ИНФОРМАЦИОНА ДИМЕНЗИЈА БЕЗБЕДНОСНОГ ОКРУЖЕЊА – ОСНОВНА ОБЕЛЕЖЈА*

Милан Миљковић**
Драган Јевтић***
Слободан Стојичевић****

Достављен: 01. 01. 2022.
Кориговано: 15. 02. 2022 и 07. 03. 2022.
Прихваћен: 06. 04. 2022.
Језик рада: Српски
Тип рада: Прегледни рад
DOI број: 10.5937/vojdelo2202018M

Информациону димензију савременог безбедносног окружења карактерише сложеност, преобиље неструктурираних информација и бројни сукоби који се воде путем информационог ратовања, што отежава анализу ове димензије. Модерна информациона технологија омогућила је свим учесницима у сукобу, пре свега недржавним актерима, да утичу на глобалну информациону димензију, а самим тим и на безбедносно окружење. Имајући у виду да у домаћој војној теорији до сада није представљена свеобухватна класификација и анализа информационе димензије безбедносног окружења, чланак има за циљ да представи, анализира и синтетизује актуелне стране теоријско-доктринарних приступа у вези с овим питањем.

Упоредна анализа и синтеза презентованих доктринарних приступа анализе информационе димензије указује на то да та анализа не може бити свеобухватна и функционална у војном смислу, уколико, осим анализе елемената, области, нивоа, актера и њихових способности деловања у информационој димензији, не обухвата и методе за анализу претњи и могућег деловања противника у информационој димензији.

* Рад је израђен као део научног пројекта Школе националне одбране „Војвода Радомир Путник“, Универзитета одбране у Београду, под називом „Неутралност и стратешко одвраћање”, у делу пројекта који разматра теоријске и практичне основе одвраћања у информационој димензији сукоба.

** Школа националне одбране „Војвода Радомир Путник“, Универзитет одбране у Београду, Београд, Република Србија, milanmiljkovic04011@gmail.com

*** Војна академија, Универзитет одбране у Београду, Београд, Република Србија.

**** Институт за националну стратегију, Нови Сад, Република Србија.

Може се закључити да само свеобухватна анализа структуре и актера информационе димензије може да пружи војним снагама информације о могућности њеног обликовања, односно могућности да деловањем кроз ову димензију утичу на потенцијалне противнике и тиме допринесу остваривању војних циљева и циљева националне безбедности.

Кључне речи: *информациона димензија, анализа, PMESII и ASCOPE метода, шаблон информационог деловања противника*

Увод

За државу и њен систем националне безбедности, безбедносно окружење је област у којој руководство државе и делови система безбедности сарађују или долазе у сукоб са другим државама или актерима ради унапређења стања националне безбедности**.** Анализа безбедносног окружења спроводи се ради сагледавања стања и трендова спољних и унутрашњих чинилаца окружења и њиховог утицаја на безбедност државе. Сагледавају се појединачни, кумулативни и хибридни утицаји војног, политичког, економског, информационог, социјалног, технолошког и других чинилаца који на различите начине утичу на безбедност државе.[1] Сваки наведени чинилац ствара специфичну димензију безбедносног окружења.

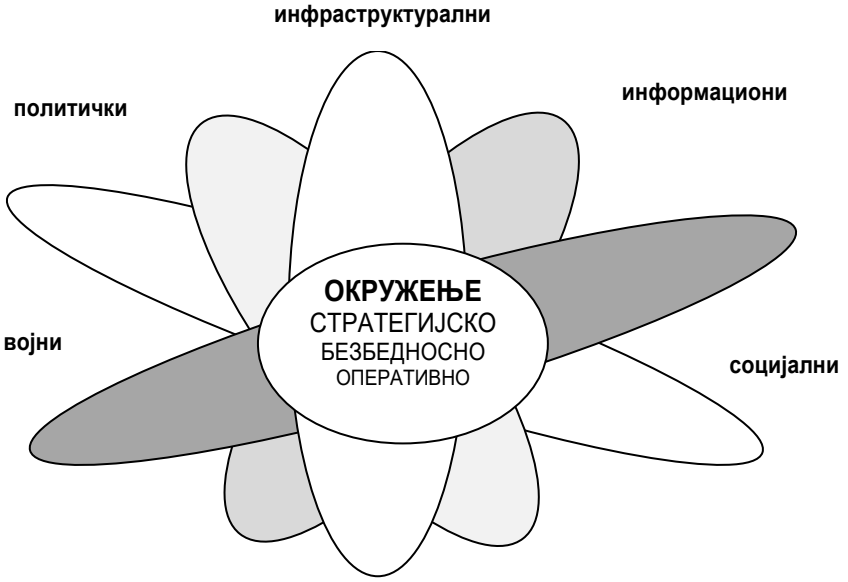
Актуелну фазу развоја и безбедности савременог друштва карактерише све већа улога информационе сфере, која представља скуп информација, информационе инфраструктуре, субјеката који прикупљају, формирају, шире и користе информације, као и система за регулисање насталих друштвених веза.[2] Информациона сфера се разматра као информациона димензија безбедносног окружења, која, као системски фактор у животу друштва, активно утиче на стање политичких, економских, одбрамбених и других компоненти безбедности националних држава. Одбрана сваке државе у савременом добу суштински зависи од заштите националних интереса у информационој димензији безбедносног окружења, а у будућем току технолошког напретка ова зависност ће се још повећавати.[3]

---

[1] Дејан Стојковић, „Израда стратегијских докумената Републике Србије у области безбедности и одбране", *Војно дело*, 6/2018, стр. 180.

[2] *Доктрина информационной безопасности Российской Федерации* (утверждена Указом Президента РФ № 646 от 5 декабря 2016 г., https://Совет Безопасности Российской Федерации, Доктрина информационной безопасности Российской Федерации (scrf.gov.ru)

[3] *Доктрина информационной безопасности Российсой Федерации*, утв. Президентом РФ от 9 сентября 2000 г. N Пр-1895, https://Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 09.09.2000 N Пр-1895) (утратила силу) | ГАРАНТ (garant.ru)



Слика 1 – *Врсте окружења и чиниоци (димензије) окружења*[4]

Информациона димензија је хетерогена глобална средина у којој људи и аутоматизовани системи посматрају, оријентишу се, одлучују и делују на основу података, информација и знања. Својом функцијом, као каналом за утицај на доношење одлука у сукобима, информациона димензија је кључна компонента безбедносног окружења. Карактерише је свеприсутност различитих медија, хиперповезаност актера, тако да данашња информациона димензија омогућава комуникацију и размену информација без преседана.[5] Савремене војне снаге морају да буду свесне информационе димензије, кроз континуирани процес њеног нагледања и анализе, као и могућности да деловањем кроз ову димензију утичу на потенцијалне противнике.

Основна обележја информационе димензије безбедносног окружења

Информациона димензија се дефинише као скуп појединаца, организација или система за прикупљање, обраду или дистрибуцију информација. Информациона димензија прожима и превазилази границе копна, мора, ваздуха, свеми-

[4] Слика прилагођена према шеми оперативног окружења из *Доктрине Војске Србије*, Медија центар „Одбрана", Београд, 2010, стр. 101.

