ОБЕЛЕЖЈА САЈБЕР ДИМЕНЗИЈЕ СУКОБА У УКРАЈИНИ ОД 2022. ДО 2024. ГОДИНЕ

Александар М. Богићевић[1]

Достављен: 14.03.2025. *Језик рада*: Српски
Кориговано: 23.04. и 17.07.2025. *Тип рада*: Прегледни рад
Прихваћен: 13.08.2025. *DOI број*: 10.5937/vojdelo2502049B

Апстракт: Руска инвазија на Украјину фебруара 2022. означила је почетак највећег оружаног сукоба у Европи након Другог светског рата, доносећи значајне промене на бојном пољу. За разлику од претходних конфликата који су садржали елемент сајбер ратовања, где би најчешће једна страна имала потпуну превласт, рат у Украјини укључује две државе са доказаним способностима на овом пољу. Сајбер сукоб је, међутим, започео још 2014. године током кризе у Донбасу, након чега је Русија покренула серију деструктивних операција које су указале на рањивост украјинске дигиталне инфраструктуре. Ови напади послужили су као основа за реформу и јачање украјинске сајбер одбране, што је уз подршку западних савезника створило предуслове за одбијање иницијалног таласа руских сајбер напада 2022. године. Након почетне сајбер офанзиве, која је пратила ону копнену и која је дала резултате слабије од очекиваних, сукоб је ушао у фазу у којој обе стране размењују нападе чија је софистицираност знатно испод нивоа какав је био присутан на самом почетку. У раду се анализира развој и динамика сајбер операција у контексту ширег конвенционалног сукоба, укључујући кључне актере, циљеве, коришћене технике и резултате постигнуте у сајбер простору. Посебна пажња посвећена је питању зашто руске сајбер операције нису постигле стратешки значајнији ефекат, упркос ресурсима које Москва поседује. Аутор закључује да се разлози за ограничене резултате могу пронаћи у благовременој и структурној припремљености украјинске стране, ефективној међународној сарадњи, као и у самом карактеру сајбер ратовања који, у условима добро организоване одбране, фаворизује дефанзиву над офанзивом. Рат у Украјини тако показује да сајбер домен, иако не пресудан, има важну улогу у комплементарном деловању са физичким фронтом, посебно у сферама комуникације, обавештајног рада и психолошког утицаја.

1 Универзитет одбране у Београду, Институт за стратегијска истраживања, Београд, Република Србија, e-mail: aleksandar.bogicevic@mod.gov.rs, https://orcid.org/0009-0006-7450-5193.

Кључне речи: *сајбер ратовање, рат у Украјини, информационо ратовање, недржавни сајбер актери, критична инфраструктура*

Увод

Упад руских оружаних снага на територију Украјине фебруара 2022. године означио је почетак највећег оружаног сукоба на простору Европе након Другог светског рата. Поред значајних промена у начину вођења конвенционалног рата, пре свега услед интензивне употребе беспилотних летелица, сукоб на истоку Европе представља прекретницу у развоју сајбер ратовања будући да је реч о првом оружаном сукобу у којем обе стране располажу развијеним капацитетима за извођење сајбер операција, без изражене асиметрије. За разлику од сукоба на копну, ваздуху и мору, конфликт у сајбер сфери присутан је без престанка од 2014. године и почетка борби у Донбасу. Иако је Москва успевала да постигне запажене успехе у украјинском сајбер простору, као што су напад на енергетски сектор 2015. године (Zetter, 2016) или *NotPetya* напад (Bajak & Satter, 2017), Украјина током две године конвенционалног сукоба није доживела сајбер напад који би је онеспособио, посебно током почетне фазе рата када се очекивало да елемент изненађења и сама концентрација напада могу изазвати „сајбер Перл Харбор" (U.S. Department of Defense, 2012).

Након почетне фазе рата коју је у сајбер простору одликовао изузетан број руских напада велике разноврсности и софистицираности (State Service of Special Communications and Information Protection of Ukraine – SSSCIP, 2023), сукоб је ушао у фазу исцрпљивања и прилагођавања околностима продуженог конфликта. Трансформација сукоба из маневарског у позициони, која је уследила након повлачења руских снага из околине Кијева, одвијала се паралелно са значајним променама и у сајбер сфери, у којој је било неопходно реорганизовати доступне ресурсе, креирати стратегију прилагођену новим околностима и идентификовати нове циљеве. Сајбер рат се тиме трансформисао из фазе константних и комплексних напада који су долазили из Русије у фазу међусобних напада који су као примарни циљ имали прикупљање обавештајних података и утицање на јавно мњење.

Рад се заснива на квалитативној анализи доступних примарних и секундарних извора, уз примену компаративног и дескриптивно-аналитичког приступа. Узимајући у обзир динамику сајбер напада и одбране у периоду од 2014. до 2024. године, као и техничке и институционалне капацитете обе стране, анализирају се структурални и контекстуални фактори који су утицали на (не)успех руских сајбер операција у Украјини. Истраживање је усмерено на разматрање узрока ограничене ефикасности руских сајбер операција током рата у Украјини, упркос широко распрострањеном уверењу о њиховој надмоћи. Настоји се да се пружи одговор због чега Русија није остварила резултате од стратегијског значаја у сајбер сфери, те какву улогу у томе имају различите компоненте украјинске одбране. Полазна претпоставка је да се узроци оваквог исхода налазе у вишегодишњим припремама и системском јачању украјинских сајбер капацитета, као и у интензивној сарадњи са државама Запада. Додатно, заузима се становиште

да сама природа сајбер ратовања значајно отежава постизање успеха на стратегијском нивоу, посебно у околностима када не постоји драстична разлика у сајбер капацитетима.

Пре него што се пређе на даљу анализу, неопходно је већ на самом почетку указати на изражену асиметрију у доступности и поузданости информација повезаних са сајбер ратовањем у контексту рата у Украјини. Највећи део релевантних података потиче из западних извора и међународних компанија и организација специјализованих за сајбер безбедност, док су подаци који долазе из руских извора изузетно ограничени и ретко доступни. За разлику од физичког простора, у ком је могуће непосредно утврдити обим и карактер штете, у сајбер окружењу таква процена је знатно отежана због његове апстрактне природе. Ову сложеност додатно појачава чињеница да је оружани сукоб и даље у току, што чини податке о ефектима и успешности конкретних сајбер напада осетљивим и често политички инструментализованим. У том контексту потребно је имати у виду и склоност зараћених страна ка умањивању сопствених губитака и претеривању у представљању сопствених капацитета и успеха.

