БЕЗБЕДНОСТ

ЧАСОПИС МИНИСТАРСТВА УНУТРАШЊИХ ПОСЛОВА РЕПУБЛИКЕ СРБИЈЕ

БЕОГРАД, година LXIII 1/2021

„БЕЗБЕДНОСТ“

Часопис Министарства унутрашњих послова Републике Србије

УРЕДНИШТВО

ГЛАВНИ И ОДГОВОРНИ УРЕДНИК
Доц. др Божидар Оташевић

УРЕДНИК
Јасмина Владисављевић

ЛЕКТУРА И КОРЕКТУРА
Јасмина Милетић

ЛЕКТОР ЗА ЕНГЛЕСКИ ЈЕЗИК
Весна Анђелић-Николенцић

АДРЕСА УРЕДНИШТВА:
Булевар Зорана Ђинђића 104
011/3148-734, 3148-739, e-mail: upobr@mup.gov.rs

ЧАСОПИС ИЗЛАЗИ ТРИ ПУТА ГОДИШЊЕ
(тираж: 800 примерака)

ШТАМПА:
Комазец, Краља Петра 1, бб, Инђија

PDF верзија часописа доступна је на адреси:
http://www.mup.gov.rs у поднаслову Публикације

Архива старих бројева од 1/2000 до 3/2015 доступна је на линковима:
http://prezentacije.mup.gov.rs/upravazaobrazovanje/bezbednost_s3.html
http://prezentacije.mup.gov.rs/upravazaobrazovanje/bezbednost_s4.html
http://prezentacije.mup.gov.rs/upravazaobrazovanje/bezbednost_s5.html

САДРЖАЈ

ОРИГИНАЛНИ НАУЧНИ РАДОВИ

ПРЕГЛЕДНИ НАУЧНИ РАДОВИ

CONTENTS

ORIGINAL SCIENTIFIC PAPERS

REVIEW PAPERS

Проф. др Ненад ПУТНИК[*]
Универзитет у Београду – Факултет безбедности
Др Бранислав МИЛОСАВЉЕВИЋ[**], научни сарадник
Институт за стратегијска истраживања, Универзитет одбране

ДОИ: 10.5937/bezbednost2101062P
УДК: 355.01:316.77/.776(470+477)
Прегледни научни рад
Примљен: 10. 1. 2021. године
Датум прихватања: 4. 3. 2021. године

Руске информационе операције у украјинском оружаном сукобу

Апстракт: *Крајњи циљеви и основни облици друштвених сукоба остали су непромењени током историје. Па ипак, данас је евидентно проширење у примени нових метода, техника и средстава за вођење рата. Непрекидном фузијом револуционарних достигнућа на пољу рачунара, сателитских комуникација и медија радикално су унапређене могућности ратовања, и поред тога што технолошка достигнућа нису суштински изменила геостратешке и политичко-економске циљеве самог рата. Сајбер простор је пружио енормне могућности за спровођење специјалних пропагандних дејстава, као и за извођење напада посредством рачунарских мрежа на противничке информационе системе, и тиме проширио простор за спровођење информационих операција. Информационе операције се могу водити самостално или као подршка конвенционалном, кинетичком сукобу.*

Аутори у раду указују на значај који информационе операције имају у савременим оружаним конфликтима на примеру сукоба у Украјини. У уводу рада дат је преглед различитих појмовних одређења информационих операција. Затим је спроведена анализа руског теоријског и стратешко-доктринарног приступа информационом ратовању. Након тога, на украјинском примеру објашњене су специфичности *информационих операција са ста-*

[*] nputnik@fb.bg.ac.rs
[**] branislav.milosavljevic@mod.gov.rs

новишта њиховог садржаја, обима, места и улоге у савременим оружаним сукобима.

Рад треба посматрати као полазну тачку ширег дискурса јер у задатом обиму није могуће расправљати о овом питању у свој његовој сложености и целовитости. Драматични догађаји у Украјини су нам недвосмислено указали да информациони аспект хибридног рата ни на који начин не треба потценити нити занемарити.

Кључне речи: *информационе операције, друштвени конфликти, украјински сукоб, медији, пропаганда.*

Увод

Једна од многобројних дефиниција информационих операција (енгл. *Information operations*) под ове активности сврстава прикупљање тактичких информација о противнику као и ширење пропаганде зарад постизања конкурентске предности над противником (RAND, 2021). Стручњаци за информационе операције (енгл. *spin doctors*) стварају жељени ефекат помоћу информације, проналазећи и измишљајући начине да се она уверљиво представи (Тофлер, Тофлер, 1998).

Информационе операције нису појава новијег датума. Историјски посматрано, изразу *информационе операције* претходио је израз *информација у рату*. Данас се у војним доктринама већине Западних земаља синонимно употребљавају и изрази *информационо ратовање* и *информације утицаја*.