[5] US Department of Defense Strategy for Operations in the Information environment, June 2016, DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf (defense.gov)

ра и сајбер простора.[6] Поједина обележја савремене информационе димензије, као што су преобиље информација, неструктуриране информације, проблематична вредност информација и ниске компетенције корисника информација, отежавају сагледавање и процену безбедносног окружења.[7]

Доносиоци одлука у савременим сукобима суочавају се са феноменом „преобиља информација" који је узрок растућих проблема са стварањем тачних обавештајних упозорења и честих пропуста обавештајних структура, тако да главни проблем који доводи до обавештајних пропуста није недостатак информација, већ „поплава информација".[8] Засипањем информацијама постиже се ентропијски ефект у самом процесу обавештавања, тј. долази до „обавештајног слепила".[9]

Такође, савремена информациона димензија довела је до трансформације савремених сукоба, чија обележја додатно отежавају правилно сагледавање безбедносног окружења. Један од основних видова савремених сукоба је информационо ратовање, које се користи ради деловања на непријатељске информације и информационе системе, као и изворе информација противника, али и на промену начина мишљења противничке стране.[10] Примарни циљ информационог ратовања јесте процес доношења одлука противничког руководства. Технолошким развојем информационог окружења развијају се и начини утицаја на противника и вођења информационог рата.[11]

Анализа и разумевање информационе димензије је предуслов за њено обликовање ради адаптације будућих услова у којима ће изводити војне активности. Сходно томе, у војним доктринарним документима САД, НАТО и Руске Федерације презентоване су одредбе у вези с анализом елемената, области, нивоа, актера и способности у информационој димензији. Наведени приступи и методе њене анализе биће представљене у даљем тексту.

---

[6] Милан Миљковић, Драган Јевтић, „Сукоби у информационом простору из угла савремене војне мисли у Руској Федерацији – искуства за безбедност Републике Србије", *Национални интерес*, Београд, број 2021/2, стр 108.

[7] Tomasz Kacała, „Military Leadership in the Context of Challenges and Threats Existing in Information Environment", *Journal of Corporate Responsibility and Leadership*, https://www.researchgate.net/publication/ 297751621, 08/12/2021.

[8] Milan Miljkovic, Vangel Milkovski, „Challenges facing information environment in contemporary conflicts", *Archibald Reiss Days 2020*, Belgrade, 18-19 November 2020, Thematic conference proceedingsof international significance, University of Criminal Investigation and Police Studies Belgrade, 2020, http://eskup.kpu.edu.rs/ dar/article/view/230/117, 08/11.2021.

[9] Милан Миљковић, „Изазови у раду обавештајних служби у информатичком добу", *Безбедност* 3/2020, стр. 148.

[10] Милан Миљковић, Драган Јевтић, „Сукоби у информационом простору из угла савремене војне мисли у Руској Федерацији – искуства за безбедност Републике Србије", *Национални интерес*, Београд, број 2021/2, стр 107.

[11] Нежданов Игорь Юрьевич, *Технологии информационных войн в интернете*, https://studylib.ru/doc/2333221 Технологии информационных войн в интернете (studylib.ru), 25/12/2021.

Анализа елемената и области информационе димензије

Као што је наведено, информациона димензија се дефинише као скуп информација, информационе инфраструктуре, субјеката који прикупљају, формирају, шире и користе информације, као и система за регулисање насталих друштвених веза.[12] Наведене одредбе из Доктрине информационе безбедности Руске Федерације из 2016. године представљају уједно ставове о основним елементима информационе димензије. Слични ставови наводе се и у америчкој војној теорији која дефинише информациону димензију као скуп индивидуа, организација и система који скупљају, обрађују, шире и реагују на информације.[13] У суштини, информациона димензија обједињује опипљиве физичке елементе (комуникационе системе и др.) и неопипљиве елементе (информације).

У складу са наведеном класификацијом, елементе информационе димензије разматрала је америчка корпорација РАНД[14] у документу „Редефинисање информационог ратовања војске у бежичном свету" у којем се наводи да информациону димензију чине и две делимично укрштајуће компоненте: друштвене мреже и сајбер простор.[15] Оцењује се да социјалне везе људи путем друштвених мрежа свакодневно расту и по релевантности и по утицају, утичући и на еволуцију савременог сукоба.

Изнетим теоријским и доктринарним одређењима представљени су ставови о основним елементима информационе димензије и извршена њена класификација на три подскупа елемената, што је довољно за почетну структуралну анализу ове димензије.

Питање даље класификације и анализе информационе димензије наставља се образлагањем теоријско-доктринарног приступа који је прихваћен и у западној и источној војној теорији, као и у нашој доктринарној теорији, а то је приступ који класификује и анализира главне области информационе димензије.[16] Војнодоктринарна теорија САД и НАТО, као и наша доктринарна документа, наводе да информациону димензију чине три области: физичка, информациона и сазнајна.[17] Америчка војна теорија износи да, у оквиру информационе димензије, учесници у сукобу мо-

[12] Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента РФ № 646 от 5 декабря 2016 г., https://Совет Безопасности Российской Федерации, Доктрина информационной безопасности Российской Федерации (scrf.gov.ru)

[13] US Department of Defense Strategy for Operations in the Information environment, June 2016, DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf (defense.gov)

[14] РАНД корпорација је америчка непрофитна организација која реализује истраживања и анализе за оружане снаге САД.

[15] Isaac R. Porche III, „Emerging Cyber Threats and Implications". *RAND Corporation* Santa Monica, CA, 2016. https://www.rand.org/pubs/testimonies/CT453.html, приступљено 07.03.2022.

[16] Упореди: AJP-3.10, NATO, Allied Joint Doctrine for Information Operations, 2015. стр. I-2; US Department of Defense Strategy for Operations in the Information environment, June 2016, - DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf (defense.gov); *Доктрина Војске Србије*, Медија центар „Одбрана", Београд, 2010, стр.101.

[17] *Доктрина Војске Србије*, Медија центар „Одбрана", Београд, 2010, стр. 101.

гу да очекују изазове кроз три међусобно повезане области: 1) *физичке области*, коју чине системи за командовање и комуникацију, као и пратећа инфраструктура која омогућава појединцима и организацијама стварање ефеката у вези са информацијама, 2) *информативне области*, сачињене од самог садржаја информација, укључујући начин на који се прикупљају, обрађују, складиште, дистрибуирају и штите и 3) *когнитивне области*, које чине ставови, уверења и перцепције оних који преносе, примају, реагују на информације или делују на основу њих.

Табела 1 – *Анализа елемената и области информационе димензије*

ОБЛАСТИ	ЕЛЕМЕНТИ АНАЛИЗЕ ИНФОРМАЦИОНЕ ДИМЕНЗИЈЕ
Физичка	– Физички свет и његов садржај, посебно онај који омогућава и подржава размену идеја, информација и порука. – Информациони системи и физичке мреже. – Комуникациони системи и мреже. – Људи и људске мреже. – Лични уређаји, ручни уређаји и графички кориснички интерфејс за друштвене медије. – Мобилни телефони, лични дигитални асистенти и графички корисник друштвених мрежа – интерфејси.
Информативна	– Садржај информација. – Квалитет и квантитет информација. – Токови информација. – Прикупљене, обрађене, ускладиштене, дистрибуиране, приказане и заштићене информације. – Софтвер за апликације за друштвене медије.
Когнитивна (сазнајна)	– Утицај информација на човекову вољу. – Контекстуалне информације и доношење човекових одлука. – Нематеријална улога, као што су морал, вредности, поглед на свет, свест о ситуацији, перцепције и јавна мишљења, веровања, емоције, систем вредности. – Менталне калкулације као одговор на стимулусе, попут допадања нечему у друштвеној заједници – медијска апликација.

Према Доктрини информационих операција НАТО-а, физичка област је област стварног света у којој се реализује међусобна интеракција појединаца, нација, култура и цивилизација; она укључује и људе, писане медије, предајнике, информационе и комуникацијске системе. Информациона област је усмерена на информације (енг. *data centric*) и представља везу између физичке и сазнајне области. Сазнајну област (енг. *human centric*), која је усмерена на људе, Доктрина НАТО назива психолошким доменом који обухвата перцепције, разумевање, веровање, емоције и систем вредности. На ове елементе утичу различити чиниоци попут: личних и културолошких веровања, норми, мотивације, осећања, искуства, морала, образовања, менталног здравља, идентитета и идеологија.[18]

[18] AJP-3.10, NATO, Allied Joint Doctrine for Information Operations, 2015. стр. I-2.

