direktorata za vojaško obveščevalno dejavnost (fr. Direction du renseignement militaire – DRM) – generalpodpolkovnik Eric Vidaud izgubil svoj položaj, ker je njegova služba ocenila, da ruski napad ni verjeten, saj bi zahteval preveliko ceno za svoj uspeh (Reuters, 2022).

[28] *FSB – Federalnaja služba bezopasnosti rosijskoj federaciji, osrednja ruska civilna varnostna in protiobveščevalna služba.*

Če Budanov napada ne bi napovedal, bi Ukrajina verjetno klonila pod rusko premočjo, saj bi bila popolnoma nepripravljena (civilna obveščevalna služba SBU je bila prepredena z ruskim kadrom in je celo zadržala poročila, ki so govorila o neizbežnem napadu), Putin pa bi lahko nemoteno nadaljeval svojo pot k obnovi ruskega imperija. Budanov je vodstvo seznanil z realnimi informacijami, in ne s tem, kar so morda želeli slišati (spomnimo se, da je predsednik Ukrajine Zelenski v tednih pred napadom javno nasprotoval ameriškim ocenam o neizbežnem napadu, saj se je bal panike in ekonomskih posledic). Tako se je tudi izpostavil in prevzel odgovornost. V nasprotju s tem pa so v FSB Putinu posredovali informacije, ki so bile blizu njegovim predsodkom (Miller, Benton, 2022), saj so se bali odziva in obtožb o nestrokovnosti. Tako so na primer izvedli prikrite ankete, ki so pokazale, da Ukrajinci Rusov ne bodo pričakali s cvetjem, vendar tega niso poročali odločevalcem. Posledično je Rusija Ukrajino napadla zaradi prikrojenih in slabih obveščevalnih podatkov, ki so kazali na uspeh take operacije.

Ta primer kaže na velik pomen racionalnega razmišljanja na obeh straneh relacije obveščevalec–vodstvo, k čemur si je treba prizadevati tudi v Sloveniji. Zveza Nato je na izrazito rusko grožnjo opozorila že leta 2019 v govoru generalnega sekretarja Stoltenberga pred ameriškim kongresom, na vrhu v Madridu leta 2022 pa je potrdila Rusijo kot najpomembnejšo in neposredno grožnjo varnosti zaveznic v Strateškem konceptu Nata.[29] ZDA so kot država z najbolj zmogljivim obveščevalnim aparatom na svetu skoraj do dne natančno napovedale ruski napad na Ukrajino leta 2022.

Kot članica Zavezništva bi Slovenija morala upoštevati razvoj ruske grožnje v prihodnosti, saj v nasprotnem primeru prevzemamo velika tveganja na vseh področjih. Zavedati se moramo, da delovanje v Zavezništvu ne obsega samo vojaškega instrumenta moči države, temveč večinoma tudi diplomatskega in posledično ekonomskega. Ob ruskih napadih na energetsko infrastrukturo Ukrajine lahko vidimo, katere ekonomske posledice povzroči onesposabljanje kritične infrastrukture. Ob tem ni nujno, da so napadi kinetični, tudi uspešen kibernetski napad na našo kritično infrastrukturo bi lahko povzročil veliko materialno škodo in morda tudi človeške žrtve.

Izkušnje iz Ukrajine nas učijo, da čeprav državno vodstvo obveščevalnih podatkov, ki ne potrjujejo njegovih domnev, včasih noče slišati in upoštevati (ker bi npr. njihovo upoštevanje in ustrezno ukrepanje povzročili ekonomske in socialne posledice oziroma zahtevali drugačne odločitve, kot so že bile sprejete), mora obveščevalno-varnostni aparat nanje vztrajno opozarjati in se ne sme ukloniti pritiskom odločevalcev ter svojih ocen prirediti njihovim željam in pričakovanjem. Posledice in stroški zavestnega neupoštevanja opozoril (tiščanja glave v pesek) in posledične nepripravljenosti na grožnjo so neprimerljivo višji kot stroški, ki jih povzročijo preventivni ukrepi in odvračalna drža. Pri tem je treba upoštevati, da grožnja uporabe jedrskega orožja še nikoli ni bila tako otipljiva, kot je danes, in ob

[29] *NATO 2022 Strategic Concept, str. 4, točka 8.*

nenehnih ruskih verbalnih grožnjah z jedrskim orožjem je verjetno, da bo tovrstno orožje kmalu dobil tudi Iran, kar bo odprlo še dodatno jedrsko grožnjo Evropi (Norman, 2023).