Без обзира на плуралитет израза и непостојање консензуса по питању њихове употребе, чињеница је да се они односе на војни аспект пропагандних активности и да упућују на офанзивну и дефанзивну употребу информација и средстава информисања у смислу искоришћавања, поткупљивања, кварења и уништења противничких информација и система који их преносе, уз истовремену заштиту властитих информација и система. У складу са овим одређењем, може се тврдити да се вођење информационог рата, као континуираног спровођења информационих операција, заснива на три принципа: сазнати, спречити другога да дође до сазнања и навести друге да дођу до неистинитог сазнања. У том смислу, могуће је разликовати три вида информационог рата: рат за ин-

формацију, рат кроз информацију (помоћу дезинформације) и рат против информације (Путник, 2012).

Информационо ратовање је облик специјалног рата у коме се информације користе као циљеви и средства ратовања, при чему се могу разликовати два аспекта ових активности – офанзивни и дефанзивни. Први аспект подразумева спровођење активности са циљем добијања поузданих, потпуних и благовремених информација о противнику, док се други односи на спречавање противника да дође до наших властитих штићених информација. Благовремено сазнавање потребних података о противнику (бројност, распоред и кретање непријатељске војске, опремљеност наоружањем, стање морала и сл.) не само да олакшава планирање и извођење војних операција, већ је уједно и предуслов за било какве озбиљније активности у домену рата, спољне политике, спољне трговине, економског и маркетиншког освајања тржишта, берзанског пословања, техничко-технолошких иновација и индустријског развоја. У том смислу, информационо ратовање представља коришћење информација као циља напада, али и као посебног оружја – средстава ратовања (Кривокапић, 2010).

Савремена технологија нуди различите могућности за извођење напада на противничке информационе системе. Неке од њих подразумевају рушење веб-сајтова влада противничких држава или неовлашћену измену њиховог садржаја, тајно убацивање погрешних података у информациони систем противника и друго (Molander et. al., 1996). Међутим, оно што информационо ратовање чини посебно примамљивим јесте широк спектар асиметричних могућности за смањење борбеног потенцијала противника. Због значаја који има, често се употребљава и синтагма „стратегијско информационо ратовање“, која подразумева различите војне и невојне мере и активности. На пример, ометање војног и државног руководства противника, његово довођење у заблуду, формирање пожељног јавног мњења, организација антивладиних активности и слично, као вид пропратне подршке у активностима смањења противникових способности (Sazonov, 2016: 68).

Догађаји из релативно блиске прошлости као што су грузијско-осетијско-руски сукоб, и такозване револуције у боји у Египту, Сирији, Либији и Украјини сведоче томе у прилог. У свим наведеним случајевима катализатор сукоба биле су субверзивне

информационе активности спроведене путем телевизије, радија, друштвених мрежа и електронских медија с циљем иницирања или ширења социјалних протеста, продубљивања конфликта, државног удара и слабљења државе у политичком, економском и социјалном смислу.

Руски теоријски и стратешко-доктринарни приступ информационом ратовању

Корени руске теорије информационог ратовања могу се наћи у теорији специјалне пропаганде која се од 1942. године изучава на Војном институту страних језика. Руски приступ информационом ратовању има својства интердисциплинарне примењене науке, с обзиром на то да покрива широк спектар акција (политичке, економске, социјалне, војне, обавештајне, контраобавештајне, дипломатске, пропагандне, психолошке, информационе, комуникационе, образовне и друге) (Darczewska, 2014: 9).

Руски приступ информационом ратовању није у сагласности са теоријама информационог ратовања и сајбер безбедности развијеним првенствено у САД и западној Европи. Опште узев, може се рећи да западна терминологија уопште није адекватна за објашњење руског приступа овом феномену. Тако изрази *сајбер ратовање*, *информационо ратовање* и *мрежно ратовање* у Русији имају потпуно различита значења (Атаманов, 2010).

Само неколико теоретичара разликује *сајбер рат* и *мрежни рат* као манифестације технолошке и социјалне димензије ратова четврте генерације. Међутим, ово се углавном односи на публикације у којима се расправља о западним ставовима. Насупрот томе, већина руских аутора схвата *информационо ратовање* као утицај на свест маса и као део ривалства између различитих цивилизацијских система, које су различите државе успоставиле у информационом простору помоћу посебних средстава за контролу информационих ресурса као „информационог оружја“. У том смислу, они не праве разлику између војног и невојног аспекта, технолошког (сајбер простор) и друштвеног поретка (информациони простор), и задржавају наратив из периода Хладног рата и *психолошког рата* између Истока и Запада. Из руске перспективе гледано, информационо ратовање је појам који се обично разматра у

два контекста: 1) као скуп дефинисаних задатака из опуса Доктрине о безбедности информација Руске Федерације и 2) као геополитичко ривалство Русије и Запада (пре свега САД и НАТО), које има политичку, идеолошку и културолошку димензију.

Геополитички и функционални („информациони ратови против Русије“) контексти су уско повезани. Геополитичка доктрина третира информације као јефтино и опасно оружје, универзално по карактеру, са неограниченим дометом, лако доступно, које превазилази све државне границе без ограничења. Борба информација и мрежа (чешће информационо-психолошка борба), укључујући њене екстремне форме попут информационо-психолошког и мрежног ратовања, средства су која држава користи за постизање својих циљева на међународном, регионалном и домаћем политичком плану, а такође и да стекне геополитичку предност.