Западна војна теорија оцењује да сазнајна област чини најзначајнију компоненту информационе димензије, јер се ефекти у физичкој и информационој области на крају региструју као утицај на људску когнитивну област, што чини да ова област представља централни објекат анализе и мету приликом извођења активности у информационој димензији.[19]

Наведеним доктринарним ставовима извршена је другачија класификација информационе димензије на три области, објашњена је њихова функција и међусобни однос, и истакнута важност когнитиве (сазнајне) области. Детаљнији доктринарни прикази елемената анализе области информационе димензије, који су представљени у табели 1, дају основу за дубљу структуралну анализу ове димензије.

Анализа нивоа информационе димензије

Према америчким доктринарним погледима, информациона димензија безбедносног окружења у структуралном смислу има свој глобални, национални и војни контекст, односно ниво.[20]

Висока стопа развоја и примене интернета и електронских медија довела је, на прелазу у нови миленијум, до формирања глобалне информационе инфраструктуре и простора. Заједно са копном, морем, ваздухом и свемиром, ову информациону димензију активно су користиле војне снаге развијених земаља за решавање широког спектра војних задатака.[21] Глобална информациона инфраструктура представља глобално повезивање комуникационих мрежа, рачунара и база података које корисницима чине доступним огромне количине информација. Она не подразумева само физичке објекте који се користе за складиштење, обраду и представљање информација. Особље које доноси одлуке и рукује пренетим информацијама чини критичну компоненту глобалне информационе инфраструктуре.[22] У анализи глобалног контекста полази се од сагледавања повезаности конкретне информационе димензије са глобалном, где се посматра повезаност актера конкретног безбедносног окружења са глобалним медијима, страним владама и међународним политичким телима, посебно са онима који могу имати негативан утицај на активност безбедносних снага. Посебно се

[19] US Department of Defense Strategy for Operations in the Information environment, June 2016, DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf (defense.gov)

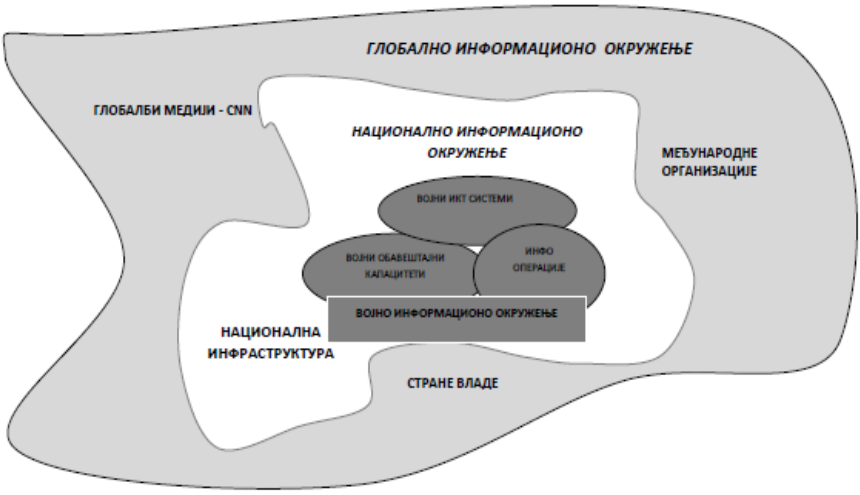
[20] Упореди: *Planner's Handbook for Operational Design*, Joint Staff, J-7, Joint and Coalition Warfighting Suffolk, Virginia, 7 October 2011, p A-14; *Information Operations, FM 100-6* , Headquarters, Department of the Army, p. 1-2; *Information Operations, Joint Publication 3-13*, 20 November 2014, p. GL-3, https://www.jcs.mil/Portals/36/Documents/ /Doctrine/pubs/JP 3-13, Information Operations (jcs.mil)

[21] Концептуальные взгляды на деятельность вооруженных сил Российской Федерации в информационном пространстве, Министерство обороны Российской Федерации, 2011 г. стр. 3.

[22] Упореди: Global Information Infrastructure, https://itlaw.fandom.com/wiki Global Information Infrastructure, The IT Law, Fandom; *Joint Doctrine for Information Operations (Joint Pub. 3-13),* U.S. Joint Chiefs of Staff, Oct. 9, 1998, at I-13 and I-14.

анализира противничка способност пробоја евентуалне информационе блокаде коју успостављају безбедносне снаге, као и међународна подршка противничком комуникационом и информационом систему.

Национална информациона инфраструктура представља националну интерконекцију комуникационих мрежа, рачунара и база података која корисницима ставља на располагање огромне количине информација.[23] Особље у држави које доноси одлуке и рукује пренесеним информацијама чини критичну компоненту националне информационе инфраструктуре.[24] Национална информациона инфраструктура је по природи и сврси слична глобалној, али се по обиму односи само на национално информационо окружење, које укључује сву владину и цивилну информатичку инфраструктуру.[25] У делу анализе националног информационог система противника сагледавају се техничке и друге способности националних комуникационих организација, национална радио, телевизијска и интернет инфраструктура. Анализира се и способност утицаја на глобалну и регионалну информациону димензију, као и карактер власничког капитала националних и регионалних медија: да ли су, и у ком проценту, власници интернет сервера, рутера и провајдерских услуга.



Слика 2 – *Нивои (контексти) информационе димензије*

[23] National information infrastructure, US DoD Definition, https://www.militaryfactory.com/dictionary/military-terms-defined.ph,term_id3588 national information infrastructure (US DoD Definition) (militaryfactory.com)

[24] *National Information Infrastructure (NII),* https://itlaw.fandom.com/ National Information Infrastructure | The IT Law| Fandom *; Joint Doctrine for Information Operations (Joint Pub. 3-13),* U.S. Joint Chiefs of Staff, Oct. 9, 1998, at at GL-7 and GL-8

[25] *Ibid,* I-14.

Војна информациона инфраструктура је мрежа комуникационих мрежа, рачунара, софтвера, база података, апликација, али и објеката и људи и других могућности који задовољавају потребе за информацијама војних снага и снага одбране у миру, кризним ситуацијама и у рату.[26] При анализи војнокомуникационе инфраструктуре и димензије испитују се карактеристике противничког одбрамбеног информационог система, његова локација, хардверски и софтверски стандарди његових телекомуникационих система и способности одбрамбеног информационог система за извођење информационог ратовања и операција, као и способности за прикупљање релевантних обавештајних информација. У вези с том способношћу, посебно се анализира да ли је противник развио доктринарно-нормативне аспекте информационог ратовања, да ли је изградио организацију и саставе за информационо деловање, као и да ли има довољно људских и материјалних ресурса за такво дејство.