Савремени концепт сајбер ратовања: карактеристике, домети и изазови

Нагли технолошки развој условљен масовном употребом рачунара и интернета условио је развој „новог поља социјалне анксиозности" (Ungar, 2001: 271) у виду сајбер претњи, чије порекло могу бити како различите криминалне групе и други недржавни актери, тако и државе, које, кроз малициозне сајбер операције, покушавају унапредити свој положај у односу на перципираног противника. Овакав вид коришћења сајбер простора окарактерисан је као сајбер ратовање. У најужем смислу под сајбер ратовањем подразумева се врста непријатељске активности која обухвата нападе усмерене против рачунарских мрежа, система и база података у циљу уништавања или деградирања ефикасности информационих и технолошких система противничке стране (Вулетић, 2017: 312). За разлику од претњи које долазе са копна, мора и ваздуха, које имају физичку форму, сајбер окружење одликује се апстрактношћу, што отежава перцепцију претњи које долазе из овог домена, како у погледу потенцијалних рањивости, тако и у погледу починиоца сајбер напада.

Могућност вршења малициозних операција у сајбер простору у циљу наношења штете другој страни од доносилаца одлука неретко бива перципирано као ново чудесно оружје, посебно као алтернатива скупом конвенционалном наоружању (Suciu, 2014). Међутим, поред технолошки напредних држава које могу искористити своју предност у информатичким технологијама у правцу нападања противника, Рустичи сматра да би „нови барут" (Novaković & Rizmal, 2017: 253) могли употребити и недржавни актери за спровођење веома деструктивних напада. (Rustici, 2011: 37) Иако се често истиче да слабије државе и недржавни актери могу путем сајбер напада нанети штету какву не би могли постићи конвенционалним средствима, стварност је знатно сложенија, посебно када се у обзир

узму околности и ресурси неопходни за извођење напада са већим стратешким последицама. (Pijpers, 2023: 7)

Упркос чињеници да сајбер напади имају карактеристике скривености и изненађења, што даје предност нападачу, да би напад уопште имао могућност успеха, неопходно је идентификовати слабост која би могла послужити нападачу као улазна тачка у рачунарску мрежу. (Hesseldahl, 2010) За разлику од конвенционалног сукоба, у сајбер ратовању неопходно је да нека од страна направи пропуст како би напад био успешан (Libicki, 2009: 14), што је у пракси значајно чешће последица људске грешке него софтвера. (Davies, 2023) Да би се уочиле мањкавости рачунарске мреже, организовали капацитети и извршио напад, неопходно је поседовати значајне људске и материјалне ресурсе, што овај вид ратовања чини недоступним за већину држава. (Pijpers, 2023: 7) За успешно спровођење сајбер напада неопходне су експертска знања, финансијска средства, као и време за припрему и организацију напада. Ипак, и после свих припрема, кључан фактор за успех напада јесу карактеристике рачунарске мреже која је таргетирана, односно карактеристике браниоца (Hesseldahl, 2010).

Посматрано у контексту конвенционалног рата, сајбер капацитети могу се користити у два правца: таргетирања рачунарске мреже намењене подршци вођењу конвенционалног рата, или, с друге стране, „извора националне моћи" (Wilde, 2024: 2), односно елемената критичне инфраструктуре, ризик коме се придаје растући значај међу свим великим силама (Stoddart, 2022: 55). Таргетирање оружаних снага донело би превласт на бојишту и олакшало победу у конвенционалном сукобу. Међутим, оружане снаге су изузетно отпорне на овакве нападе, пре свега због улагања у заштиту комуникација и дигиталних система (Libicki, 2009: 19). С друге стране, напади могу таргетирати невојне циљеве, пре свега критичну инфраструктуру, у циљу отежаног функционисања државног апарата и пољуљавања поверења грађана у институције. Ипак, сајбер напади на критичну инфраструктуру такође захтевају значајне ресурсе услед посебне пажње коју државе посвећују њеној заштити. У том контексту државе укључене у савремене сукобе, попут Русије и западних земаља, развиле су различите концептуалне приступе разумевању и дефинисању сајбер ратовања.

За разлику од држава Запада, у којима се сајбер ратовање посматра са његовог техничког аспекта, у облику нарушавања интегритета рачунарске мреже (Poulsen & Staun, 2021: 328), Русија сукоб у сајбер сфери види као део концепта информационог рата. Тако Министарство одбране Русије у једном акту из 2011. године дефинише информациони рат као „сукоб између две државе у информационом простору са циљем наношења штете информационим системима, процесима и ресурсима, као и критично важним и другим структурама; поткопавајући политички, економски и социјални поредак; изводећи масовне психолошке кампање уперене против становништва циљане државе са циљем да се дестабилизује друштво и влада, као и да се друга држава натера на доношење одлуке у корист њених противника" (Ministry of Defense of the Russian Federation, 2011). У Доктрини о информационој безбедности из 2016. године, на самом врху претњи по безбедност државе и друштва идентификована је управо злоупотреба информационо-комуникационих технологија од стране других држава

и недржавних актера зарад постизања геополитичких циљева (Security Council of the Russian Federation – SCRF, 2016). Као главни механизам за слабљење моћи Русије активностима у информационој сфери истичу се операције утицања на ставове јавног мњења, због чега је један од приоритетних циљева доктрине обезбеђивање „...међународној јавности поузданих информација о државној политици Руске Федерације и њеном званичном ставу о друштвено значајним догађајима у Русији и у свету" (SCRF, 2016), односно вођење сопственог информационог рата.

С друге стране, Украјина је, поучена искуством руских напада на њену критичну инфраструктуру (Zetter, 2016; Greenberg, 2018) и оружане снаге (Eshel, 2016), одлучила да посебну пажњу посвети сајбер одбрани, најпре кроз успостављање нормативних оквира, а потом и изградњом одбрамбених капацитета. Украјинске институције су, почевши од 2017. године са Доктрином информационе безбедности (President of Ukraine, 2017) и Законом о принципима имплементације сајбер безбедности (Verkhovna Rada of Ukraine, 2017), дале значајан замах развоју капацитета неопходних за одбрану у сајбер простору, о чему говори значајна сарадња са државама чланицама НАТО-а и оснивање Команде за везу и сајбер безбедност 2020. године (Ministry of Defence of Ukraine, 2022: 15; 70-76) као команде специјализоване за вођење информационог ратовања на начин на који га Русија и Украјина дефинишу.