Представници руске геополитичке мисли Игор Панарин и Александар Дугин имали су посебан утицај на популаризацију ове теме. Ови теоретичари посматрају потезе противника као организоване и усмерене акције, софистицираније од оних које су коришћене током периода Хладног рата. Њихов допринос огледа се у освешћивању руске јавности о постојању спољних информационих претњи, као и у обликовању руског система за борбу против информационих кампања (Darczewska, 2014: 9).

Руска стратешка документа посматрају информационо ратовање као део савременог хибридног рата који се састоји од комбинације политичких, војних, техничких, дипломатских, економских, информационих и психолошких средстава. Руска перспектива заснована је на идеји да је главни борбени простор ум, те да су у ратовима нове генерације доминантни информациони и психолошки аспекти, јер се помоћу њих постиже супериорност у контроли трупа и оружја, морала, као и психолошког депримирања људства непријатељских оружаних снага и цивилног становништва (Berzins, 2014).

Стратегија националне безбедности Руске Федерације не обрађује појам информационих операција на директан начин, али садржаји њених појединих делова јасно указују на информационо ратовање и његове алате. Тако је, на пример, посебним одредбама наглашено да је „појачана конфронтација у глобалној арени информација изазвана тежњом појединих држава да користе информа-

ционе и комуникационе технологије за постизање својих геополитичких циљева, укључујући манипулацију свешћу јавности и фалсификовање историје, што има све већи утицај на природу међународних односа“ (Стратегия национальной безопасности Российской Федерации до 2020 года, 2009: пар. 21). Осим тога, у параграфу 43 Стратегије у претње држави и јавној безбедности сврставају се и активности повезане са употребом информационих и комуникационих технологија у циљу ширења и промовисања идеологије фашизма, екстремизма, тероризма и сепаратизма и угрожавања грађанског мира и политичке и социјалне стабилности у друштву. То недвосмислено указује да је Русија свесна ефикасности и моћи савремених дезинформационих кампања и пропаганде.

Војна доктрина Руске Федерације специфичнија је у погледу дефиниције појма *информационо ратовање*. У њој се, у параграфима 11, 12 и 13, посебно наглашава да постоји тенденција преусмеравања војних ризика и војних претњи у информациони простор и унутрашњу сферу Руске Федерације. Интерни војни ризици односе се на „субверзивне активности информисања против становништва, посебно његовог млађег дела, усмерене на поткопавање историјске, духовне и патриотске традиције везане за одбрану отаџбине“ (Military Doctrine of the Russian Federation, 2014). Поред тога, у параграфу 62 Доктрине указује се и на постојање спољних војних ризика по Руску Федерацију међу којима је и „употреба информационих и комуникационих технологија у војно-политичке сврхе у циљу предузимања радњи које су у супротности са међународним правом, а које су усмерене против суверенитета, политичке независности, територијалног интегритета државе и уједно представљају претњу глобалној безбедности и стабилности“ (Military Doctrine of the Russian Federation, 2014).

Концепт спољне политике Руске Федерације сматра да је мека моћ постала саставни део напора за постизање спољнополитичких циљева. То пре свега укључује алате које нуди цивилно друштво, као и различите методе и технологије – од информација и комуникација, до хуманитарних и других средстава. У складу са предметним концептом важна је теза према којој Русија „настоји да обезбеди да свет има објективну слику те државе, да развије сопствене ефективне начине за утицај на међународну јавност с

циљем промовисања Русије и руских медија у глобалном информационом простору, пружајући им неопходну државну подршку, као и да спроводи проактивну међународну информациону сарадњу уз предузимање неопходних мера како би сузбила претње њеној информационој безбедности. У том циљу користи се нова информационо-комуникациона технологија. Русија намерава да промовише низ правних и етичких норми у погледу безбедне употребе такве технологије, и уједно потврди право сваког појединца на приступ објективним информацијама о глобалним дешавањима и различитим гледиштима“ (Foreign Policy Concept of the Russian Federation, 2016: пар. 61, 62).

Најрелевантнији стратешки документ који се дотиче информационог ратовања јесте *Доктрина информационе безбедности Руске Федерације*. Овај документ фокусиран је искључиво на информациону безбедност Руске Федерације и у њему су дате операционалне дефиниције кључних појмова: информациона безбедност, информациона област, информационе претње и информациона инфраструктура. Доктрина такође идентификује националне интересе Руске Федерације у информационом подручју, главне информационе претње, стратешке циљеве и кључна подручја за осигурање информационе безбедности, као и институционални оквир информационе безбедности (Doctrine of Information Security of the Russian Federation, 2016).

Без икакве сумње, Русија посебну пажњу посвећује информационој безбедности, информационом ратовању и његовим алатима, при чему дугогодишње руско искуство са пропагандом у комбинацији са масовним улагањима у медије чини ратовање информацијама најопаснијим безбедносним претњама са којима се тренутно суочавају државе чланице ЕУ и НАТО.