Иначе, америчка доктринарна теорија указује на то да се савремене војне снаге суочавају са проблемом експанзије глобалног информационог окружења, али и са ширењем националне и војне информационе инфраструктуре. С тим у вези, наводи се да традиционалне границе између држава, између војних и политичких домена, као и између војних и цивилних домена, постају све нејасније у информационом добу. Због прекограничне природе и архитектуре глобалних информационих мрежа у којима информације теку више или мање слободно преко државних граница, и у којима националне информационе инфраструктуре постају неодвојиви делови глобалне информационе инфраструктуре, политичке границе, као и границе између војне и цивилне сфере постају порозне. Ширење бојног простора на виртуелни простор и на људску перцепцију доводи до већег учешћа цивилних снага у савременим сукобима. По будућем сценарију ратовања, класичан војни сукоб више није крајњи чин, јер информациона димензија пружа много ниже трошкове и боље услове за тајно покретање сукоба.[27]

Ставови о класификацији и анализи нивоа информационе димензије на глобални, национални и војни, иако се делом усмеравају на анализу техничке карактеристике инфраструктуре, дају нови квалитет, указујући на критичан значај међусобне повезаности ових нивоа, посебно везе са глобалним нивоом, имајући у виду његов значај и утицај на однос светског јавног мњења према сукобу, као и на важност људи као критичним елементом анализе. Додатни квалитет представљају ставови о потреби анализе способности у оквиру војног нивоа, за извођење информационог ратовања и утицаја на глобалну информациону димензију, са тежиштем на постојање доктринарно-нормативне теорије, организације и састава, људских и материјалних ресурса за информационо деловање.

[26] Упореди: *Capstone Requirements Document: Global Information Grid 70* (GIG), JROCM 134-01, U.S. Joint Forces Command, Aug. 30, 2001; *U.S. DoD Information Technology Security Certification and Accreditation Process (DITSCAP)*. U.S. Department of Defense, DoD Instruction 5200.40, Dec. 30, 1997.

[27] Myriam Dunn, *Information Age Conflicts A Study of the Information Revolution and a Changing Operating Environment*, Zurich, November 2002, P 38-39, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/ZB_64.pdf/ Information Age Conflicts (ethz.ch)

Анализа способности актера информационе димензије

Теоретичари наводе да се актери информационе димензије могу поделити на неколико група, на основу својих интересовања и активности. То су: *појединци* којима нове технологије пружају прилику без преседана да постану директно укључени у јавне комуникације, затим *медији* који користе традиционалне и нове канале за масовне комуникације, *приватне компаније* које прикупљају и одржавају информације, нудећи или продајући приступ њима, *државне и локалне институције*, *предузећа* која користе комуникационе канале за маркетинг и одржавање веза са својим клијентима, *разне интересне групе* (укључујући политичке странке, јавне организације и удружења) и други *недржавни актери* који комуницирају са својим учесницима и присталицама.[28]

Приликом разматрања актера, у доктринарној војној теорији се наводи да је један од главних изазова у савременој информационој димензији и кључни покретач активности у њој драматична и стална дифузија информација и технологија коју користе како појединци, мањи и недржавни актери, тако и државе.[29] Ниска цена активности које се спроводе у информационом окружењу, било путем друштвених медија, формалне штампе, сајбер активности или неким другим средствима, дала је недржавним и мањим актерима на међународном плану одређене предности и опције за деловање о којима су могли само да сањају пре 20 година. Дифузија моћи употребом информационе технологије омогућила је појединцима и групама да утичу на глобалну информациону сферу. Способност информационог деловања ради друштвених и политичких промена некада је била ексклузивна способност држава. Међутим, данас и појединци имају способност да креирају, трансформишу и шире информације на глобалном нивоу како би мобилизовали друштвене и политичке активности и промене.

Брзо ширење информација доводи у питање способност неких држава да контролишу своје становништво и одржавају унутрашњу политичку стабилност.[30] Приступ информацијама и информационим платформама, готово у реалном времену, пружа јавности могућност и платформу за оспоравање легитимитета активности државних органа у кризним ситуацијама. Ови јавни форуми могу да утичу на јавно мњење и да наметну јавну оцену да је активност безбедносних снага неприхватљива пракса, као

[28] Inta Brikše, *The information environment: theoretical approaches and explanations*, p 383-384. Brikše I (2006). In: Informācijas vide Latvijā: 21. gadsimta sākums. Riga: Zinātne, pp. 368–415. Available at: https://www.szf.lu.lv/fileadmin/user_upload/szf_faili/ Petnieciba/sppi/mediji/inta-brikse_anglu.pdf

[29] Joint Concept for Operating in the Information Environment (JCOIE), United States Department of Defense, 25 July 2018

[30] Robert Ehlers, *Making Old Things New Again: Strategy, the Information Environment, and National Security*, January 3,2017.
https://thestrategybridge.org/the-bridge/2017/1/3/making-old-things-new-again-strategy-the-information environment-and-national-security, 25/10/2021.

и да повећавају осетљивост јавности на колатералну штету.[31] Често се догађало да су легитимне снаге биле неспремне и неспособне да одговоре на велику количину вишеканалних информационих дејстава и пропаганде која се шаље путем текста, видеа, звука и слика које се шире путем интернета, друштвених медија, сателитске телевизије и традиционалних медија.

Прилагодљиви недржавни актери вешто користе информације како би стекли предност у односу на државне актере. То захтева разумевање информационе димензије и активности које се спроводе у њој, односно активности информационог ратовања.[32] Због свега наведеног, при анализи актера информационе димензије посебно се анализира њихова способност извођења активности информационих ратовања и операција, као што је приказано у табели 2.

Табела 2 – *Способности и активности којима актери делују у информационој димензији*

Врсте ИО активности	Активности	Циљне групе/циљеви	Циљ активности	Ко спроводи активност
Електронско ратовање	Електронски напад	Физички/ информациони	Уништити, ометати, одлагати	Појединци, владине институције, војска
	Електронска одбрана	Физички	Обезбедити коришћење електромагнетног спектра	Појединци, компаније, владине институције, војска
	Подржавајуће активности	Физички	Идентификовати и лоцирати претњу	Војска, обавештајни органи
Компјутерске мрежне операције	Компјутерске нападне операције	Физички/ информациони	Уништити, ометати, одлагати	Појединци, владине институције, војска
	Компјутерске одбрамбене операције	Физички/ информациони	Заштитити компјутерску мрежу	Појединци, компаније, владине институције, војска
	Компјутерске обавештајне операције	Информациони	Прикупити информацију из компјутера и компјутерске мреже противника	Појединци, владине институције, војска
Психолошке операције	Психолошко пропагандне активности	Когнитивни	Утицај на емоције, понашање и одлуке противника	Компаније, владине институције, војска
Војно обмањивање	обмањивање	Когнитивни	Обманути	Војска
Оперативна безбедност	Безбедност сопствених операција	Когнитивни	Негирати	Компаније, владине институције, војска
Блиске активности	Цивилно-војни односи	Когнитивни	Утицај	Владине институције, војска
	Јавни послови	Когнитивни	Информисати	Владине институције, компаније
	Јавна дипломатија	Когнитивни	Информисати	Владине институције

[31] Colin S Gray, *Recognizing and understanding revolutionary change in warfare: The Sovereignty of Context. Carlisle*, Strategic Studies Institute, U.S. Army War College, 1 February 2006. https://ssi.armywarcollege.edu/2006/pubs/recognizing-and-understanding-revolutionary-change-in-warfare-the sovereignty-of-context. 01/11/2021.

[32] Joint Concept for Operating in the Information Environment (JCOIE), United States Department of Defense , 25 July 2018

Америчка војна теорија дефинише информационе операције као координацију пет централних активности којима се делује у информационој димензији. Те активности су: психолошке операције, војно обмањивање, оперативна безбедност, електронско ратовање и компјутерско-мрежне операције.[33]

Презентована анализа актера информационе димензије, иако у основи има структурални прилаз, квалитативним ставовима о способностима појединаца и недржавних актера у односу на државне актере и војне снаге, даје додатни квалитет и функционални аспект анализе информационе димензије, указујући на важност анализе способности деловања у информационој димензији, као и на недостатке и слабости државних актера у овим активностима.