Danes je prehod med vojno in mirom zabrisan, kar bo še močneje veljalo v prihodnosti, zato si mora obveščevalno-varnostna struktura prizadevati, da bodo postopkovne in taktične razlike med delovanjem v vojni in miru čim manjše, seveda znotraj zakonsko predpisanih okvirov. Grožnje bodo kompleksnejše, resnejše in bolj sofisticirane,[30] demografska slika v Sloveniji pa ne kaže, da bi lahko strukture kadrovsko povečevali, zato je integracija civilnih in vojaških struktur v obveščevalno-varnostni dejavnosti na Ministrstvu za obrambo nujna. Le tako bomo lahko v vedno bolj negotovi prihodnosti podprli vse v sistemu, ki to potrebujejo, in ostali kredibilen partner v okviru Nata in EU.

Analize ruskega napada na Ukrajino kot bistvene pomanjkljivosti izpostavljajo slabo obveščevalno oceno in neprimerno vodenje ter poveljevanje. Razlog za napačno obveščevalno oceno lahko najdemo v slabem načrtovanju, tudi zaradi neustreznega delovanja FSB v procesih odločanja. Posledica slabega vodenja in poveljevanja pa je delno rezultat premajhnega pomena vojaških štabov (ruska vojaška kultura ne prepozna vodenja s poslanstvom in tudi številčnost štabov, posebej na taktični ravni, je manjša, kot jo poznamo v Natu). Tudi na ukrajinski strani se pojavljajo pomanjkljivosti pri izvajanju vojaške obveščevalne dejavnosti, zlasti pri obveščevalni podpori enot na terenu. Obrambna obveščevalna služba GUR izvaja centralizirano vodenje obveščevalne dejavnosti in je v resnici ločena od vojaške organizacije, ki naj bi jo podpirala. Ker ukrajinska vojska v štabni strukturi nima primerne J-2, obveščevalni podatki pogosto ne pridejo do vojaških enot, ki jih potrebujejo, ali pa niso oblikovani tako, da jih podpirana enota lahko koristno uporabi (Grant, 2023).

## Sklep

Štabni proces dela z vojaško obveščevalno analizo, izoblikovanimi variantami delovanja in kakovostnim preigravanjem teh variant je bistven za uspeh tako v procesu načrtovanja kakor tudi pri sprejemanju odločitev med delovanjem.

Za učinkovitejše izvajanje vojaških obveščevalnih nalog v Slovenski vojski bi bilo optimalno, da se J-2 na strateški ravni kot del obveščevalno-varnostnega sistema Republike Slovenije poveže z OVS na način, ki bo omogočal pravočasno in ustrezno (angl. fit for purpose) obveščevalno podporo celotnega obrambnega sistema. Tako bi najhitreje rešili kadrovski primanjkljaj, ki se pojavlja na vseh področjih v obrambnem sistemu, in hkrati uskladili delovanje, da se ne bi več podvajale naloge obeh.

[30] *Resolucija o splošnem dolgoročnem programu razvoja in opremljanja Slovenske vojske do leta 2035, 2. poglavje, Ljubljana 2022, str. 6.*

Tak primer vidimo pri britanski Obrambni obveščevalni službi (DI) ali španskem Obveščevalnem centru oboroženih sil (CIFAS), ki izpolnjujeta podobni vlogi v obrambnem sistemu države.

Pri dejavnosti je poudarjena analiza obveščevalnih podatkov, pridobljenih iz različnih virov oziroma zvrsti (angl. »all source«). Obe entiteti (OVS in VOPVD) imata strokovnjake na različnih področjih, vendar je ob trenutnem normativnem stanju vojaška obveščevalna dejavnost v funkcionalnosti zakonsko omejena. Integracija VOPVD z OVS bi prinesla tudi trdno umeščenost vojaške obveščevalne dejavnosti v sedanji zakonodajni okvir.

Našo obrambno in vojaško obveščevalno dejavnost bomo težko v popolnosti razmejili in opredelili podobno, kot sta britanska Obrambna obveščevalna služba ali španski Obveščevalni center oboroženih sil, saj gre za bistveno obsežnejša sistema z neprimerljivo večjimi zmogljivostmi. Lahko pa povzamemo nekaj pomembnejših značilnosti:

- smiselna umestitev – na Generalštab SV (oziroma obrambni štab) in Ministrstvo za obrambo;
- tesno sodelovanje z drugimi agencijami, v našem primeru s Sovo;
- poudarjena delitev obveščevalne dejavnosti na analitično in funkcijo IRM & CM[31] − ta bi omogočila centralizirano upravljanje vseh obveščevalnih zmogljivosti oziroma disciplin v Slovenski vojski po funkcijsko podrejenih organih, v katerih so te zmogljivosti;
- analitični del temelji na podatkih »All Source«;
- upoštevanje različnosti obveščevalnih potreb rodov vojske (letalstvo, mornarica, artilerija, pehota) in domen (kopno, zrak, morje, vesolje, kibernetski prostor) imajo lahko bistveno različne potrebe po obveščevalnih podatkih;
- enotno usposabljanje pripadnikov vseh obveščevalno-varnostnih struktur ministrstva v okviru šole, pri čemer program usmerjata integrirana SVOPVD in OVS.