Остали званични документи, као што је Доктрина о безбедности информација Руске Федерације, концептуални погледи у вези са активностима Оружаних снага Руске Федерације у информационом простору, као и основна начела државне политике Руске Федерације у области међународне безбедности информација, третирају операције путем рачунарске мреже као саставни део информационе безбедности. То је такође видљиво у терминологији која се користи у руским стратегијама и доктринама. Уместо западне *сајбер безбедности*, централно место има *инфор-*

мациона безбедност (рус. *информационная безопасность*). То упућује на закључак да Русија информације посматра не само са техничког већ и са когнитивног аспекта.

Поред наведеног, важно је напоменути и постојање снажне перцепције да је Русија постала стална мета информационог ратовања (Panarin, 2012). Отуда је и разумљива намера да се дефинише и заштити граница руског „информационог окружења" или „информационог простора". Чињеницу да је Русија свесна разлика у употреби терминологије, што је јасно видљиво у стратегијско-доктринарним документима, поткрепљује и академски дискурс који посвећује посебну пажњу информацијама. Информације су постале оружје, при чему оне не представљају само прост додатак ватреној снази, нападу и маневру, већ и трансформацију и обједињавање свега тога. У научном дискурсу можемо уочити и покушаје потпунијег разумевања западњачких ставова о феноменима у сајбер простору и настојањима да се створи адекватна терминологија која је потребна за сузбијање страног утицаја (Balybin et al., 2014).

Потенцијална снага информација чврсто је укорењена у руском војном и политичком промишљању. Штавише, Русија сматра да је мета информационог рата, при чему руска научна литература јасно даје до знања да постоји раскол између Русије (или „историјског руског света", чији је Украјина део) с једне стране, и „Запада" са САД као главним протагонистом, с друге стране. Из те перспективе САД континуирано спроводи информационе операције против других држава. Тако је распад Совјетског Савеза резултат онога што Панарин назива „првим информационим ратом". Увод у „други информациони рат" био је петодневни рат у Грузији, августа 2008. године, а он је настављен и континуирано се води против Русије и Сирије (Панарин, 2018).

Савремени оружани сукоби одвијају се путем неоружаних и оружаних дејстава. Сукоб обично започиње неоружаним активностима (специјалним операцијама), а наставља се (по потреби) оружаним дејствима у којима неоружана и даље трају. Неоружана дејства трају непрекидно, док се оружана, ако до њих дође, догађају повремено и ациклично. Према томе, може се констатовати да савремени рат у многим својим аспектима почиње да зависи од примене психолошких операција. Ко успе да задобије сопствена и

противничка „срца и умове“, или да их не изгуби, изаћи ће као победник у конфликту (Lätsch, Moccand, 2010).

Специфичност украјинског сукоба

У циљу потпунијег разумевања информационог аспекта украјинског сукоба од посебне је важности размотрити разлог избијања украјинске кризе. Реакцију Русије на догађаје у Украјини који су се одвијали од 2013. године, посебно је анализирао Збигњев Бжежински који је Украјину пре две деценије описао као важан простор на Евроазијској шаховској табли, и чија је контрола предуслов да Русија постане снажна империјална држава која обухвата Европу и Азију. Независност Украјине 1991. године тешко је прихваћена од стране патриотски оријентисаних руских политичких група јер је, између осталог, представљала пораз стратегије Русије у покушају геополитичке контроле простора око руских граница. Повратак геополитике увек је био важан фактор за Русију у остваривању њене међународне политике након распада Совјетског Савеза, а губитак Украјине је умањио њену могућност да влада црноморским регионом, у коме Крим и Одеса имају важан не само историјски већ и стратешки положај у Црном мору, па чак и Медитерану (Бжежински, 1997: 46). Историјски посматрано, Украјина је увек била део наратива везаног за стварање руске нације. Украјина има посебно место у руским националним митовима у којима се Кијев традиционално посматра као „мајка свих руских градова“, па се с правом може тврдити да Украјина игра не само кључну улогу у руском геополитичком стратешком размишљању, већ има и симболичку вредност као простор руске цивилизације (Петровић, 2008: 65).

Интензивна борба за „срца и умове” украјинског становништва почела је још 2004. године, кроз активности супротстављених политичких актера у овој држави. До ескалације унутрашњих сукоба дошло је крајем 2013. године на протестима на кијевском Тргу независности. Јануковичев споразум о економској помоћи с Руском Федерацијом, наштрб преговора с Европском унијом, „проевропски“ опредељени грађани Украјине окарактерисали су као издају националних интереса. Западни медији одмах су ове догађаје описали као украјинску револуцију, али је тешко сложи-

ти се с тим да су догађаји на Тргу одговарали појму револуције. Револуција подразумева радикалну промену друштвено-економског и политичког система државе. Насупрот томе, захтеви демонстраната на Тргу независности сводили су се на захтев за промену власти унутар истог, капиталистичког, система друштвених односа. У најкраћем, захтеви демонстраната били су напуштање блиских односа са Руском Федерацијом и стварање партнерских са Сједињеним Америчким Државама и Европском унијом.