Анализа информационе димензије уз употребу PMESII и ASCOPE матрице

Војске и обавештајно-безбедносне службе западних земаља користе различите комбинације модела како би унапредиле перцепцију окружења.[34] Ови модели, који су углавном засновани на анализи „инструмената националне моћи", познати су по акронимима DIME, DIMEFIL, ASCOPE и PMESII.[35]

Метод за анализу безбедносног окружења, односно оперативног окружења када се ради о војним снагама, назван PMESII, представља холистички приступ за анализу окружења који је развило Министарство одбране САД ради унапређења анализе спољашњег окружења и развијања бољих стратегија према безбедносним претњама у Ираку и Авганистану.[36] Приручник Оружаних снага САД за извођење борбених операција у иностранству, под називом FM 3-0, значајно се фокусира на употребу модела PMESII за анализу спољних чинилаца који

[33] Милан Миљковић, *Посебност информационих операција у раду савремених обавештајних служби*, Факултет Безбедности, Београд, 2016, стр. 29-30.

Посебност информационих операција у раду савремених обавештајних служби (mpn.gov.rs) https://nardus.mpn.gov.rs/handle/123456789/ 8473.

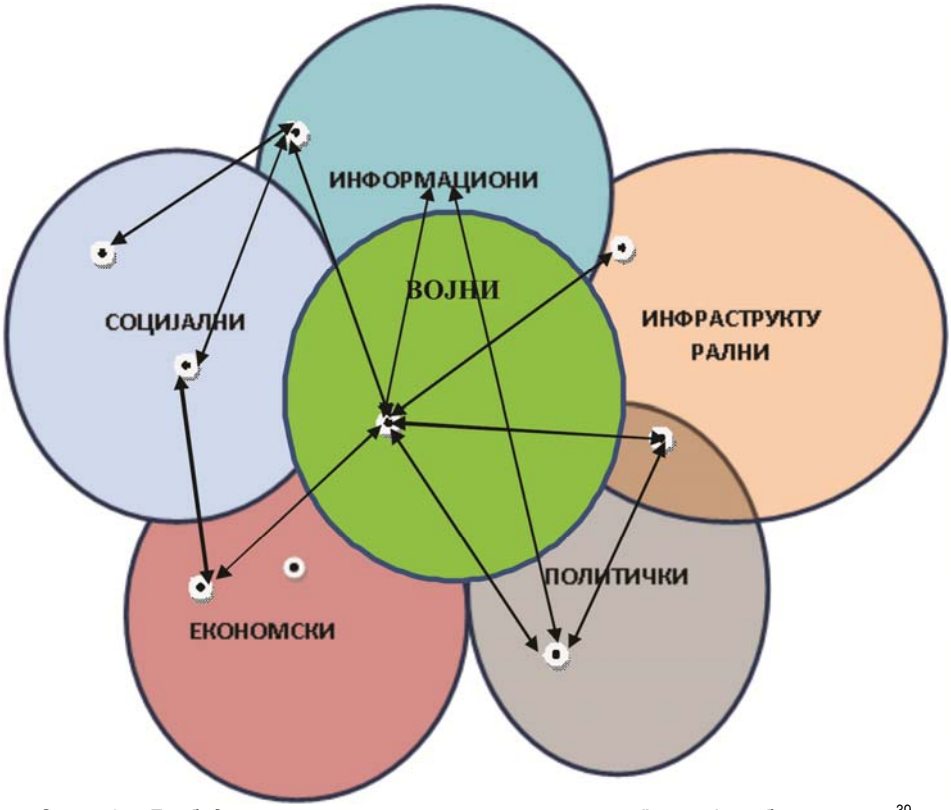
[34] Види: Fred Bruls and A. Walter Dom, „Human Security Intelligence: Towards a Comprehensive Understanding of Complex Emergencies", *Open Source Intelligence in the Twenty-First Century New Approaches and Opportunities,*https://walterdorn.net/pdfHumanSecurityIntel_Bruls-Dorn_OSI-Book_Palgrave-Macmillan_June2014.pdf; Jack Kern, 'Understanding the Operational Environment: The Expansion of DIME, Military Intelligence (2007), Vol. 33, No. 2, p.l., https://www.proquest.com/docview Understanding the Operational Environment: The - ProQuest, 21/12/2021.

[35] Акроними: DIME (*diplomatic, information, military and economic*, тј. дипломатски, информациони, војни и економски); DIMEFIL (*diplomatic, information, military, economic, financial, intelligence and law*

enforcement, тј. дипломатски, информациони, војни, економски, финансијски, обавештајни и правни), ASCOPR (areas, structures, capabilities, organizations, people and events, тј. области, структуре, способности, организације, људи и догађаји) и PMESII (political, military, economic, social, information and infrastructure, тј. политички, војни, економски, друштвени, информациони и инфраструктурни).

[36] *Researching with pmesii-pt analysis*, Researching with PMESII-PT Analysis, DINFOS Pavilion, Article

могу да утичу на америчке војне операције.[37] Овај модел постао је и стандард за анализу спољњег окружења мировних операција које спроводе земље чланице НАТО-а.[38] Чинилац, односно димензија коју истражује модел PMESII јесте и информациона димензија.



Слика 3 – *Безбедносно окружење као „систем система" са међусобним везама*[39]

Филозофски посматрано, ова метода има посебан значај јер посматра безбедносно окружење као „систем система" који се налазе у међусобној у интеракцији. Другачије речено, посматра се интеракција информационе димензије са осталим димензијама безбедносног окружења. Доктринарна теорија указује на то

[37] Види: US Army, Field Manual 3-0: Operations (Washington, DC, 2008).

[38] Метода *PMESII* је једна од неколико техника анализе безбедносног окружења, укључујући: *SWOT* анализу (снага, слабост, прилике, претње), *PESTLE* анализу (политички, економски, социјални, технолошки, правни и еколошки) и *QUEST* анализу (техника брзог скенирања околине).

[39] *Исто.*

да информациона променљива приказује природу, обим и ефекте појединаца, организација и система који прикупљају, обрађују, шире или делују на информације у безбедносном окружењу. Информационо окружење разматра формална и неформална средства комуникације међу људима, као и употребу ефекта глобалног информационог окружења на одређено безбедносно окружење. Примери питања који се користе за анализу веза са информационом променљивом су: каква је природа јавних комуникационих медија, колико је контролисано или отворено информационо окружење и које су могућности противника за вођење информационог ратовања у наведеном операционом окружењу.[40]

Метода PMESII често се комбинује са методом ASCOPE. Комбиновање ова два модела у матрици пружа користан алат за војне снаге ради бољег разумевања и анализирања безбедносног окружења. Иначе, модел ASCOPE се користи за анализу цивилног аспекта безбедносног окружења у следећим димензијама:

– *области*: анализа утицаја кључних цивилних подручја на војне операције и обрнуто;

– *структуре*: анализа физичке инфраструктуре, као што су зграде, мостови, путеви, железнице и комуникациони торњеви;

– *способности*: анализа способности које су потребне у окружењу за одржавање и унапређење живота, као што су храна, хитне службе и здравствена заштита;

– *организације*: анализа присуства, активности и организационог састава невојних група и институција у окружењу с обзиром на њихов утицај на становништво, војне мисије и обрнуто;

– *људи*: анализа невојних лица у окружењу у смислу мишљења, деловања и политичког утицаја;

– *догађаји*: анализа догађаја у окружењу који утичу на становништво, војне операције, невојне организације, верске и националне празнике и изборе.

Због сложености табеле, и теме чланка, биће приказана само информациона димензија анализирана према моделу ASCOPE.