Ob tem vzpostavljena funkcija IRM & CM na strateški ravni bi poleg optimalnega upravljanja in načrtovanja pridobivanja obveščevalnih podatkov prispevala tudi h krepitvi nadzora in sodelovanja z vojaškimi obveščevalnimi organi na operativni in taktični ravni. Tako bi lahko optimalno izkoristili materialne in človeške vire za pridobivanje obveščevalnih podatkov in se izognili nepotrebnemu podvajanju.

[31] *Intelligence Requests Management and Collection Management − upravljanje obveščevalnih zahtev in pridobivanje obveščevalnih podatkov je proces, ki upravlja in organizira zbiranje obveščevalnih podatkov iz različnih virov oziroma obveščevalnih zvrsti.*

Pri vsem je nujno zavedanje, kaj je vojaška obveščevalna dejavnost, kaj je obrambna[32] obveščevalna dejavnost (Obveščevalno varnostna služba, 2023) in kaj je »civilna«[33] obveščevalna dejavnost (O Slovenski obveščevalno varnostni agenciji, 2023), katere produkte te pripravljajo in koga z njimi podpirajo pri odločanju. Ko se tega zavemo, vidimo, da za izvajanje potrebujemo osebe z različnimi kompetencami in specifičnim strokovnim znanjem.

Podvajanje preprečimo tudi z jasno ločenostjo strateške, operativne in taktične ravni. Operativna in taktična raven vojaške obveščevalne dejavnosti morata izvesti vsaka svojo vlogo pri delovanju, pri čemer podpirata svoje poveljnike in hkrati dajeta prispevek v obveščevalno sliko na strateški ravni. Strateška raven daje jasne usmeritve z načrti pridobivanja obveščevalnih podatkov in hkrati tudi potrebne podatke podrejenim, najpogosteje z odgovori na zahtevke za informacije (ZZI). Strateška raven vojaške obveščevalne dejavnosti v časovni dimenziji (24/7) ocenjuje obzorje, torej predvideva konflikte, ki se še niso zgodili in bi lahko vplivali na delovanje Slovenske vojske, konflikte, ki se že dogajajo in bi lahko vplivali na delovanje Slovenske vojske, oziroma tiste, ki so se že zgodili in tam že delujemo, njihov razvoj pa bi lahko bistveno spremenil delovanje Slovenske vojske. Operativna raven ocenjuje tekoče operacije s časovnim obzorjem nekaj mesecev oziroma dokler traja operacija, medtem ko taktična raven ocenjuje bojišče z obzorjem nekaj dni. Če so te vloge jasno razmejene, potem se težko zgodijo podvojitve.

Obveščevalna dejavnost v obrambnem sistemu Republike Slovenije mora biti integrirana na način, da OVS zbira in obdeluje obveščevalne podatke, ki so pomembni za obrambo državo, ob tem pa J-2 na GŠSV vodi in usmerja vojaško obveščevalno in izvidniško dejavnost v Slovenski vojski ob sodelovanju podrejenih funkcijskih organov. Tako lahko produktom OVS dodamo še vojaško oceno, tudi na podlagi podatkov, ki jih pridobijo sistemi ISTAR v sestavi Slovenske vojske. V tem primeru lahko z minimalnimi spremembami vzpostavimo robusten in učinkovit sistem, ki bo lahko deloval v miru in vojni, tako samostojno kot v sodelovanju z zavezniki.

Usposabljanje obveščevalnega osebja bi zato z namenom večje interoperabilnosti izvajali v šoli, podobni britanski Obrambni obveščevalni akademiji, ki bi jo umestili v strukturo Centra vojaških šol (CVŠ), vendar bi jo strokovno upravljal J-2 v

---

[32] *Obveščevalno varnostna služba (OVS) je obrambna obveščevalno-varnostna služba, organizirana v statusu direktorata na Ministrstvu za obrambo. Služba opravlja obveščevalne, protiobveščevalne in varnostne naloge, zadolžena pa je še za zagotavljanje enotnega sistema varovanja tajnih podatkov na Ministrstvu za obrambo (Obveščevalno varnostna služba, 2023).*

[33] *Slovenska obveščevalno-varnostna agencija (SOVA) je osrednja civilna obveščevalno-varnostna služba. Med njene temeljne naloge spada delovanje pri zaščiti nacionalnih interesov na varnostnem, političnem in gospodarskem področju oziroma zagotavljanje nacionalne varnosti.*
*Zakon o Sovi v 2. členu opredeljuje tri osnovne naloge agencije:*
*1. pridobivanje podatkov,*
*2. vrednotenje podatkov,*
*3. posredovanje informacij iz tujine ali v povezavi s tujino.*
*Delovno področje agencije obsega obveščevalno, protiobveščevalno in varnostno razsežnost delovanja (O Slovenski obveščevalno-varnostni agenciji, 2023).*

povezavi z OVS. V taki šoli bi usposabljali pripadnike Slovenske vojske in OVS po enotnem programu (usposabljanja za vojaško evidenčno dolžnost (VED), specifike za rodove in specialistično usposabljanje za posamezne obveščevalne discipline), prilagojenem glede na potrebe službe ali naloge. Spremljanje in analiziranje naučenih lekcij iz konfliktov po svetu bi tako ustrezno vključili v programe usposabljanja tudi za potrebe CVŠ.