С друге стране, НАТО и даље посматра сајбер ратовање као активност одвојену од деловања у широј информационој сфери, што је уочљиво и у Стратешком концепту усвојеном на самиту у Мадриду јуна 2022. године (NATO, 2022: 3-4). Сличан тренд приметан је и у стратешким документима Сједињених Америчких Држава који се односе на сајбер безбедност. Иако у Националној сајбер стратегији из 2018. године постоји имплицитна повезаност између сајбер безбедности и сузбијања малициозних страних утицаја у виду манипулацијама информацијама (The White House, 2018: 23), у њеној следећој итерацији из 2023. изостала је и имплицитна повезаност између сајбер ратовања и информационе сфере (The White House, 2023), чиме се додатно потврђује дистинкција између руског (и украјинског) виђења сајбер ратовања, с једне, и западног, с друге стране.

Различита виђења сајбер ратовања нису само теоријске природе, већ имају директне импликације на обликовање стратегија, одређивање циљева и прерасподелу ресурса. Док западни приступ, фокусиран на техничке аспекте заштите рачунарских мрежа и система, омогућава прецизно дефинисање претњи и развој одговарајућих одбрамбених механизама, руско-украјински свеобухватни приступ препознаје повезаност између сајбер и информационе димензије модерног ратовања. Управо ови различити приступи разумевању сајбер претњи нашли су конкретну примену у оружаном сукобу између Русије и Украјине, пружајући јединствену прилику за испитивање ефикасности концептуалних оквира у условима стварног ратовања.

Сајбер напади и информационо деловање у руско-украјинском сукобу (2015–2024)

Потписивање другог Минског споразума фебруара 2015. године довело је до окончања отворених борби на истоку Украјине, али сукоб у сајбер простору остао је активан. Имплементирајући у пракси закључке до којих је дошао Валериј Герасимов о природи нових сукоба у свом раду „Вредност науке у предвиђању" (Gerasimov, 2013: 25), Москва је континуирано примењивала невојне облике притиска према Украјини, при чему су сајбер операције представљале значајан сегмент стратегије. Извођење таквих операција подразумевало је ангажовање како државних актера (примарно обавештајних служби), тако и оних недржавних, који су функционисали у оквиру одређених модалитета сарадње са званичним институцијама: од непосредног делегирања задатака и начелног руковођења акцијама до прећутне подршке сајбер нападима. (Maurer, 2018: 42)

Период који је претходио руском нападу фебруара 2022. године обележен је изразитом ефикасношћу њених сајбер операција. Координисани напади на критичну енергетску инфраструктуру Украјине током зима 2015. и 2016. године довели су до прекида снабдевања електричном енергијом, чиме је било погођено неколико стотина хиљада грађана (BBC News. 2017). Паралелно са нападима на енергетски сектор 2016. године, украјинске финансијске институције претрпеле су паралишући напад који је онемогућио њихов рад и уништио важне базе података (Некрасов, 2016). На удару руских сајбер снага нашле су се и Оружане снаге Украјине, чије су артиљеријске јединице трпеле велике губитке у Донбасу од 2014. године услед коришћења вирусом зараженог софтвера за корекцију ватре, који је одашиљао њихов положај противничкој страни (Volz, 2016). Кулминацију овог таласа сајбер напада чинио је NotPetya напад јуна 2017, који је, иако иницијално усмерен на украјинску привреду, ескалирао у глобалну кризу, изазивајући економске губитке процењене на десет милијарди америчких долара (Steinberg, Stepan, & Neary, 2021: 6). Међутим, потоњи напади на украјинску критичну инфраструктуру и привреду нису донели значајне резултате.

У периоду пред почетак рата фебруара 2022. године стратешки фокус сајбер операција померен је према систематском прикупљању различитих стратешки релевантних информација. Ове активности обухватиле су прибављање података критичних за реализацију војних операција (геопозиционирање радарских система, локације војних инсталација, командно-контролних центара и осталих стратешки значајних објеката), као и за пацификацију окупираних територија (базе података органа унутрашњих послова и локалних самоуправних јединица) (Microsoft, 2022a: 5). Оваква усмереност на прибављање прецизних и оперативно корисних информација указује на дубоку укљученост организованих и технолошки напредних сајбер актера, међу којима се посебно издвајају државне обавештајне службе као кључни носиоци ових активности. (2022a: 4-8)

Са почетком активних војних дејстава 2022. сајбер операције добиле су потпуно нову димензију оличену интензитетом извођења операција, техничком со-

фистицираношћу и бројем актера који у њима учествују. Један час пре него што су руске снаге прешле границу на деловима територије у околини Кијева сајбер нападом онеспособљена је сателитска мрежа америчке компаније *ViaSat*, *што је за п*оследицу имало прекид комуникације између јединица на фронту и команде, дајући тиме локалну предност руским снагама. Убрзо су уследили напади и на друге елементе дигиталне мреже Украјине који су имали за циљ уништавање података или онеспособљавање опреме користећи велику разноликост малвера (SSSCIP, 2023; Microsoft, 2022b: 11; Iacob & Ionita, 2022). Међутим, према доступним подацима, иницијални руски сајбер напади нису резултовали трајним онеспособљавањем украјинских оружаних снага, а ни државног апарата, који је успео да одржи своју позицију у сајбер простору (Mueller et al., 2023).

Након иницијалног таласа сајбер активности у првим недељама оружаног сукоба (Microsoft, 2022b), забележено је смањење учесталости технички софистицираних напада, уз истовремену промену њихових примарних циљева. Већ у априлу 2022. године уочен је нагли пад броја операција усмерених на уништавање података или трајно онеспособљавање рачунарских система, док је растући број напада био усмерен на државну администрацију, привредне субјекте и различите сегменте цивилне инфраструктуре (SSSCIP, 2023: 7–10). Посебно су били изложени веб-сајтови државних институција, који су често били мета DDoS напада, чији је циљ био привремено онемогућавање њиховог рада. Поред тога, медијске куће и новинске агенције представљале су честу мету не само због свог информативног утицаја већ и због потенцијала за злоупотребу њихових сервера и уређаја за емитовање у циљу ширења малвера и дистрибуције пропагандног садржаја. (2023: 21)

Напади усмерени на енергетска постројења, који су 2015. и 2016. године постизали значајне резултате, у наредном периоду нису били подједнако успешни (Bateman, 2022: 13). У једном таквом инциденту из априла 2022. хакерска јединица 74455, која делује у оквиру Главне управе Генералштаба Оружаних снага Руске Федерације (познатијег под ранијим акронимом ГРУ) (Bowen, 2022), покушала је да искористи приступ украјинским рачунарским мрежама стекнут најкасније у фебруару 2022, односно пре почетка инвазије. Користећи модификовану верзију малвера примењеног у нападу из 2016. године, ова јединица покушала је да понови ранији успех. Међутим, брзом интервенцијом украјинских сајбер одбрамбених структура и компаније ESET напад је неутрализован у раној фази извршења (ESET Research, 2022). Убрзо сајбер домен рата почео је да поприма динамику пат позиције, карактеристичну за фронт у физичком простору, што је омогућило Русији и Украјини да се прилагоде новонасталим околностима, пре свега кроз ангажовање додатних капацитета у виду недржавних актера и ширења спектра циљева сајбер операција.