Табела 3 – *Анализа информационе димензије помоћу модела ASCOPE*[41]

Анализа информационог фактора – модел ASCOPE	
Области	– Подручје које покрива емитовање државне телевизије – Подручје у којем постоји досег друштвених медија – Подручје у којем се користи метод „од уста до уста” – Подручје где се користе „графити”

[40] *Operational Environment and Army Learning*, Headquarters, Department of the Army, Washington, DC, 26 November 2014, p 1-6, https://armypubs.us.army.mil/doctrine/index.html

[41] *The conduct of information operations*, ATP 3-13.1, Headquarters, Department of the Army, Washington, DC, 04 October 2018, p. 2-6., https://irp.fas.org/doddir/army/atp3-13-1.pdf. 01/11/2021; *The application of COIN doctrine and theory,* A Counterinsurgent's Guidebook, Counterinsurgency Training Center – Afghanistan, KABUL, Version 2: November 2011, p 12. https:// info.publicintelligence.net/CTC-A-COIN-Guidebook.pdf. 11/12/2021.

Структуре	– Торањ за мобилну телефонију – Антена или објекат за емитовање ТВ и радио-програма – Физичка структура за интернет – Поштанске услуге – Штампарија
Способности	– Медијске операције – Штампане новине – Платформе за друштвене медије – Стопа писмености – Обавештајне агенције – Приступ интернету
Организације	– Медијске агенције – Агенције за односе са јавношћу и испитивање јавног мења – Групе и агенције за социјалне медије – Новинске агенције
Људи	– Доносилац политичких одлука – Старешине – Верске вође – Личности од утицаја на интернет форумима (*influencer*)
Догађаји	– Цензура – Објављивање важних догађаја и датума – Лансирање важних вести преко интернета – Брифинг за штампу – Прекид емитовања програма

Метода PMESII, иако се у основи заснива на анализи елемената информационе димензије, представља нови квалитет анализе, јер приказује природу, обим и ефекте појединаца, организација и система који прикупљају, обрађују и делују у информационом окружењу. Примена модела ASCOPE обогаћује анализу, имајући у виду да познате елементе анализе сагледава на квалитетно другачији начин, као и да уводи „догађаје од значаја за информациону димензију" као елемент анализе. Ове методе помажу у бољем организовању, синтези и примени информација као кључном делу стратешког размишљања и одлучивања.

Анализа претњи и могућег деловања противника у информационој димензији

После наведених приступа структуралне анализе, анализираће се доктринарни приступ функционалне анализе информационе димензије који помаже да се боље и сликовитије представи утицај информационе димензије на активности војних снага, као и да се идентификују потенцијалне претње и рањивости

које војне снаге могу да искористе у сукобу, односно да се од њих заштите.[42] Овај модел анализе садржи четири фазе:

– дефинисање информационе димензије,

– описивање ефеката информационе димензије,

– процену информационе ситуације и претње, и

– утврђивање праваца деловања противника у информационој димензији.

У оквиру фазе дефинисања информационе димензије, идентификују се обележја све три њене сфере (физичке, информативне и когнитивне) унутар зоне дејства сопствених снага, и то оне које могу утицати на сопствене снаге, односно које могу негативно да утичу на токове сопствених операција и на процес доношења одлука сопственог командног кадра. У ту сврху анализирају се следећи елементи информационе димензије:

– *терен (и време),* који са физичког, географског и атмосферског аспекта утиче на садржај и проток информација,

– *становништво*, где се проучавају демографски и језички фактори,

– *друштвене структуре*, где се идентификују неформалне социјалне и друштвене мреже,

– *државна (органи власти) и војна информационо-комуникациона инфраструктура*, за потребе командовања, као и за потребе доношење одлука државних органа,

– *цивилна информациона и комуникациона инфраструктура*, која преноси информације кроз цело информационо окружење,

– *медији у зони операције* који могу утицати на дејства сопствених и противничких снага,

– *независне и невладине организације*, чији се ставови разликују од званичних.

У оквиру друге фазе описивања ефеката информационог окружења, анализирају се обележја информационог окружења која су идентификована у првом кораку, ради утврђивања њиховог утицаја на сопствене и противничке активности у свакој димензији. Као и раније, и у овој фази тежиште је на опису могућег утицаја активности противничких снага, терена и временских прилика, као и цивилног фактора, на активности сопствених снага. У овој фази је важно да се утврде могућности информационог деловања непријатељских снага, концептуални и доктринарни ставови везани за информационо деловање, односно способности за утицај на информациону димензију. Описивање начина на који цивилно окружење може да утиче на сопствене и противничке операције помаже да се изабере и одреде циљеви сопственог информационог деловања (информациони напад, одбрана или стабилизација) или одговарајућа комбинација деловања. Табела 4 илуструје анализу могућег утицаја медија, становништва и комуникационе инфраструктуре на све три сфере информационе димензије.

[42] *The conduct of information operations*, ATP 3-13.1, Headquarters, Department of the Army, Washington, DC, 04 October 2018, p. 2-1., https://irp.fas.org/doddir/army/atp3-13-1.pdf. 01/11/2021.

Табела 4 – *Пример анализе могућег утицаја медија, становништва и комуникационе инфраструктуре на области информационе димензије*[43]

Медији	**Сазнајни**	Медијске куће имају генерално позитиван став према нашим безбедносним снагама и операцијама.
	Информа-циони	Вести медијских кућа покривају око 68% популације и тежишно извештавају о случајевима криминала, корупције и социјалним проблемима.
	Физички	Радио-инфраструктура је застарела, постоји мањи број сателитске опреме, присутна је комбинација стационираних и покретних антена за мобилну телефонију.
Становништво	**Сазнајни**	Постоји делимична подршка владајућој партији. Нема отворене подршке акцијама безбедносних снага.
	Информа-циони	Становништво увелико размењује информације методом „од уста до уста", а највише је заинтересовано за економска и социјална питања.
	Физички	75% популације су Срби, а 25% остали. 65% посто популације живи у градским срединама.
Информацио-но-комуника-циона инфра-структура	**Сазнајни**	Становништво има делимично поверење у инфратруктуру.
	Информа-циони	Због непоуздане инфраструктуре размена информација је отежана, па становништво у великој мери размењује информације путем нетехничких средстава.
	Физички	Ограничена земљана комуникациона мрежа, због чега се користи мобилна телефонија као замена. Торњеви мобилне телефоније су мете напада због чега су несигурни.

У оквиру трећег корака спроводи се *процена информационе ситуације и претњи у информационој димензији*. У овој фази анализирају се могућности противника за информационо деловање, његови доктринарни принципи, тактике и технике, укључујући и начин на који распоређују своје снаге за деловање у овој димензији. У идеалном случају, анализа деловања противника у информационој димензији заснована је на моделовању или шаблонирању. Два уобичајена алата која се користе јесу утврђивање шаблона информационог деловања противника и анализа његових „центара гравитације". Шаблони информационог деловања противника су резултат пажљиве анализе његових способности, његове рањивости, доктринарних принципа и пожељних тактика, техника и поступака који заузврат воде ка развоју модела информационог деловања противника. Они се представљају визуелно (на карти или дигиталној мапи), уз поштовање основних доктринарних принципа информационог деловања противника и обично обухватају три различита шаблона:

– шаблон доношења одлука или размене информација противника,
– шаблон информационе инфраструктуре противника и
– шаблон примене доктрине информационог деловања противника.

[43] *The conduct of information operations*, ATP 3-13.1, Headquarters, Department of the Army, Washington, DC, 04 October 2018, p. 2-11., https://irp.fas.org/doddir/army/atp3-13-1.pdf. 01/11/2021.

Шаблон доношења одлука противника приказује „чворове и везе људи" које он користи за размену информација, са посебним нагласком на начине на које политички и војни руководиоци примају и размењују информације. За израду овог шаблона потребно је разумевање организационих структура противника, важних веза и међусобних односа кључног особља које утиче на процес доношења одлука. Шаблон информационе структуре противника приказује средства које он користи за размену информација. Шаблон доктрине информационог деловања противника моделује начин на који он распоређује или користи своје информационе ресурсе и могућности.