Pri tem je pomembno zavedanje, da skupno usposabljanje in sodelovanje na vajah omogočata pravilno načrtovanje za prihodnje konflikte, krize ali vojne in zagotavljata pripravljenost za delovanje v njih (načelo usposabljaj se, kot se boš bojeval, angl. »train as you fight«).

Ena izmed mogočih in precej preprostih rešitev je, da vojaški del (J-2) integriramo s civilnim (OVS) na način poveljniškega razmerja OPCON[34] po sistemizaciji delovnih mest (spremeniti je treba aktualno ureditev v Aktu o notranji organizaciji in sistemizaciji delovnih mest Ministrstva za obrambo z organi v sestavi, ki ga podpisuje minister za obrambo, ter iz tega izhajajoče normativne dokumente), tako da je vojaški višji častnik namestnik direktorja OVS (visokega civilnega uradnika) v miru in izrednih razmerah, medtem ko se vlogi v vojnem stanju zamenjata.[35] Pri tem obrambna obveščevalna dejavnost z integracijo vojaške obveščevalne dejavnosti pridobi »legitimnost«, hkrati pa vojaška obveščevalna dejavnost z integracijo v obrambno obveščevalno dejavnost pridobi »legalnost«. Ta sinergija omogoča gladek prehod iz delovanja v miru na delovanje v izrednih razmerah in od tod na delovanje v vojni.

**Predlagana možnost umeščenosti integracije VOPVD in OVS v strukturo MO in GŠSV**

Iz sheme (Slika 2) je razvidno, da so produkti usmerjeni glede na potrebe in zahteve uporabnikov ter omogočajo večji učinek v procesih odločanja na vseh ravneh, tako za potrebe miru, izrednih razmer ali vojne. Tako bi vsi uporabniki v obrambnem resorju dobili kakovosten in integriran produkt, prilagojen njihovim potrebam in primeren tudi za širšo uporabo v okviru celotnega nacionalnega varnostnega sistema.

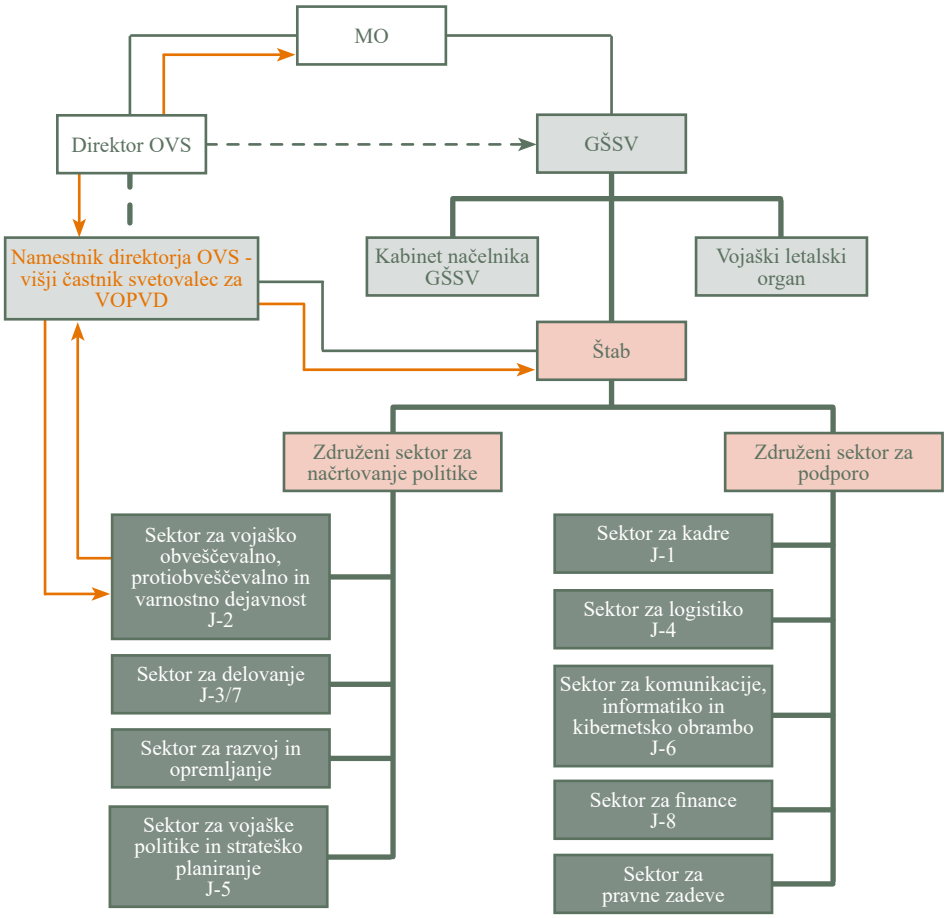
V sedanji organigram bi dodali namestnika direktorja OVS, ki bi bil vojaška oseba in kot tak primernejši za udeležbo na sestankih/odborih Zavezništva, na katerih so prisotni predstavniki zavezniških entitet za vojaško obveščevalno dejavnost.