С једне стране, након *wiper* напада, који се користе за трајно брисање података или оштећење хардверских компоненти, који нису дали адекватне резултате на почетку рата, Москва је приоритизовала операције које су имале за циљ прикупљање обавештајних података. Циљеви ових операција били су институције које располажу осетљивим информацијама, као што су лични подаци припадника оружаних снага, планови националне одбране, као и подаци са плат-

форме „Делта", софтвера који украјинске снаге користе за команду и контролу, али и за прецизно навођење артиљеријске ватре на бојишту (SSSCIP, 2023:18). Такође, Русија је временом интензивирала своје деловање у информационој сфери, где се тежиште померало са Украјине према државама чланицама НАТО-а (European Union Agency for Cybersecurity (ENISA), 2024: 95). Фокусирани на друштвене мреже као главно поље деловања, руски државни и недржавни сајбер актери настоје да преплаве информациони простор порукама које би легитимисале њихове борбе у Украјини, дискредитовале владу у Кијеву, унеле раздор међу савезницима и скренуле пажњу јавности на унутрашње проблеме уместо на сукоб на истоку Европе (*CyberPeace Institute*, 2023: 15). Посебну пажњу сајбер актера привлачиле су државе блиске Украјини у којима су одржавани избори чији би исходи могли утицати на подршку Кијеву, пре свих Сједињене Државе. (Microsoft, 2023)

За сада најуспешнију операцију коју су извеле руске хакерске групе, о чијим резултатима постоје информације признате од западних извора, извела је сајбер јединица ГРУ-а маја 2023. године, која је успела да се инфилтрира у рачунарску мрежу компаније *Kyivstar*, највећег телекомуникационог оператера у Украјини, чије услуге користи приближно 24 милиона грађана (Balmforth, 2024). Напад је имао за последицу озбиљно нарушавање функционисања дигиталне инфраструктуре компаније и безбедности података корисника, укључујући личне информације, геолокацијске податке, СМС комуникацију и потенцијално садржаје апликације *Telegram*, платформе коју војници обе стране активно користе за размену визуелног и текстуалног садржаја везаног за ратне активности (Balmforth, 2024). Наведени случајеви илуструју трансформацију руских сајбер операција од неефикасних офанзивних кампања усмерених према деструкцији украјинске дигиталне инфраструктуре, ка софистицираним обавештајним и информационим активностима које истовремено таргетирају украјинске критичне системе и међународни информациони простор.

С друге стране, Украјина, поучена искуствима стеченим након 2014. године, успела је да издржи иницијалну офанзиву у сајбер простору, ангажујући сопствене капацитете како за борбу у информационој сфери, тако и за нападе на елементе руске критичне инфраструктуре. Међутим, за разлику од руских сајбер операција, подаци о украјинским нападима су изузетно оскудни, што значајно ограничава могућност верификације медијских извештаја и анализа. Украјински сајбер актери били су посебно активни у раној фази рата у области дисеминације проукрајинских наратива на друштвеним мрежама: у првих петнаест дана од почетка сукоба чак 90% од укупно 5,2 милиона твитова који су изражавали отворену подршку некој од страна у конфликту односило се на подршку Кијеву, при чему је значајан део тих порука потекао са бот-налога или налога са обележјима аутоматизованог понашања (Smart et al, 2022: 34-35).

Украјинске хакерске групе такође су спровеле одређени број офанзивних сајбер операција на руску дигиталну инфраструктуру, међу којима се истиче напад на рачунарску мрежу Федералне пореске службе Руске Федерације. Према тврдњама званичника у Кијеву, припадници хакерске јединице ГУР-а (украјинске војнообавештајне агенције) остварили су приступ одређеним базама података

ове институције (Gatlan, 2023; Litvinova, 2023), што је потврђено у интервјуу који је дао Артем Старосјек, директор компаније *Molfar*, специјализоване за отворене изворе података. Његова компанија је, користећи податке добијене упадом у базе података руске пореске службе, успела да идентификује чланове руских специјалних јединица који учествују у операцијама на украјинској територији (Molfar, 2024).

Као што се могло видети у случају Киевстара или Федералне пореске службе Русије који су били мета напада, највећу претњу по Украјину и Русију чине хакерске групе састављене од лица која раде у оквиру различитих обавештајних служби, као што је руски ГРУ или украјински ГУР. Међутим, проблем с оваквим видом организовања сајбер капацитета јесте ограниченост људских ресурса у поређењу са потребама рата, јер нагло укључивање већег броја људи у обавештајне службе представља потез који носи значајне безбедносне ризике. Решење за овај проблем Кијев и Москва потражиле се у мобилизацији различитих недржавних актера као допуне постојећим капацитетима. Ипак, недржавни актери (изузимајући компаније специјализоване за сајбер безбедност) углавном немају вештине које имају знатно обученији хакери обавештајних служби. Дистинкција у способностима између државних и недржавних актера показује се кроз поделу врста напада коју ови актери предузимају: DDOS напади и наруживање сајтова најчешће се налазе у надлежности недржавних актера, док су за упаде у базе података, употребу малвера и искоришћавање рањивости у рачунарским мрежама задужене обавештајне службе (Holt et al, 2023: 83). Међутим, све већа сарадња државних институција са недржавним актерима, као и напредак у погледу техничких знања, чини недржаве хакерске групе потентним актерима за будуће конфликте (Stoddart, 2022: 371).