Од 2014. године улога стварне војне интервенције била је мала у односу на различите форме асиметричног рата, као што су информациони рат, економске мере, сајбер рат и психолошки рат на свим нивоима. Наведене форме асиметричног рата називају се једним именом – хибридни рат. У хибридном рату оружана сила се углавном користи као средство одвраћања, а не као средство отворене агресије. Међутим, овај сукоб је као новину донео високу ефикасност и координацију различитих средстава (од политичких, војних и специјалних операција до информационих мера и активности) која се у многим случајевима одвијала скоро у реалном времену (Sazonov, 2016: 67-68). У таквим околностима, иако релативно невидљива, доминантна је улога служби безбедности сукобљених страна. У том смислу, амерички Стејт департмент истакао је да Русија наставља да спинује лажи и неистине како би оправдала своје илегалне акције у Украјини. Тако је, на пример, тврдња Кремља да руски агенти нису активни у Украјини оповргавана наводним чињеницама да је украјинска Влада у априлу 2014. године ухапсила више од десет Руса за које се сумњало да су припадници руских обавештајних служби. У првој недељи априла 2014. године, Влада Украјине је добила информацију да су руски „ГРУ“ официри активирали појединце у Харкову и Доњецку, са саветима и инструкцијама да се воде протести, заузимају и држе под опсадом зграде владе, одузима оружје из владиних магацина и користи за друге насилне акције (Američki Stejt Department, 2014: 14-22). На крају, ваља поменути и утицај глобалног тренда приватизације на рат и учешће великог броја плаћеника на обе стране, што умногоме употпуњује слику сложености украјинског сукоба и разгранатост његових форми.

Информационо ратовање у Украјини

На савремене ратове је веома тешко применити класични Клаузевицев приступ, који подразумева да оружани конфликт започиње објавом рата, те да се заснива на суровим, али легитимним поступцима. Актуелна руска војна доктрина из децембра 2014. године експлицитно наводи да је у савременим ратним дешавањима информациона супериорност преко потребна да би се постигла победа на физичком бојном пољу.

У савременим оружаним сукобима циљ је потпуна стратешка парализа непријатеља и урушавање његових капацитета за пружање отпора. То се постиже циљањем на виталне тачке не само система одбране већ и друштвеног система као целине. Ратна ситуација се посматра као скуп међусобно повезаних друштвених подсистема које је потребно онеспособити, што се чини на различите начине: директним оружаним путем, економским акцијама, циљањем на информационе токове, или дипломатским деловањем, које је највећим делом засновано на притиску да се одређене радње изврше, или на одвраћању силом. Када је реч о информационим операцијама руске стране у Украјинском сукобу, на западу се најчешће спомињу „Раша тудеј“ и „Спутњик“ као носиоци информационе кампање преко масовних медија. Поред тога, коришћени су и многи руски национални телевизијски канали као што су *LifeNews*, *Россия1*, *Россия 24*, *Первый канал*, *НТВ*, *РЕН ТВ*, као и многи други, између осталог и они који су у Украјини забрањени, али их је ипак могуће пратити преко сателита.

Међутим, то су само јасно уочљиви елементи у веома широком спектру деловања, који укључује и оне чије су активности биле прикривене. С тим у вези, медији су имали другачије приступе и користили су различите форме информација, од пласирања једноставних дезинформација, преко полуистина, до софистицираних аргумената. То је имало за циљ стварање информационе доминације руске стране.

Руска пропагандна машинерија није имала за циљ само војнике, већ и њихове рођаке и пријатеље. Циљ је био поделити породицу и друге друштвене групе, узимајући у обзир процене даљег погоршања сукоба у складу са етничким, верским, језичким, политичким и регионалним идентитетом. У остварива-

њу овог циља коришћене су различите методе манипулације информацијама у мас-медијима, зарад остваривања превласти у информационо-психолошком аспекту сукоба. Према руским изворима основни принципи медијске кампање су:

- скривање критичних (важних) информација,
- скривање драгоцених података у маси бескорисних информација,
- поједностављење, потврда и понављање информација,
- „директне“ лажи које имају сврху дезинформисање домаћег становништва и међународне јавности,
- увођење забране за одређене облике информација или категорије вести,
- употреба концепата и термина чије је значење нејасно, што отежава стварање праве слике догађаја,
- препознавање слика, захваљујући чему медијски познати политичари и друге личности могу учествовати у акцијама и на тај начин вршити утицај на следбенике и њихов поглед на догађаје и
- пружање негативних информација, које ће јавност лакше прихватити него позитивне (Жутдиев et al., 2014: 12).

С друге стране, Украјина је показала потпуну неприпремљеност за свеобухватни информациони рат. У каснијим фазама оружаног сукоба, она је реаговала на ширење руских медија углавном ограничено, тежећи да руском свеприсуству у националном информационом простору парира јачањем контрапропаганде у украјинским медијима и стварањем законодавног оквира за осигурање доминантног положаја садржаја на украјинском језику у националним медијима. Међутим, за сада украјинска страна нема довољно капацитета за дугогодишњи информациони сукоб са руском страном.