---

*[34] OPCON (»Operational Control« oziroma operativna kontrola) je pooblastilo, ki ga prejme poveljnik za vodenje dodeljenih sil, s katerim lahko izvede naloge, običajno omejene z vsebino, časom in prostorom. V Slovenski vojski je več primerov enot pod OPCON, npr. 16. CNKZP kot del NATINAMDS (NATO integrated Air Defense System) v razmerju do Natovega AIRCOM CAOC Torrejon oziroma slovenski kontingenti v mednarodnih operacijah.*

*[35] Pri delovanju v kompleksni krizi ali vojni bi bilo tudi smiselno umestiti načelnika GŠSV v Državni operativni štab obrambe – DOŠO.*

**Slika 2:** Predlog umeščenosti v strukturo MO in GŠSV




Učinek bi še povečali, če bi integrirali MO in GŠSV v obrambni štab.[36] Vendar ima tudi v predlagani možnosti ta rešitev največ učinka z najmanjšimi stroški in minimalnimi posegi v normativno ureditev.

Časa za spremembe je vse manj, saj je Evropa že vsaj od leta 2014 izpostavljena hibridnim napadom, zlasti v kognitivni in tudi kibernetski domeni, vedno bolj pa se povečuje tudi tveganje za uporabo jedrskega orožja.

[36] *Poročilo Examination of the Current Status of the Slovenian Armed Forces: Findings (bis) (18 April 2018), ki ga je ameriški Center for Civil-Military Relations predstavil po pregledu stanja v Slovenski vojski, kot posebno težavno izpostavlja pomanjkanje integracije med MO in GŠSV ter »vzpostavljanje samozadostnosti obeh entitet kot kompenzacije, saj entiteti nista integrirani med sabo« (Young, 2018). Vzpostavitev integriranega obrambnega štaba bi to škodljivo »samozadostnost« in s tem podvajanje funkcij odpravilo.*

## Literatura


1. *AAP-06 Edition, 2021. NATO GLOSSARY OF TERMS AND DEFINITIONS (ENGLISH AND FRENCH), NSO 2021. https://standard.di.mod.bg/pls/mstd/MSTD.blob_upload_download_routines.download_blob?p_id=281&p_table_name=d_ref_documents&p_file_name_column_name=file_name&p_mime_type_column_name=mime_type&p_blob_column_name=contents&p_app_id=600.*
2. *Adam, K., 2022. How U.K. intelligence came to tweet the lowdown on the war in Ukraine, The Washington Post. https://www.washingtonpost.com/world/2022/04/22/how-uk-intelligence-came-tweet-lowdown-war-ukraine/, 12. 3. 2023.*
3. *A. K., 2023. Pirc Musarjeva: Naša vojska je sposobna braniti ozemeljsko celovitost Slovenije, Siolnet. https://siol.net/novice/slovenija/pirc-musar-nasa-vojska-je-sposobna-braniti-ozemeljsko-celovitost-slovenije-603079.*
4. *AJP-5 Allied Joint Doctrine for the Planning of Operations, Edition A, Version 2 with UK national elements, NSO, 2019. https://www.gov.uk/government/publications/allied-joint-publication-ajp-05a-allied-joint-doctrine-for-the-planning-of-operations, 12. 3. 2023.*
5. *Beale, J., 2022. Ukraine war: Predicting Russia's next step in Ukraine, BBC News. https://www.bbc.com/news/world-europe-62520743, 10. 3. 2023.*
6. *Britovšek, J., Čretnik, A., 2016. Obveščevalno-varnostni sistem Republike Slovenije: reorganizacija in sistemske rešitve. Varstvoslovje, letnik 18, št. 3, str. 325–348.*
7. *Bundesheer. Die Nachrichtendienste des Bundesheeres. https://www.bundesheer.at/organisation/beitraege/n_dienste/index.shtml, 1. 3. 2023.*
8. *Bundesministerium Inneres, Die DSN. https://dsn.gv.at/101/, 1. 3. 2023.*
9. *Center vojaških šol, Pravila za štabno delo, elektronska izdaja, Ljubljana, 2019.*
10. *Chekinov, S. G., & Bogdanov, S. A., 2013. On the nature and content of a new generation of war. Military Thought, 10, 13–24 [in Russian] prevod v angleščino. https://www.semanticscholar.org/paper/The-Nature-and-Content-of-a-New-Generation-War-Chekinov-Bogdanov/c8874593b1860de12fa40dadcae8e96861de8ebd, 12. 3. 2023.*
11. *Clark, M., 2020. Russian Hybrid Warfare Military Learning and the Future of War Series, ISW, Washington 2020. https://www.understandingwar.org/report/russian-hybrid-warfare, 5. 3. 2023.*
12. *Clonan, T., 2006. Irish Intelligence Staff Work From Kosovo To Kabul, Dublin: The Irish Times. https://arrow.tudublin.ie/aaschmedart/61/, 13. 3. 2023.*
13. *Defence Cyber Operations Group: Finance, Question for Ministry of Defence, 2016. https://questions-statements.parliament.uk/written-questions/detail/2016-02-08/26326, 14. 3. 2023.*
14. *Defence Intelligence. https://www.gov.uk/government/groups/defence-intelligence, 15. 3. 2023.*
15. *Defence Intelligence – communicating probability. Defence Intelligence – communicating probability – GOV.UK (www.gov.uk), 15. 3. 2023.*
16. *Defence Intelligence: roles. https://www.gov.uk/guidance/defence-intelligence-services, 15. 3. 2023.*
17. *Delo, 2022. Ljudje bolj zaupajo v ključne politične institucije, vojsko in policijo. https://www.delo.si/novice/slovenija/ljudje-bolj-zaupajo-v-kljucne-politicne-institucije-vojsko-in-policijo/, 27. 2. 2023.*
18. *Devanny, J., Stevens, T., 2021. What will Britain New Cyber Force Actually Do?, War on the Rocks. https://warontherocks.com/2021/05/what-will-britains-new-cyber-force-actually-do/, 14. 3. 2023.*
19. *Dnevnik, 2022. Pahor: Napredek SV za izboljšanje ocene pripravljenosti še ni zadosten, a SV je sposobna ubraniti suverenost Slovenije. https://www.dnevnik.si/1042984499, 25. 2. 2023.*
20. *Esih, U., 2020. Večjih vlaganj v opremo in oborožitev Slovenske vojske nismo imeli že desetletje, Večer. https://vecer.com/slovenija/vecjih-vlaganj-v-opremo-in-oborozitev-slovenske-vojske-nismo-imeli-ze-desetletje-10225123, 25. 2. 2023.*