Тренд ангажовања и подршке недржавним актерима у сајбер операцијама, као метода за повећање капацитета за офанзивна дејства на дигиталну инфраструктуру супротстављене стране, постао је све учесталија пракса на обе стране у сукобу. На бројним руским форумима доступне су обуке за извођење DDoS напада, као и различити малициозни програми, укључујући чак и познати израелски софтвер за надзор мобилних уређаја *Pegasus* (CyberPeace Institute, 2023: 16). С друге стране, украјинске хакерске групе, пре свега „ИТ армија Украјине", на својој званичној интернет страници објављују детаљна упутства о томе како појединци могу уступити ресурсе свог рачунара ради учешћа у проукрајинским сајбер офанзивама. Као последица регрутације сајбер актера, руско-украјински сајбер простор постао је бојиште у коме активно учествује око 120 различитих државних и недржавних група, доминантно проруских, међу којима је идентификовано 23 као директно спонзорисаних од државе, а 64 као хактивистички колективи са различитим степеном сарадње са државним институцијама (CyberPeace Institute, 2023: 15). Укључивање недржавних актера у извођење малициозних сајбер операција носи велики ризик, пре свега у значајном замагљивању идентитета и мотива нападача, чиме се отежава процес атрибуције и правне одговорности. Истовремено, оваква пракса доприноси брисању јасне линије између активних учесника у сукобу и цивила, што може имати далеко-

сежне импликације по питању међународног хуманитарног права и норми које регулишу ратовање у сајбер домену.

Отпорност и адаптација: зашто сајбер напад није паралисао Украјину

Иницијални талас руских сајбер операција није довео до колапса украјинске дигиталне инфраструктуре, а последично ни до трајног паралисања цивилних власти и оружаних снага. Њихови ефекти су, судећи према доступним подацима, били знатно испод очекивања постављених током иницијалне фазе сајбер операција (2014–2017). Значајна разлика у исходу између претходних дејстава и операција покренутих током 2022. године намеће питање зашто сајбер офанзива на почетку инвазије није донела конкретније резултате. Одговори се могу пронаћи у самој природи сајбер ратовања, али и у припремљености и приступу зараћених страна овој врсти сукоба.

Скоро читава деценија врло активног руског сајбер деловања на различите делове украјинске рачунарске инфраструктуре допринела је подизању свести о значају сајбер безбедности међу доносиоцима одлука у Кијеву и потреби за системским унапређењем заштитних механизама. Како истиче начелник одељења за сајбер безбедност Службе безбедности Украјине Иља Витјук, управо су искуства са претходним нападима указала на структурне слабости у систему, што је иницирало реформе у којима је значајну улогу имала међународна сарадња (McLaughlin, 2023). У том сегменту посебно се издваја улога Сајбер команде Сједињених Држава (*United States Cyber Command*), чији су представници у децембру 2021. боравили у Кијеву ради процене стања заштите критичне инфраструктуре, приликом чега је Украјини уступљена савремена опрема и софтвери за детекцију и превенцију сајбер претњи (McLaughlin, 2023).

Такође, подршку су пружиле и бројне приватне компаније, како кроз уступање софтвера за напредну борбу против сајбер претњи (*Microsoft*, *CrowdStrike*, *ESET*, *Google*), тако и кроз обезбеђивање телекомуникационе инфраструктуре, пре свега путем *Starlink* система компаније *SpaceX*. Ова подршка омогућила је украјинским војним и административним структурама релативно стабилну комуникацију и ефикаснији одговор на сајбер и кинетичке претње. Убрзо по избијању рата украјинске власти донеле су одлуку да преместе најважније податке на *cloud* платформе, чиме је знатно умањен ризик њиховог уништења у случају физичког или сајбер напада (Stupp, 2022). У прилог оправданости ове одлуке говори и успешан напад крстарећим ракетама на дата центар у Кијеву, у коме је уништен део сервера на коме су похрањени подаци државних институција (Burgan, 2022). Захваљујући правовременој миграцији на *cloud* сервере, овај напад није изазвао трајно уништење осетљивих државних докумената.

Рат у Украјини демонстрирао је да сајбер одбрана, иако захтевна, није немогућа. Успех сајбер напада у великој мери зависи од способности одбрамбених структура да благовремено идентификују, неутралишу и закрпе рањивости у сопственим рачунарским мрежама. Иако су руски актери на почетку конфликта

користили разноврсне нове типове малициозних програма, већина тих напада није дала очекиване резултате. У ситуацијама када су одређене акције биле успешне, пропусти у одбрани су релативно брзо уочавани и затварани, чиме је онемогућено њихово поновно коришћење. Пад интензитета руских сајбер операција усмерених на уништење украјинске дигиталне инфраструктуре указује и на ограничене кадровске ресурсе унутар обавештајних структура (у односу на обим сукоба који се одвија), као најпотентнијих актера у сајбер простору, што ће у потоњим месецима бити тек делимично надомештено укључивањем недржавних сајбер актера у сукоб.

Искуство Русије у овом сукобу, али и Украјине након неколико иницијалних месеци одбране, недвосмислено указује да државе које намеравају да се у значајнијој мери ослоне на сајбер операције као средство за уништавање противничке инфраструктуре или прикупљање осетљивих информација, морају уложити знатне ресурсе у регрутовање, едукацију и техничко опремање високо обученог стручног кадра. Ипак, чак и у условима интензивног улагања, исход оваквих операција остаје неизвестан, нарочито када је мета држава са добро развијеним капацитетима за сајбер одбрану. Ангажовање недржавних актера може допринети повећању способности за извођење офанзивних операција, проширујући спектар потенцијалних циљева. Међутим, овакве групе у највећем броју случајева не поседују вештине и ресурсе упоредиве са оним којима располажу државни сајбер актери, док покушаји њихове веће интеграције носе ризике који произилазе из дилеме између принципала (државе) и агента (спонзорисаних сајбер група) (Canfil, 2022: 2; Bateman, 2022: 45). Иако се дугорочно ангажовање недржавних сајбер актера у информационом домену може показати корисним, њихова способност да онеспособе сложене рачунарске мреже, какве су у случају критичне инфраструктуре, значајно је лимитирана.

Из доктринарне перспективе Украјина и Русија демонстрирале су конзистентност у примени принципа деловања у сајбер простору развијених током претходних петнаест година. Руски покушаји утицаја на украјинско јавно мњење, усмерени ка ерозији подршке властима у Кијеву, нису произвели очекиване резултате, а исти исход имали су покушаји дискредитације руских војних операција и Владимира Путина међу њеним грађанима, што указује на развијену отпорност обеју страна према информационим операцијама. Насупрот томе, западни савезници Украјине, који су такође били изложени руским информационим кампањама, показали су знатно нижи степен отпорности. Ова рањивост посебно се манифестовала у контексту америчких председничких избора и изјава чланова Републиканске партије, предвођене председничким кандидатом Доналдом Трампом (Stradner & Ruggiero, 2023; Turner, 2024; Raskin, 2024). Рат у Украјини демонстрирао је да ефективност информационих и сајбер операција не зависи само од техничке супериорности већ и од степена друштвене кохезије, институционалне отпорности и стратешке припремљености актера који су им изложени.