Анализирајући специфичност руског информационог рата против Украјине, треба напоменути да је Украјина била (и углавном је још увек) изузетно рањива на медијску офанзиву Русије. Присуство „пете колоне“ у украјинском медијском систему, владиним органима, јавним удружењима и политичким странкама представљали су пресудно важан фактор руске доминације. Међутим, не смемо заборавити да је у ширењу информација умногоме коришћено проруско расположење великог дела украјинског ста-

новништва, посебно у Источном региону. Медијска агресија је омогућена повољним условима као што су недостатак језичке баријере, ментална сличност грађана обе државе, заједничка историја, извесна близина националних култура, огромна мрежа породичних контаката и друго (Pashkov, 2017: 109).

Суочена са озбиљном опасношћу, Украјина је усвојила одређене безбедносне мере како би се супротставила руском ширењу информација. Тако је у децембру 2014. године формирала Министарство информационе политике, а касније, октобра 2015. године, покренула је Међународну мултимедијалну платформу националног карактера. У периоду 2015–2016. године увела је пакет санкција против руских медија, новинара, уметника и издавачких кућа. Украјинска влада отказала је међувладин споразум са Русијом о сарадњи у области телевизије и радио-дифузије у периоду 2014–2016. године. Поред тога, Национални савет за радио и телевизију забранио је емитовање 78 руских ТВ канала. Украјинска државна филмска агенција забранила је емитовање преко 500 руских филмова и ТВ серија у биоскопима и на телевизијским каналима. У октобру 2016. године основан је Међународни информативни конзорцијум „Бастион“, како би се супротставио руском информационом утицају (Oleksandr Turchynov, 2016).

Значајан утицај у супротстављању руској информационој агресији имала је и нова Доктрина безбедности информација у Украјини. У том документу се посебно апострофира да „Русија користи најновије информационе технологије за утицај на људске умове у Украјини, с циљем подстицања националне и верске тензије и ширења пропаганде, залажући се уједно за агресивни рат и насилну промену уставног поретка, кршења суверенитета и територијалног интегритета украјинске државе“ (Decree of the President of Ukraine, 2017). То је уједно један од покушаја супротстављања „деструктивном утицају Русије у контексту хибридног рата“. Ипак, украјинске контрамере су у великој мери ситуационе, секторске и далеко су од тога да представљају адекватан одговор руској експанзији. Истовремено, распоређивање ефективног отпора који би обухватио читав социокултурни спектар ометан је недостатком државне политике, а самим тим свеобухватне подршке информационим активностима (Analytical report of the Razumkov Centre, 2015).

Русија ће несумњиво наставити своју информациону кампању према Украјини, не само унутар сопственог информационог простора већ и украјинског, као и на међународном нивоу. Такође је јасно да се и у околностима „замрзавања“ сукоба на Донбасу очекује активније ангажовање главног адута руског рата информационог карактера. Према проценама САД источна Украјина, поред осталог, представља „нову“ лабораторију за будуће ратовање у овом веку. У овом сукобу Русија је искористила своју висококофистицирану и ефикасну технологију за спровођење напада, укључујући ГПС обмане у циљу заваравања система навигације и навођења (Giles, 2016: 64). За Русију информационо ратовање није активност ограничена искључиво на ратни период или на почетну фазу сукоба пре отпочињања непријатељства.

Украјински сукоб обилује многим активностима које су се одвијале и у сајбер простору. Примери су бројни: напад на телекомуникационе мреже 2013. године кроз експлоатацију телекомуникационе инфраструктуре од стране владе Виктора Јануковича за директно слање порука демонстрантима преко мобилних телефона (Maurer, Janz, 2014), напади на мобилне телефоне украјинских чланова Парламента, ДДОС напади, напади пророских и проукрајинских хакера на противничке веб-странице, хаковање рачунара и сервера украјинског премијера и разних украјинских амбасада широм света помоћу малициозног кода „Снејк“ (*Snake*). Током праћења украјинских председничких избора у марту 2014. године, украјинске службе безбедности открили су присуство малициозног кода у системима Централне изборне комисије. Код је, наводно, имао за циљ да саботира обраду гласова, а одговорност за напад преузела је пророска хакерска група „Сајбер беркут“ (*CyberBerkut*).

С обзиром на акције непријатељске стране, друге земље су предузеле мере подршке Украјини. Између осталог, уследила је и подршка НАТО у износу од 20 милиона долара финансијске помоћи у невојним одбрамбеним ресурсима, а нарочито у сфери сајбер одбране (Maurer, Janz, 2014). Иначе, хакерска група „Сајбер беркут“ сноси одговорност и за напад на три НАТО веб-локације (nato.int, ccdco e.org и nato-pa.int), а према доступним извештајима наведени инциденти били су без трајних последица (Declaration by the NATO spokesperson, Oana Lungescu, 2014). Група је на

својој веб-страници изјавила да не прихвата присуство окупаторских снага НАТО на украјинском тлу. Од почетка немира циљ групе била је борба против неофашиста и пропаганда против медија за које су сматрали да су корумпирани. Верује се да је наведена група одговорна за преко сто хакерских напада на украјинске веб-странице, као и за ометање украјинских телекомуникационих система, при чему је на мети напада био и „Уркtелеком“ (*Ukrtelecom*), главни телеком оператер у Украјини (Finley, 2014).