21. *Eurasia Groups top risks for 2023. https://www.eurasiagroup.net/issues/top-risks-2023, 1. 3. 2023.*
22. *Fitsanakis, Dr. J., 2023. Australia to deport Kazakh-Born Irish woman for allegedly spying for Russia, Intelnews.org. https://intelnews.org/2023/02/27/01-3258/, 14. 3. 2023.*
23. *Garda Siochana. Garda National Crime & Security Intelligence Service. https://www.garda.ie/en/about-us/our-departments/garda-national-crime-security-intelligence-service1/, 14. 3. 2023.*
24. *Gallagher, C., 2022. Russia still plans to extend Dublin embassy's espionage role, say experts The Irish Times. https://www.irishtimes.com/news/ireland/irish-news/russia-still-plans-to-extend-dublin-embassy-s-espionage-role-say-experts-1.4814532, 14. 3. 2023.*
25. *Gilles, A., 2020. Valery Gerasimov's Doctrine, from Soviet armor officer to strategic mastermind? https://www.researchgate.net/publication/346195526_'Valery_Gerasimov's_Doctrine', 10. 3. 2023.*
26. *Glas ljudstva. Stop militarizaciji in omejitev investicij v vojaško opremo. https://glas-ljudstva.si/zahteve/110/, 11. 3. 2023.*
27. *Grant, G., 2023. Glen Grant. 2023 – a time and chance for military change in Ukraine. https://maidan.org.ua/en/2023/02/glen-grant-2023-a-time-and-chance-for-military-change-in-ukraine/, 12. 4. 2023.*
28. *Intelligence and Security Committee of Parliament Annual Report 2021–2022, https://isc.independent.gov.uk/wp-content/uploads/2022/12/ISC-Annual-Report-2021%E2%80%932022.pdf, 15. 3. 2023.*
29. *Irish Defence Forces, About The General Staff. https://www.military.ie/en/the-general-staff/about-the-general-staff/, 12. 3. 2023.*
30. *Irish Echo, 2011. Ireland a new front in global intelligence game. https://group.irishecho.com/2011/02/ireland-a-new-front-in-global-intelligence-game-2/, 15. 3. 2023.*
31. *Joint Doctrine Publication 2-00 Understanding and Intelligence Support to Joint Operations, (3rd Edition), 2011. MoD. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/311572/20110830_jdp2_00_ed3_with_change1.pdf.*
32. *Miller, G., Belton, C., 2022. Russia's spies misread Ukraine and misled Kremlin as war loomed, Washington Post. https://www.washingtonpost.com/world/interactive/2022/russia-fsb-intelligence-ukraine-war/, 13. 3. 2023.*
33. *Ministarstvo obrane Republike Hrvatske, O Vojnoj sigurnosno-obavještajnoj agenciji. https://www.morh.hr/o-vojnoj-sigurnosno-obavjestajnoj-agenciji/, 12. 3. 2023.*
34. *Ministrstvo za obrambo, Resolucija o splošnem dolgoročnem programu razvoja in opremljanja Slovenske vojske do leta 2035, Ljubljana 2022, 12. 3. 2023.*
35. *Ministerio de Defensa. Armed Forces Intelligence Centre (CIFAS). https://emad.defensa.gob.es/en/unidades/cifas/, 25. 2. 2023.*
36. *Ministry of Defence, 2020. How Defence Works, Version 6.0, Sep 2020. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/920219/20200922-How_Defence_Works_V6.0_Sep_2020.pdf, 15. 3. 2023.*
37. *Murtagh, P., 2017. Why Irish security forces would struggle in a terror attack, The Irish Times. https://www.irishtimes.com/news/ireland/irish-news/why-irish-security-forces-would-struggle-in-a-terror-attack-1.3114021, 15. 3. 2023.*
38. *National Cyber Force. https://www.gov.uk/government/organisations/national-cyber-force, 15. 3. 2023.*
39. *NATO Strategic Communications Centre of Excellence. About Strategic Communications. https://stratcomcoe.org/about_us/about-strategic-communications/1, 27. 2. 2023.*
40. *NATO 2022 Strategic Concept, 2022. https://www.nato.int/strategic-concept/, 15. 3. 2023.*
41. *NATO 2010 Strategic Concept, 2010. https://www.nato.int/cps/en/natohq/topics_82705.htm, 16. 3. 2023.*