Закључак

Рат у Украјини представља први велики оружани сукоб у историји у коме су се сукобиле две државе са развијеним капацитетима за извођење сајбер операција. За разлику од претходних конфликата у којима је сајбер домен представљао помоћно поље деловања, у овом рату добио је потпуни оперативни и стратешки значај. Ипак, упркос очекивањима да ће Русија, која је до тада остварила неколико запажених успеха у украјинском сајбер простору, остварити доминацију и овог пута, испоставило се да су ефекти њених офанзивних операција били знатно испод првобитних претпоставки и очекивања.

Један од кључних разлога зашто иницијална сајбер офанзива Русије није довела до колапса украјинске дигиталне инфраструктуре јесте темељна припремљеност Кијева. Искуства стечена након 2014. године, када су Украјина и њене институције биле на мети неколико деструктивних сајбер напада, створила су висок степен свести међу доносиоцима одлука о неопходности изградње институционалних, техничких и људских капацитета за одбрану у сајбер домену. Значајну улогу у овом процесу имали су међународни партнери, пре свега Сједињене Америчке Државе, али и бројне приватне компаније које су обезбедиле софтверску, инфраструктурну и оперативну подршку. Овај заједнички напор показао је да у савременим условима успешна сајбер одбрана није немогућа уколико постоји добра организација ресурса, квалитетна припрема, финансијски ресурси и стратешка подршка споља. Пренос осетљивих података на cloud платформе, изградња одбрамбене архитектуре и стално праћење претњи омогућили су Украјини да очува функционалност својих институција и командне структуре током критичних првих недеља рата. Такође, значајно је што се показало да чак и високо софистицирани малвери могу бити неутралисани уколико системи одбране функционишу ефикасно и координисано.

С друге стране, ограничен домет руских офанзивних сајбер операција условио је прилагођавање њене стратегије. Уместо покушаја деструкције украјинских рачунарских мрежа и њених података, руски сајбер актери временом су се фокусирали на прикупљање обавештајних података и спровођење информационих операција. Напори су усмерени на добијање увида у украјинске војне и административне капацитете, али и на утицај на јавно мњење у земљама које подржавају Украјину. Манипулације наративима у информационој сфери показале су се као подручје у ком Русија и даље има одређени степен утицаја, посебно у западним друштвима са високим степеном политичке поларизације.

Један од најзначајнијих аспеката овог сукоба јесте масовно ангажовање недржавних актера, са различитим степеном кооперације са државним структурама. Ове групе активно су учествовале у ширењу пропаганде, дистрибуцији малициозних софтвера и извођењу DDoS напада на критичну инфраструктуру. Међутим, њихова оперативна ефикасност остаје спорна, док правне и етичке дилеме које произилазе из замагљене линије између цивила и борца у кибернетичком простору представљају озбиљан изазов за постојеће оквире међународног хуманитарног права, посебно у контексту примењивости принципа разликовања између бораца и осталих актера у сајбер домену.

Закључно, сајбер димензија рата у Украјини указује да у сукобу високог интензитета сајбер операције имају споредну, али не и занемарљиву улогу. Њихов значај се огледа више у континуираном притиску, обавештајним и психолошким ефектима, него у остваривању брзих и деструктивних резултата. Стога државе које се желе припремити за евентуалне конфликте у сајбер домену морају уложити значајне напоре у одбрану, едукацију, координацију са међународним партнерима и развој сопствених доктрина које одговарају специфичностима сајбер простора. Сукоб на истоку Европе представља за сада најбољу демонстрацију улоге сајбер ратовања у великом конвенционалном сукобу – сајбер операције, иако не одлучују исход рата („сајбер Перл Харбор"), представљају његов неизоставан сегмент у коме је неопходно деловати како у правцу очувања сопствене дигиталне инфраструктуре, тако и у правцу борбе у информационој сфери.

Литература:

[1] Администрация Президента Российской Федерации. (2016). *Доктрина информационной безопасности Российской Федерации* (утверждена Президентом РФ 5 декабря 2016 г. № Пр-2233).

[2] Некрасов, В. (2016, 9. децембар). Украина програє кібервійну. Хакери атакують державні фінанси. *Економічна правда*. Преузето 13. avgusta 2024. https://epravda.com.ua/publications/2016/12/9/613957/.

[3] Bajak, F., & Satter, R. (2017) Companies still hobbled from fearsome cyberattack. *The Associated Press*. www.apnews.com/ce7a8aca506742ab8e8873e7f9f229c2

[4] Balmforth, Tom. (2024). Exclusive: Russian hackers were inside Ukraine telecoms giant for months. *Reuters*. Preuzeto: 11. avgusta 2024. reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/.

[5] Bateman, Jon. (2022). *Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications.* Carnegie Endowment for international peace.

[6] BBC News. (2017). Russian hackers 'behind cyber-attack on Netflix and Airbnb'. *BBC News*. Preuzeto 22. avgusta 2024. https://www.bbc.com/news/technology-38573074.

[7] Bowen, A. S. (2022, February 2). *Russian cyber units* (Congressional Research Service In Focus No. IF11718). Congressional Research Service.

[8] Burgan, Cate. Ukraine Data Centers Became Physical Targets When Cyberattacks Failed. *Meri Talk*. Preuzeto: 13. avgusta 2024. meritalk.com/articles/ukraine-data-centers-became-physical-targets-when-cyber-attacks-failed/

[9] Canfil, J. K. (2022). The illogic of plausible deniability: Why proxy conflict in cyberspace may no longer pay. *Journal of Cybersecurity*, Vol 8 (1), 1-16.

[10] CyberPeace Institute. (2023). Cyber Dimensions of the Armed Conflict in Ukraine: Quarterly Analysis Report Q3 July to September 2023. Preuzeto: 8. avgusta

2024. cyberpeaceinstitute.org/wp-content/uploads/2023/12/Cyber-Dimensions_Ukraine-Q3-2023.pdf

[11] Davies, Josh. (2023). Why humans are the weakest link in cybersecurity. *Alert Logic*. Preuzeto 18. avgusta 2024. https://www.alertlogic.com/blog/why-humans-weakest-link-cybersecurity/

[12] ESET Research. (2022). Industroyer2: Industroyer reloaded. *WeLiveSecurity*. Preuzeto: 17. avgusta 2024. welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

[13] Eshel, Tamir. (2016). Russians Used Cyber Bots to Target Ukrainian Artillery. *Defense update*. Preuzeto: 17. avgusta 2024. defense-update.com/20161223_trojan-2.html#google_vignette

[14] European Union Agency for Cybersecurity. (2024). *ENISA threat landscape 2024 (ENISA Report)*.