Поред тога, не смемо заобићи чињеницу да су друштвене мреже (превасходно Твитер и Фејсбук) биле важно средство у служби демонстраната, али и надлежних државних органе за надгледање комуникационог простора, анализу прикупљених информација и инфилтрирање на друштвеним мрежама. При томе, треба напоменути да је већина размењеног садржаја Украјинаца преко Твитера била на енглеском језику како би се привукла пажња широке међународне заједнице (Barbera, 2014).

Закључак

Циљ савремених ратова јесте потпуна стратешка парализа противника и ланчани „домино ефекат“ урушавања његових капацитета за успешан отпор, усмеравањем на виталне тачке не само система одбране већ друштвеног система као целине. Ратна ситуација посматра се као скуп међусобно повезаних друштвених подсистема које је потребно онеспособити, било директно оружаним путем, било путем економских мера, дипломатским деловањем или, пак, циљањем на информационе токове. Да би се циљ остварио, примењују се различите стратегије, технике и методи.

Информационо ратовање у стратегијско-доктринарним документима Руске Федерације, као и других технолошки развијених држава, има посебан значај, те је постало предмет изучавања на различитим цивилним и војним високошколским установама и институтима. Оно данас равноправно учествује у остварењу стратешких циљева током конфликта, упоредо са оружјем за масовно уништење, класичним војним снагама, економијом, политичко-дипломатским и обавештајним капацитетима. Појављује се као претходница војних операција, затим као њихов саставни део, а потом и у експлоатацији њихових резултата.

Украјина је једно од актуелних попришта побуна, политичких криза и сукоба, на којем се манифестује веза између политичких промена и капацитета за овладавање информационим технологијама и информационим простором различитих државних и недржавних актера.

Док се кампања у Грузији 2008. године углавном фокусирала на демонстрацију руске војне моћи, главно обележје кампање у Украјини јесу управо информационе операције, у којима војне активности често само подржавају главне битке вођене путем медијских канала.

Постоји много аргумената који иду у прилог претпоставци да Русија у украјинској кризи тестира своју нову војну стратегију, у којој се за постизање војних циљева често користе различите невојне акције у склопу такозваног хибридног ратовања. Због тога не изненађује чињеница да је руски концепт информационог ратовања, заједно са другим руским инструментима моћи, постао предмет изненадног и интензивног интересовања на Западу још почетком украјинске кризе 2014. године.

Литература

1. Američki Stejt Department (2014). Nastavak ruske fikcije – još deset lažnih tvrdnji o Ukrajini. *Novi vek*, broj 7, https: //www.ceas-serbia.org/images/2015-i-pre/Novi_vek_br07.NASTAVAK_RUSKE_FIKCIJE.pdf, доступан 8. 1. 2021.
2. Analytical report of the Razumkov Centre (2015). Prospects of Russia-Ukraine Relations. *National Security and Defence*, No. 8/9, https: //razumkov.org.ua/uploads/journal/eng/NSD157-158_2015_eng.pdf, доступан 8. 1. 2021.
3. Атаманов, Г. А. (2010). *Информационная война: экспликация понятия*, http: //www.naukaxxi.ru/materials/254/, доступан 7. 1. 2021.
4. Balybin, C., Donskov, Yu., Boyko A. (2014). Electronic Warfare Terminology in the Context of Information Operations. *Military Thought*, 23(3).
5. Barbera, P. (2014). Tweeting the Revolution: Social Media Use and the #Euromaidan Protests, *Huffington Post*, 31 3. 2014, http:

//www.huffingtonpost.com/pablo-barbera/tweeting-the-revolution-s_b_4831104.html, доступан 7. 1. 2021.
6. Berzins, J. (2014). Russia's New Generation Warfare in Ukraine: Implications for Latvian Defence Policy. *National Defence Academy of Latvia. Center for Security and Strategic Studies*, http: //www.naa.mil.lv/~/media/NAA/AZPC/Publikacijas/PP%2002-2014.ashx, доступан 7. 1. 2021.
7. Бжежински, З. (1997). *Велика шаховска табла*. Подгорица: ЦИД.
8. Darczewska, J. (2014). *The anatomy of Russian information warfare*, *the Crimean operation, a case study*. Centre for Eastern Studies, Warsaw
9. Decree of the President of Ukraine No. 47, "On the Decision of the Ukrainian National Security and Defence Council", 25 2. 2017, http: //www.president.gov.ua/documents/472017–21374, доступан 21. 12. 2019.
10. Declaration by the NATO spokesperson, Oana Lungescu, on Twitter on 15 March 2014. http: //rt.com/news/nato-websites-ddos-ukraine-146, доступан 7. 1. 2021.
11. Doctrine of Information Security of the Russian Federation. (2016), https: //www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163, доступан 8. 1. 2021.
12. *Foreign Policy Concept of the Russian Federation*. (2016). https: //www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2542248, доступан 8. 1. 2021.
13. Giles, K. (2016). *Handbook of Russian Information Warfare*. Rome: NATO Defense College.
14. Кривокапић, Б. (2010). *Енциклопедијски речник међународног права и међународних односа*. Београд: ЈП Службени гласник.
15. Lätsch, D., Moccand, D. (2010). Moderne Verteidigung. *Military Power Revue*, 2/2010, 3-10.
16. Mathew, J. (2014). Equipment Installed in Crimea to Tap Lawmakers' Phones: Ukraine Security Services Chief. *International Business Times*, 4. 3. 2014, http: //www.ibtimes.co.uk/equipment-installed-crimea-tap-lawmakers-