42. *NATO. Joint Intelligence, Surveillance and Reconnaissance. https://www.nato.int/cps/en/natohq/topics_111830.htm, 15. 3. 2023.*
43. *Norman, L., 2023. Iran Could Produce Nuclear Weapon in Several Months if It Decides to Do So, Mark Milley Says, The Wall Street Journal. https://www.wsj.com/articles/iran-could-produce-nuclear-weapon-in-several-months-if-it-decides-to-do-so-mark-milley-says-ecd38f07, 28. 3. 2023.*
44. *Lally, C., Carswell, S., 2023. Case of Irish-Russan Woman in Australia highlights Republic's »security complacency«, The Irish Times. https://www.irishtimes.com/crime-law/2023/02/27/case-of-irish-russian-woman-in-australia-highlights-security-complacency/, 15. 3. 2023.*
45. *O Slovenski obveščevalno-varnostni agenciji. https://www.gov.si/drzavni-organi/vladne-sluzbe/slovenska-obvescevalno-varnostna-agencija/o-sovi/, 11. 3. 2023.*
46. *Obveščevalno varnostna služba. https://www.gov.si/drzavni-organi/ministrstva/ministrstvo-za-obrambo/o-ministrstvu/obvescevalno-varnostna-sluzba/, 11. 3. 2023.*
47. *O'Keefffe, C., 2022. Defence Forces ramps up covert surveillance of threats to State, Irish Examiner. https://www.irishexaminer.com/news/arid-41030210.html, 15. 3. 2023.*
48. *Oxford Reference, 10.2. 2023. https://www.oxfordreference.com/display/10.1093/oi/authority.20110810105412812.*
49. *Posebni Eurobarometer EP 98.1\EB042EP Nacionalni pregled Slovenija. https://europa.eu/eurobarometer/surveys/detail/2932, 25. 2. 2023.*
50. *Reuters, 2022. French military intelligence head steps down over Ukraine-reports, Reuters. https://www.reuters.com/world/europe/french-military-intelligence-head-steps-down-over-ukraine-reports-2022-03-31/, 20. 2. 2023.*
51. *Safeguarding and Enhancing the Critical Capabilities of the Defence Forces Intelligence function in Ireland's National Security in the 21st century, Commission on the Defence Forces Public Consultation Response Template. https://assets.gov.ie/194103/dbdc843e-1010-4ede-8f4e-0afb4cc9ecfa.pdf, 15. 3. 2023.*
52. *Schweitzer Armee. Militarischer Nachrichtendienst (MND). https://www.vtg.admin.ch/de/organisation/kdo-op/mnd.html, 11. 3. 2023.*
53. *Spyscape, J2 Spies: Ireland's Shadowy Intelligence Unit (n.d.). https://spyscape.com/article/j2-spies-who-are-irelands-equivalent-to-the-cia#:~:text=The%20Irish%20Defense%20Forces'%20military,what%20else%20does%20J2%20do%3F, 15. 3. 2023.*
54. *Stratagem, Cognitive warfare and use of force. https://www.stratagem.no/cognitive-warfare-and-the-use-of-force/#_ftn2, 11. 3. 2023.*
55. *World Economic Forum, Global Risks. https://www.weforum.org/global-risks, 1. 3. 2023.*
56. *Young, T., 2018. Examination of the Current Status of the Slovenian Armed Forces: Findings (bis) (18 April 2018).*
57. *Zabrodsky, M., Watling, J., Danylyuk, O., Reynolds, N., 2022. Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February-July 2022, RUSI, London. https://rusi.org/explore-our-research/publications/special-resources/preliminary-lessons-conventional-warfighting-russias-invasion-ukraine-february-july-2022, 18. 2. 2023.*
58. *Zakon o obrambi (Uradni list RS, št. 103/04 – uradno prečiščeno besedilo, 95/15 in 139/20).*