Четврти корак анализе представља *утврђивање праваца деловања противника у информационој димензији* и обухвата поступак у шест корака који укључују: идентификовање вероватних циљева противника и жељеног крајњег стања у информационој димензији, идентификовања свих могућих варијанти његовог деловања у информационом димензији, евалуацију и степеновање по значају сваке варијанте тог деловања, детаљно моделовање и разраду сваке варијанте његовог деловања, утврђивање циљева противничког информационог деловања за сваку варијанту, и утврђивање података који су потребни противнику да би започео планирање сваке варијанте деловања.

Иако шаблони деловања противника уважавају доктринарне принципе противника, његове уобичајене методе и обрасце деловања, они морају да прикажу како он може информационо да делује прилагођавајући своје снаге, способности и доктрину конкретном оперативном окружењу. У табели 5 приказан је пример шаблона информационог деловања противника.

Табела 5 – *Пример шаблона информационог деловања противника*

ШАБЛОН ИНФОРМАЦИОНОГ ДЕЛОВАЊА ПРОТИВНИКА	
Циљеви информационог деловања противника: – Спречити супротну страну да прикупља обавештајне податке. – Деградирати противнички командни и информациони систем. – Подстаћи незадовољство цивила код противника.	
Јавне информације	**Задатак**: У медијима истицати колатералне грешке и употребу неприлагођене силе од стране противничких оружаних снага. **Циљ**: Дискредитовати мисију противничке коалиције. **Метод**: Међународни медији, локални радио и ТВ.
Пропаганда	**Задатак**: Утицати на јавно мњење (расељене цивиле). **Циљ**: Изазвати ометање коалиционих операција. **Метод**: Штампани пропагандни материјали, АМ радио-програм, ХУМИНТ агенти.
Електронско ратовање	**Задатак**: Ометати радио-везе противничких оружаних снага на тактичком нивоу противника. **Циљ**: Спречити прикупљање података сопственим снагама у првој линији. **Метод**: Јединица за електронско ратовање.
Специјалне операције	**Задатак**: Нападати командна места противника. **Циљ**: Успорити офанзивне операције противника. **Метод**: Директна акција, артиљеријска ватра.

Представљени приступ анализе претњи и могућег деловања противника у информационој димензији представља квалитетнију анализу, имајући у виду да њени резултати треба да идентификују потенцијалне могућности, претње и рањивости у информационој димензији које војне снаге могу да искористе у сукобу, односно да се од њих заштите. Посебно се истиче значај анализе шаблона који се односи на доношење одлука противника, као и утврђивање могућих праваца његовог деловања у информационој димензији.

Закључак

У досадашњој домаћој војној теорији није извршено свеобухватно сагледавање обележја, као ни класификација и анализа савремене информационе димензије безбедносног окружења. Наиме, у нашој доктринарној теорији извршена је само класификација информационе димензије на когнитивну, физичку и информациону област, при чему су укратко описани елементи ових области, без дубљег сагледавања њихових међусобних веза и односа. То не представља довољну основу за квалитетну анализу која ће војним снагама дати основе за њено упознавање и процену вероватног начина информационог деловања противника. Страна доктринарна литература пружа више примера класификације и анализе информационе димензије, различитих нивоа квалитета.

Када је у питању опште обележје информационе димензије, може се закључити да њена сложеност и вишедимензионалност отежавају процену безбедносног окружења. С тим у вези, анализа саме информационе димензије помаже да се боље и сликовитије идентификују претње, али и потенцијалне информационе могућности које војне снаге могу да искористе у сукобу.

Сагледавање страних теоријско-доктринарних приступа класификације и анализе информационе димензије указује на то да један део приступа представља парцијалне структуралне анализе, пружајући сагледавање само елемената и области, само нивоа, или актера и њихових способности деловања у информационој димензији, уз низак ниво анализе њихових међусобних односа и веза, што их чини недовољно функционално применљивим за војне снаге. Позитивно је то што наведени приступи указују на значај когнитивне области информационе димензије као најважнију и уједно централну област анализе и мете информационог деловања. Приступ који у структуралном смислу сагледава глобални, национални и војни контекст информационе димензије доноси додатни квалитет, јер се њиме сагледава међусобни однос ових нивоа, као и релевантни противнички капацитети и способности.

Анализа актера информационе димензије, квалитативним ставовима о способностима појединаца и недржавних актера у односу на државне актере и војне снаге, даје додатни квалитет и функционални значај, указујући на важност анализе способности деловања у информационој димензији, као и на недостатке и слабости државних актера у овим активностима.

Примена методе PMESII, иако се у основи заснива на анализи основних елемената информационе димензије (субјеката, система и организација), представља квали-

тетну анализу јер приказује природу, обим и ефекте појединаца, организација и система који прикупљају, обрађују и делују у информационом окружењу. Такође, представља користан алат за дубље разумевање и анализу информационе димензије у којој се налазе безбедносне снаге, поготово ако су у противничким окружењу. Примена модела ASCOPE обогаћује анализу, имајући у виду да познате елементе анализе сагледава на квалитетно другачији начин, као и да уводи „догађаје од значаја за информациону димензију" као елемент анализе. Ове методе помажу у бољем организовању и синтези информација као кључног дела стратешког размишљања и одлучивања.

Доктринарни приступ који се усмерава на анализу претњи и могућег деловања противника у информационој димензији представља функционалну анализу која садржи четири фазе, и то: 1) дефинисање информационе димензије, 2) описивање ефеката информационе димензије, у којој се користи PMESII и ASCOPE матрица, 3) процену информационе ситуације и претње, у оквиру које се утврђује могући шаблон и доктрина информационог деловања противника у конкретној ситуацији и 4) утврђивање праваца деловања противника у информационој димензији.

Може се закључити да само свеобухватна анализа, која сагледава елементе, области, нивое, актере и њихове способности деловања у информационој димензији, као и анализу претњи и могућег деловања противника у тој димензији, може да пружи војним снагама потпуну слику информационе димензије, али и функционалне информације о могућности да деловањем кроз ову димензију утичу на потенцијалне противнике и тиме допринесу остваривању како војних, тако и циљева националне безбедности.

Литература

[1] *Allied Joint Doctrine for Information Operations*, AJP-3.10, NATO, 2015.

[2] *Capstone Requirements Document: Global Information Grid 70* (GIG), JROCM 134-01, U.S. Joint Forces Command, Aug. 30, 2001; *U.S. DoD Information Technology Security Certification and Accreditation Process (DITSCAP)*. U.S. Department of Defense, DoD Instruction 5200.40, Dec. 30, 1997.

[3] Colin S Gray, *Recognizing and understanding revolutionary change in warfare: The Sovereignty of Context. Carlisle*, Strategic Studies Institute, U.S. Army War College, 1 February 2006. https://ssi.armywarcollege.edu/2006/pubs/recognizing-and-understanding-revolutionary-change-in-warfare-the sovereignty-of-context. 01/11/2021.

[4] *Critical Infrastructure Protection XV*, 5th IFIP WG 11.10 International Conference, ICCIP 2021, Virtual Event, March 15–16, 2021, Revised Selected Papers.

[5] Дејан Стојковић, „Израда стратегијских докумената Републике Србије у области безбедности и одбране", *Војно дело*, 6/2018, стр. 180.

[6] *Доктрина информационной безопасности Российсой Федерации*, утв. Президентом РФ от 9 сентября 2000 г. N Пр-1895, https://Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 09.09.2000 N Пр-1895) (утратила силу) | ГАРАНТ (garant.ru)

[7] *Доктрина Војске Србије*, Медија центар „Одбрана", Београд, 2010, стр. 101.