phones-ukrainesecurity-services-chief-1438821, доступан 8. 1. 2021.
17. Maurer, T., Janz, S. (2014). The Russia–Ukraine conflict: cyber and information warfare in a regional context, ETH ISN Zurich, https: //www.files.ethz.ch/isn/187945/ISN_184345_en.pdf, доступан 8. 1. 2021.
18. Military Doctrine of the Russian Federation. (2014). https: //rusemb.org.uk/press/2029, доступан 8. 1. 2021.
19. Molander, R., Riddile, A., Wilson, P. (1996). *Strategic Information warfare, A New Face of War*. National Defense Research Institute, Santa Monica.
20. Oleksandr Turchynov called for establishing an information army that will give a proper response to Russia's propaganda. (2016). http: //www.rnbo.gov.ua/news/2622.html, доступан 8. 1. 2021.
21. Панарин, И. (2012). *О Доктрине информационного противоборства России*, http: //topwar.ru/16540-o-doktrine-informacionnogo-protivoborstva-rossii.html, доступан 08.01.2021.
22. Панарин, И. (2018). *Информационная война и коммуникации*. Горячая линия–Телеком, Москва.
23. Pashkov, M. (2017). Russia's information expansion: Ukrainian foothold, Tomáš Čižik (ed.): *Information Warfare – New Security Challenge for Europe*. Centre for European and North Atlantic Affairs, Bratislava:
24. Петровић, Д. (2008). *Геополитика постсовјетског простора*. Прометеј, Нови Сад
25. Путник, Н. (2012). *Кибер ратовање – нови облик савремених друштвених конфликата*, докторска дисертација. Београд: Универзитет у Београду – Факултет безбедности.
26. RAND (2021). https: //www.rand.org/topics/information-operations.html, доступан 9. 1. 2021.
27. Sazonov, V., Müür, K., Mölder, H. (2016). *Russian Information campaign against the Ukrainian state and Defence Force*. NATO Strategic Communications Centre of Excellence,Tartu
28. *Стратегия национальной безопасности Российской Федерации до 2020 года*. (2009). http: //www.kremlin.ru/supplement/424, доступан 8. 1. 2021.

29. Тофлер, А., Тофлер, Х. (1998). *Рат и антират*. Paideia, Београд:
30. Finley J. C. (2014). *Telecom services sabotaged in Ukraine's Crimea region*, 28 February 2014, https: //www.upi.com/Top_News/World-News/2014/02/28/Telecom-services-sabotaged-in-Ukraines-Crimea-region/7611393621345/, доступан 9. 1. 2021.
31. Жутдиев, Б. Б., Кулешов, Ю. Е., Ничипорович, О. С., Федоров, Д. А. (2014). Теоретические аспекты информационно-психологического противоборства в современных условиях. *Нацыянальнай акадэміі навук Беларусі*, 3, 10-18.

Russian Information Operations in the Ukrainian Armed Conflict

Abstract: *The ultimate goals and basic forms of social conflict have remained unchanged throughout history. Nevertheless, today there is an evident expansion in the application of new methods, techniques and means for waging war. The continuous fusion of revolutionary achievements in the field of computers, satellite communications and the media has radically improved the possibilities of warfare, despite the fact that technological achievements have not substantially changed the geostrategic and political-economic goals of the war itself. Cyberspace provided enormous opportunities for conducting special propaganda actions as well as for carrying out attacks via computer networks on enemy information systems and thus expanded the space for conducting information operations. Information operations can be conducted independently or in support of conventional, kinetic, conflict.*

The authors of the paper point out the importance that information operations have in modern armed conflicts on the example of the conflict in Ukraine. In the introduction, an overview of different conceptual definitions of information operations is given. Then, an analysis of the Russian theoretical and strategic-doctrinal approach to information warfare was conducted. After that, the specifics of information operations from the point of view of their content, scope,

place and role in modern armed conflicts, on the Ukrainian example, are explained.

The paper should be viewed as a starting point for a broader discourse, because it is not possible to discuss this issue comprehensively in all its complexity within the given format. The dramatic events in Ukraine have unequivocally indicated to us that the information aspect of the hybrid war should not be underestimated or neglected.

Keywords: *information operations, social conflicts, Ukrainian conflict, media, propaganda.*