**email: anze.rode@mors.si**
**email: lojze.pavic@mors.si**
**email: rok.ravnak@mors.si**

**e-mail: anze.rode@mors.si**

**Brigadir dr. Anže Rode** se je v Slovenski vojski zaposlil leta 1997 kot univerzitetni diplomirani inženir strojništva. Leta 2001 je magistriral na Fakulteti za družbene vede, leta 2011 pa je na Fakulteti za logistiko doktoriral iz vojaške obveščevalne dejavnosti. Leta 2018 je končal magisterij na US Army War College. Usposabljal se je v Zvezni republiki Nemčiji in v ZDA. Bil je v mednarodni operaciji in na misiji v Afganistanu leta 2010 ter na Kosovu leta 2014. Je načelnik štaba Generalštaba Slovenske vojske.

**Brigadier Anže Rode, PhD,** was employed by SAF as university graduated machine engineer in 1997. In 2001 achieved Master of Science on Faculty of social sciences with thesis on security policies and in 2011 achieved Master of Science in logistics on Faculty for logistics. In 2011 he achieved PhD on military intelligence. In 2018 achieved Master of Science in strategic studies on US Army War College. He accomplished military training in Germany and in United States. His deployments abroad include missions in Afghanistan in 2010 and Kosovo in 2014. At the moment he serves as Chief of Staff of the General Staff of the SAF.

**e-mail: lojze.pavic@mors.si**

**Podpolkovnik Lojze Pavič** je veteran vojne za Slovenijo, nosilec odlikovanja bojne akcije Brnik 1991 in spominskega znaka Obranili domovino 1991. Je načelnik sektorja za vojaško obveščevalno, protiobveščevalno in varnostno dejavnost na Generalštabu Slovenske vojske. Po obveščevalnem področju je opravljal poveljniške in načelniške dolžnosti tudi na mednarodnih misijah v tujini. Specializacijo je opravil na Fakulteti za družbene vede na temo sodobnega terorizma. Je avtor knjige Terorizem smo ljudje. Leta 2022 je diplomiral na Ratni školi Ban Josip Jelačić v Republiki Hrvaški.

**Lt. Col. Lojze Pavič** is a veteran of the war for Slovenia, recipient of the Brnik 1991 combat award and the award for defending the homeland in 1991. In the Slovenian Army, he serves as the head of the sector for military intelligence, counterintelligence and security activities at the General Staff of the Armed Forces. In the field of intelligence, he performed command and staff duties in the Slovenian Army and duties in the field of intelligence in international missions abroad. He completed his specialization at the Faculty of Social Sciences, on the subject of modern terrorism. He is the author of a book in this field entitled “Terrorism is people”. In 2022, he graduated from the “War college” Ban Josip Jelačić in the Republic of Croatia.

**e-mail: rok.ravnak@mors.si**

**Major Rok Ravnak** je pripadnik Slovenske vojske od leta 2000. Diplomiral je na Fakulteti za družbene vede v Ljubljani, na Oddelku za politologijo, in sicer na Katedri za obramboslovje. Na obveščevalno-varnostnem področju deluje od leta 2005, opravljal pa je tudi dolžnosti načelnika S-2 v 20. motoriziranem bataljonu v Celju in načelnika odseka za obveščevalne, protiobveščevalne in varnostne zadeve v 15. polku vojaškega letalstva v Cerkljah ob Krki. Je avtor vojaških strokovnih člankov v Reviji obramba. Je višji častnik za vojaške obveščevalne standarde in meteopodporo na Generalštabu Slovenske vojske.

**Major Rok Ravnak** has been member of Slovenian Armed Forces (SAF) since 2000. He graduated politology - defense studies on Faculty of Social Sciences in Ljubljana in 2000 and has been working in intelligence and security activities in SAF since 2005. Among other duties he served as head of S-2 sector in 20. Motorized battalion in Celje in years 2008 and 2009 and as the head of the sector for intelligence and security activities in military aviation 15. Wing in Cerklje ob Krki in years 2018-2022. He authored many articles on military matters for Revija Obramba defence magazine. At the moment he serves in the sector for intelligence, counterintelligence and security activities at the General Staff of the SAF.