[8] *Доктрина информационной безопасности Российской Федерации* (утверждена Указом Президента РФ № 646 от 5 декабря 2016 г., https://Совет Безопасности Российской Федерации, Доктрина информационной безопасности Российской Федерации (scrf.gov.ru)

[9] Fred Bruls and A. Walter Dom, „Human Security Intelligence: Towards a Comprehensive Understanding of Complex Emergencies", *Open Source Intelligence in the Twenty-First Century New Approaches and Opportunities,*
https://walterdorn.net/pdfHumanSecurityIntel_Bruls-Dorn_OSI-Book_Palgrave-Macmillan_June2014.pdf;

[10] Global Information Infrastructure, https://itlaw.fandom.com/wiki Global Information Infrastructure | The IT Law | Fandom;

[11] *Information Operations, FM 100-6*, Headquarters, Department of the Army, 1996.

[12] *Information Operations, Joint Publication 3-13*, 20 November 2014.

[13] Inta Brikše, *The information environment: theoretical approaches and explanations*, p 383-384. Brikše I (2006). In: Informācijas vide Latvijā: 21. gadsimta sākums. Riga: Zinātne, pp. 368–415. Available at: https://www.szf.lu.lv/fileadmin/user_upload/szf_faili/Petnieciba/sppi/mediji/inta-brikse_anglu.pdf

[14] Isaac R. Porche III, „Emerging Cyber Threats and Implications". *RAND Corporation* Santa Monica, CA, 2016.
https://www.rand.org/pubs/testimonies/CT453.html, приступљено 07.03.2022. године.

[15] Jack Kern, „Understanding the Operational Environment: The Expansion of DIME, Military Intelligence" (2007), Vol. 33, No. 2., https://www.proquest.com/docview Understanding the Operational Environment: The – ProQuest, 21/12/2021.

[16] *Joint Concept for Operating in the Information Environment* (JCOIE), United States Department of Defense, 25 July 2018.

[17] *Joint Doctrine for Information Operations (Joint Pub. 3-13),* U.S. Joint Chiefs of Staff, Oct. 9, 1998.

[18] Концептуальные взгляды на деятельность вооруженных сил Российской Федерации в информационном пространстве, Министерство обороны Российской Федерации, 2011.

[19] Милан Миљковић, „Изазови у раду обавештајних служби у информатичком добу", *Безбедност* 3/2020, стр. 148.

[20] Милан Миљковић, Драган Јевтић, „Сукоби у информационом простору из угла савремене војне мисли у Руској Федерацији – искуства за безбедност Републике Србије", *Национални интерес*, Београд, број 2021/2, стр. 108.

[21] Милан Миљковић, Драган Јевтић, „Сукоби у информационом простору из угла савремене војне мисли у Руској Федерацији – искуства за безбедност Републике Србије", *Национални интерес*, Београд, број 2021/2, стр. 107.

[22] Милан Миљковић, *Посебност информационих операција у раду савремених обавештајних служби*, Факултет Безбедности, Београд, 2016, стр. 29-30.

[23] Milan Miljkovic, Vangel Milkovski, „Challenges facing information environment in contemporary conflicts", *Archibald Reiss Days 2020*, Belgrade, 18-19 November 2020, Thematic conference proceedingsof international significance, University of Criminal Investigation and Police Studies Belgrade, 2020
/http://eskup.kpu.edu.rs/ dar/article/view/230/117, 08/11.2021.

[24] Myriam Dunn, *Information Age Conflicts A Study of the Information Revolution and a Changing Operating Environment*, Zurich, November 2002, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/ZB_64.pdf/ Information Age Conflicts (ethz.ch)

[25] *National Information Infrastructure (NII),* https://itlaw.fandom.com/ National Information Infrastructure | The IT Law| Fandom *;*

[26] Нежданов Игорь Юрьевич, *Технологии информационных войн в интернете*, https://studylib.ru/doc/2333221 Технологии информационных войн в интернете (studylib.ru), 25/12/2021.

[27] *Operational Environment and Army Learning*, Headquarters, Department of the Army, Washington, DC, 26 November 2014. https://armypubs.us.army.mil/doctrine/index.html

[28] *Planner's Handbook for Operational Design*, Joint Staff, J-7, Joint and Coalition Warfighting Suffolk, Virginia, 7 October 2011, p A-14;

[29] *Researching with pmesii-pt analysis*, Researching with PMESII-PT Analysis, DINFOS Pavilion, Article. 12/12/2021.

[30] Robert Ehlers, *Making Old Things New Again: Strategy, the Information Environment, and National Security*, January 3,2017. https://thestrategybridge.org/the-bridge/2017/1/3/making-old-things-new-again-strategy-the-information environment-and-national-security, 25/10/2021.

[31] *The conduct of information operations*, ATP 3-13.1, Headquarters, Department of the Army, Washington, DC, 04 October 2018, p. 2-6. https://irp.fas.org/doddir/army/atp3-13-1.pdf, 01/11/2021.

[32] *The application of COIN doctrine and theory,* A Counterinsurgent's Guidebook, Counterinsurgency Training Center – Afghanistan, KABUL, Version 2: November 2011, https:// info.publicintelligence.net/CTC-A-COIN-Guidebook.pdf. 11/12/2021.

[33] Tomasz Kacała, „Military Leadership in the Context of Challenges and Threats Existing in Information Environment", *Journal of Corporate Responsibility and Leadership*, https://www.researchgate.net/publication/ 297751621, 08/12/2021.

[34] *US Department of Defense Strategy for Operations in the Information environment*, June 2016, DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf (defense.gov)

[35] US Army, Field Manual 3-0: Operations (Washington, DC, 2008).

Р е з и м е

Информациону димензију савременог безбедносног окружења карактерише сложеност, преобиље неструктурираних информација и бројни сукоби који се воде путем информационог ратовања. Наведена сложеност информационе димензије и проблем исправног сагледавања безбедносног окружења актуелизује питање примене савремених и проверених метода за њихову анализу. Ове методе представљају користан алат за разумевање информационе димензије, поготово ако се ради о страном или противничком окружењу и помажу у ор-

ганизовању, синтези и примени информација као кључног дела комуникационог планирања и стратешког размишљања и одлучивања.

Структурална анализа информационе димензије обухвата анализу: а) *елемената информационе димензије*, пре свега информационе инфраструктуре, системе и уређаје за прикупљање, пренос, обраду и достављање информација, информације и њихове токове, као и персонал и организације које обављају различите делатности у вези са информацијама, б) *области информационе димензије*, тј. физичку, сазнајну и информациону област, в) *нивоа информационе димензије*, који се деле да глобални, национални и војнобезбедносни ниво и г) *актера информационе димензије*, пре свега појединце, недржавне и државне актере, усмерујући анализу на њихове способности деловања у информационој димензији, односно извођења информационих операција.

Функционална фаза анализе информационе димензије, с друге стране, садржи следеће фазе: 1) дефинисање информационе димензије, 2) описивање ефеката информационе димензије, у којој се користи PMESII и ASCOPE матрица, 3) процену информационе ситуације и претње, у оквиру које се утврђује могући шаблон и доктрина информационог деловања противника у конкретној ситуацији и 4) утврђивање праваца деловања противника у информационој димензији.

Може се закључити да само свеобухватна анализа, која сагледава све елементе структуре информационе димензије, као и елементе функционалне анализе, пружа војним снагама потпуно сагледавање информационе димензије и функционалне информације о могућности обликовања информационе димензије ради деловања на противничке снаге и лакшег остваривања задатака.

Кључне речи: *информациона димензија, анализа, PMESII и ASCOPE метода, шаблон информационог деловања противника*