[15] Gatlan, S. (2023). Ukrainian military says it hacked Russia's federal tax agency. Bleeping Computer. Preuzeto 18. avgusta 2024. https://www.bleepingcomputer.com/news/security/ukrainian-military-says-it-hacked-russias-federal-tax-agency/.

[16] Gerasimov, Valery. (2016). "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations." *Military Review*.

[17] Greenberg, A. (2018). The untold story of NotPetya, the most devastating cyberattack in history. *Wired*. Preuzeto 20. avgusta 2024. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[18] Hesseldahl, Arik. (2010). Computer Worm May Be Targeting Iranian Nuclear Sites. *Bloomberg*. Preuzeto: 16. avgusta 2024. bloomberg.com/news/articles/2010-09-24/stuxnet-computer-worm-may-be-aimed-at-iran-nuclear-sites-researcher-says

[19] Holt, T. J., Griffith, M., Turner, N., Greene-Colozzi, E., Chermak, S., & Freilich, J. D. (2023). Assessing nation-state-sponsored cyberattacks using aspects of Situational Crime Prevention. *Criminology & Public Policy*, 22, 825-848.

[20] Iacob, I., & Ionita, L. M. (2022, August 12). *The anatomy of wiper malware, part 1: Common techniques*. CrowdStrike. Preuzeto 14. avgusta 2024. https://www.crowdstrike.com/en-us/blog/the-anatomy-of-wiper-malware-part-1/

[21] IT Army of Ukraine. *Instructions for setting up DDoS attacks on the enemy country*. Preuzeto: 15. avgusta 2024. itarmy.com.ua/instruction/?lang=en.

[22] Kim Zetter. (2016). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. *Wired*. Preuzeto: 12. avgusta 2024. wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[23] Libicki, Martin C. (2009).*Cyberdeterrence and Cyberwar*. RAND Corporation.

[24] Litvinova, D. (2023). Ukraine faces heavy attack from air and cyberspace while Zelenskyy in US presses for more funding. *Associated Press.* Preuzeto 17. avgusta 2024. https://apnews.com/article/ad01b573ecc912c112ece8d63993a4ac.

[25] Maurer, T. (2018). *Cyber mercenaries: The state, hackers, and power*. Cambridge University Press.

[26] McLaughlin, Jenna. (2023). An inside look at Ukraine's cyber war with Russia. *NPR*. Preuzeto: 13. avgusta 2024. npr.org/2023/09/04/1197548380/an-inside-look-at-ukraines-cyber-war-with-russia.

[27] Microsoft. (2022a). *Special Report Ukraine: An overview of Russia's cyberattack activity in Ukraine*. Microsoft Corporation, 2022.

[28] Microsoft. (2022b). *Defending Ukraine: Early Lessons from the Cyber War*. Microsoft Corporation.

[29] Microsoft. (2023). *A year of Russian hybrid warfare in Ukraine* (Microsoft Threat Intelligence Report).

[30] Ministry of Defence of Ukraine. (2022). *White Book 2021: Defence policy of Ukraine.*

[31] Ministry of Defense of the Russian Federation. (2011). *Conceptual Views on the Activities of the Armed Forces of the Russian Federation in Information Space*.

[32] Molfar. (2024). Elite killers who spread terror to civilians in Ukraine: Senezh - the Russian special forces. The list of liquidated. *Molfar*. Preuzeto: 29. avgusta 2024. molfar.com/en/blog/senezh-specpryznachenci-rf-perelik-likvidovanyh

[33] Mueller, G. B., Jensen, B., Valeriano, B., Maness, R. C., & Macias, J. M. (2023). *Cyber operations during the RussoUkrainian War: From strange patterns to alternative futures*. Center for Strategic and International Studies.

[34] North Atlantic Treaty Organization**. (2022).** *Strategic concept for the defence and security of the members of the North Atlantic Treaty Organization*.

[35] Novaković, Igor & Rizmal, Irina. (2017). Cyber warfare: new type or warfare or additional element of conventional warfare. *ISIKS 2017: Asymmetry and Strategy*. Beograd.

[36] Pijpers, Peter B.M.J. (2023). Revisiting the Stability/Instability Paradox in Cyberspace: Lessons from the Russo-Ukraine War. *Amsterdam Law School Research Paper No. 2023-28*. Amsterdam Center for International Law.

[37] Poulsen, Niels Bo. & Staun, Jørgen (eds.). (2021). *Russia's Military Might: A Portrait of Its Armed Forces*. Copenhagen.

[38] President of Ukraine. (2017). *Decree No. 472/2017 On the Decision of the President of Ukraine "On the Cybersecurity Strategy of Ukraine"*. Official website of the President of Ukraine.

[39] Raskin, J. (2024). *Democratic memo for April 17 full committee hearing on CCP weaponization*. House Committee on Oversight and Government Reform.

[40] Rustici, Ross. (2011). Cyberweapons: Leveling the International Playing Field. *The US Army War College Quarterly Parameters*, Carlisle, Vol 41 (3), 32-42.

[41] Smart, B., Watt, J., Benedetti, S., Mitchell, L., & Roughan, M. (2022, October). "# IStandWithPutin versus# IStandWithUkraine: the interaction of bots and humans in discussion of the Russia/Ukraine war." In *International Conference on Social Informatics*, 34-53. Cham: Springer International Publishing.

[42] State Service of Special Communications and Information Protection of Ukraine. (2023). *Russia's Cyber Tactics: Lessons Learned in 2022*. Cabinet of Ministers of Ukraine.

[43] Steinberg, S., Stepan, A., & Neary, K. (2021). *NotPetya: A Columbia University Case Study* (SIPA21022.1). Picker Center Digital Education Group, School of International and Public Affairs, Columbia University.

[44] Stoddart, K. (2022). *Cyberwarfare: Threats to critical infrastructure*. Edinburgh University Press.

[45] Stradner, I., & Ruggiero, A. (2023). America is still losing the information war against Russia. *Foreign Policy*. Preuzeto 20. avgusta 2024. https://foreignpolicy.com/2023/03/10/us-russia-information-war-bioweapon-biolab-conspiracy-theory-tucker/.

[46] Stupp, Catherine. (2022). Ukraine Has Begun Moving Sensitive Data Outside Its Borders. *Wall Street Journal*. Preuzeto: 12. avgusta 2024. wsj.com/articles/ukraine-has-begun-moving-sensitive-data-outside-its-borders-11655199002.

[47] Suciu, Peter. (2014). Why cyber warfare is so attractive to small nations. *Fortune*. Preuzeto: 13. avgusta 2024. fortune.com/2014/12/21/why-cyber-warfare-is-so-attractive-to-small-nations/

[48] **T**he White House. (2018). *National cyber strategy of the United States of America*.

[49] The White House. (2023). *National cyber strategy of the United States of America*.

[50] Turner, M. (2024). House intelligence chair says Republicans are 'absolutely' repeating Russian propaganda. *The Guardian*. Preuzeto 21. avgusta 2024. https://www.theguardian.com/us-news/2024/apr/08/republican-mike-turner-russia-propaganda.

[51] U.S. Department of Defense. (2012). *Remarks by Secretary Panetta on cybersecurity to the Business Executives for National Security*.

[52] Ungar, S. (2001). "Moral panic versus the risk society: The implications of the changing sites of social anxiety". *The British Journal of Sociology*, Vol 52 (2), 271-291.

[53] Verkhovna Rada of Ukraine. (2017). *Law of Ukraine No. 2163-VIII on the principles of cybersecurity in Ukraine*.

[54] Volz, D. (2016). *Russian hackers tracked Ukrainian artillery units using Android implant: report*. Reuters. Preuzeto 18. avgusta 2024. https://www.reuters.com/article/technology/russian-hackers-tracked-ukrainian-artillery-units-using-android-implant-report-idUSKBN14B0CU/

[55] Vuletić, Dejan V. (2017). Upotreba sajber prostora u kontekstu hibridnog ratovanja. *Vojno delo*, Ministarstvo odbrane Republike Srbije, Univerzitet odbrane u Beogradu – Institut za strategijska istraživanja. Beograd. Vol 69 (7), 308–325.

[56] Wilde, Gavin. (2024). *Russia's Countervalue Cyber Approach: Utility or Futility?*. Carnegie Endowment for international peace.

Р е з и м е

Улазак оружаних снага Руске Федерације на територију Украјине у фебруару 2022. године означио је почетак највећег оружаног сукоба у Европи након Другог светског рата. Поред дубоких последица у геополитичком и безбедносном смислу, овај конфликт представља прекретницу у развоју и разумевању сајбер ратовања јер је први оружани сукоб у коме обе стране располажу значајним капацитетима за извођење сајбер операција, што је резултирало интензивном и обостраном употребом сајбер средстава у циљу подривања способности противника. Оваква симетрија у сајбер капацитетима омогућила је настанак преседана у анализи савремених конфликата, јер први пут постоји могућност систематског праћења, упоређивања и евалуације офанзивних и дефанзивних сајбер стратегија у реалним ратним условима.

За разлику од конвенционалних борби, које су обустављене склапањем Споразума у Минску 2015, сајбер сукоб између Русије и Украјине непрестано траје од 2014. године, односно почетка борби у региону Донбаса. У том периоду Русија је извела више успешних сајбер операција, међу којима се истичу напади на украјински енергетски сектор 2015. и 2016. године, као и NotPetya напад 2017, који је имао глобални домашај, изазивајући економску штету изражену у више милијарди долара. Ови напади у значајној мери утицали су на безбедносне процене у Кијеву и подстакли развој националних капацитета за сајбер одбрану како би се спречили даљи деструктивни напади на њену дигиталну инфраструктуру.

Иницијални руски сајбер напад фебруара 2022. године није дао резултате какви су очекивани на основу ранијих искустава. Изузев онеспособљавања сателитске мреже компаније *ViaSat*, иницијална сајбер офанзива Русије није дала друге опипљиве резултате. Захваљујући сарадњи са Сједињеним Државама, као и западним компанијама специјализованим за рану детекцију и одбрану од сајбер претњи (*Microsoft*, *Google*, *Amazon*, *ESET* и друге), Украјина је успела да у првим недељама рата одржи стабилност своје дигиталне инфраструктуре и командно-комуникационих канала, након чега је број руских деструктивних напада почео опадати. Искуство Украјине показало је да чак и најсофистицираније малвери могу бити неутралисани уколико систем одбране функционише ефикасно, координисано и уз подршку међународних партнера.

Ограничени домет почетних руских операција условио је прилагођавање њене стратегије. Фокус је померен на обавештајне активности и манипулацију информацијама, пре свега у информационом простору њених западних савезника. Информационе операције, нарочито у поларизованим западним друштвима, показале су се као средство дугорочног утицаја и стратегијског притиска, у чему запажену улогу имају недржавни актери, чије масовно учешће на обе стране представља специфичност овог сукоба. Иако њихово деловање често није институционално координисано са званичним државним структурама, и једна и друга страна пружају барем прећутну подршку њиховим активностима, чиме се додатно усложњава природа конфликта. Групе попут „IT Army of Ukraine", као и различите проруске хакерске формације, илуструју замагљеност граница

између државних и недржавних актера, али и цивила и борца у сајбер простору. Овакав тренд отвара низ етичких и правних питања, нарочито у контексту примене међународног хуманитарног права, одређивања статуса актера у сајбер простору, као и прецизирања одговорности за сајбер нападе и проузроковану штету.

Закључно, сајбер димензија руско-украјинског конфликта демонстрира да у сукобима високог интензитета сајбер операције заузимају секундарну, али стратешки релевантну позицију. Њихов примарни значај манифестује се кроз способност континуираног вршења притиска, генерисање обавештајних предности и психолошких ефеката, уместо кроз остваривање тренутних и деструктивних резултата карактеристичних за кинетичке операције. Последично, државе које теже адекватној припремљености за потенцијалне конфликте у сајбер домену морају усмерити значајне ресурсе ка развоју људских и техничких капацитета, промовисању међународне сарадње, као и успостављању нормативних оквира прилагођених специфичностима сајбер простора и могућим претњама. Сукоб на истоку Европе представља најбољу демонстрацију улоге сајбер ратовања у великим конвенционалним конфликтима до сада, илуструјући да сајбер операције, иако не поседују капацитет аутономног одлучивања исхода рата (одсуство „сајбер Перл Харбора"), конституишу неизоставну компоненту савремене ратне доктрине која налаже деловање у два правца – заштите националне дигиталне инфраструктуре, те у правцу активног ангажовања у информационој сфери конфликта.

Кључне речи: *сајбер ратовање, рат у Украјини, информационо ратовање, недржавни сајбер актери, критична инфраструктура*