https://doi.org/10.18485/iipe_gsfuturebalk.2025.ch11

САЈБЕР НАПАДИ КАО СТРАТЕГИЈСКИ ИНСТРУМЕНТ СПОЉНЕ ПОЛИТИКЕ: ЗАПАДНИ БАЛКАН У ЕРИ ХИБРИДНОГ РАТА

Александар БОГИЋЕВИЋ*
Универзитет одбране – Институт за стратегијска истраживања

Сажетак: Раст тензија између доминантне силе тренутног међународног поретка (Сједињених Америчких Држава) и држава изазивача, пре свега Кине, Русије и Ирана, негативно се одразио на стабилност поретка, а последично и глобалну безбедност. У креирању таквог небезбедног окружења све важнију улогу играју претње из сајбер сфере које државе све учесталије користе с циљем наношења штете другим актерима и утицања на њихове политичке одлуке. Чест недостатак конкретних доказа о починиоцима напада и могућност одбијања одговорности за њихово спровођење чине сајбер простор идеалним за актере који стављају фокус на вођење борбе у „сивој зони". Додатни изазов државама на простору Европе поставио је рат у Украјини, покренувши нову фазу борби у сајбер простору, карактеристичну по броју напада и њиховој софистицираности. У жељи да се капацитети за вођење сајбер операција повећају, а такође и задржи способност одбацивања одговорности, све запаженију улогу у сајбер простору преузимају хакерске групе које ступају у мањи или већи степен сарадње са државним органима заузимајући улогу сајбер проксија. У све

* E-адреса: aleksandar.bogicevic@mod.gov.rs ORCID: https://orcid.org/0009-0006-7450-5193.

Рад је настао као део пројекта Министарства одбране: „Безбедносни изазови земаља Западног Балкана у европској безбедносној парадигми", бр. ИСИ/ДХ1/24–25, а који истраживачки тим и истраживачка група за проучавање регионалне безбедности Института за стратегијска истраживања и спољних сарадника реализује у периоду 2024–2025.

нестабилнијем међународном контексту смештене су у државе Западног Балкана које, услед својих спољнополитичких оријентација и ставова, бивају изложене нападима различитих сајбер актера на које не могу одговорити. Циљ овог рада јесте идентификација и анализа стратегијске употребе сајбер напада у спољној политици, с посебним освртом на импликације на Западни Балкан. Посебна пажња биће посвећена анализи конкретних случајева који илуструју кључне ризике са којима се балканске државе суочавају у сајбер простору. У зависности од својих спољнополитичких позиција, укључујући подршку Украјини, одржавање неутралности или пружање уточишта опозиционим групама у Ирану, ове државе постају мета сајбер напада различитих актера. Напади усмерени на државне институције и критичну инфраструктуру не само да угрожавају њихово функционисање већ представљају и значајан безбедносни ризик, нарочито у погледу заштите личних података грађана, који могу бити злоупотребљени као средство за даље нападе.

Кључне речи: сајбер ратовање, хибридни рат, спољна политика, сајбер безбедност, Западни Балкан

Увод

Нагли развој дигиталних технологија који је обележио почетак новог века, као и њихова раширена примена у друштву, утицала је на појаву сајбер простора као новог поља надметања држава. Идеја да се супарнику може нанети штета у физичком простору без директног напада и наглог подизања тензија учинила је дигиталан простор врло привлачним, како државама тако и недржавним актерима. Иако дебата међу ауторима и доносиоцима одлука о деструктивности овог „новог барута" (Novaković, Rizmal, 2019: 253) није довела до начелне оцене његове ефикасности, државе нису одустале од развоја сопствених сајбер капацитета, интегришући их у своје обавештајне агенције и оружане снаге.

Паралелно са овим процесом, развијала се и заједница хакера усмерених на криминалне активности, организованих у групе различитих величина и степена способности. Неомеђеност и анонимност дигиталног простора омогућила је специфичну интеракцију између држава и сајбер криминалаца креирајући уникатан вид сарадње који је резултовао настанком сајбер проксија. Ови „државни криминалци" (Martin & Whelan,

2023) временом су постали веома важан сегмент деловања држава у сајбер простору, омогућавајући им ометање функционисања других држава пружајући заузврат заштиту од кривичног гоњења. De facto инкорпорирање недржавних актера у међудржавна сајбер надметања доводи до замагљивања дистинкције између криминалних активности које спроводе хакерске групе с циљем стицања личне користи и напада сајбер јединица појединих држава којима се покушава стећи предност над супарником.

Изазивачи међународног поретка обележеног америчком доминацијом, пре свега Русија и НР Кина али и Иран и Северна Кореја, предњаче у масовној употреби сајбер ресурса с циљем вођења асиметричне борбе против САД и њених савезника, изводећи акције с циљем шпијунаже, саботаже и манипулисања наративима у јавности (ENISA, 2024: 8). Међутим, почетак рата у Украјини означио је нову фазу у сајбер надметању која, према броју учесника, напада и њиховој разорности, превазилази све до сада виђено. У размени напада између САД и њених савезника, с једне стране, и Русије и њој блиских држава, с друге стране, нашле су се и балканске државе, трпећи сајбер нападе који угрожавају функционисање њихових институција и безбедност грађана. Тензије између великих сила, постојање активног сукоба у Европи и покушаји пројекције моћи кроз шаренолик спектар прикривених и присилних мера (D'Cunha, Ferraro & Rodenhäuser, 2025) негативно су утицали на безбедност држава на Западном Балкану, што је посебно видљиво управо у сајбер сфери где норме и међународна сарадња још нису заживели.

Циљ рада је идентификација и анализа досадашње употребе сајбер напада као инструмента спољне политике, са освртом на државе на Балкану у периоду од почетка сукоба у Украјини, које су у контексту надметања великих сила актери са ограниченим значајем. Посебна пажња биће пружена конкретним примерима који представљају квинтисекцију ризика са којима се суочавају ове државе у сајбер простору. Рад указује на постојање значајног ризика по сајбер безбедност западнобалканских држава, односно њихових институција и критичне инфраструктуре услед сајбер напада изазваних као последица одређених спољнополитичких одлука. Овакви напади не само да могу отежати

нормалан рад државних органа већ могу значајно угрозити и безбедност података грађана, што може даље бити искоришћено као увод у нове нападе и даље продубљивање проблема.

Сајбер ратовање у геополитичким сукобима

Интеграција рачунарске технологије у функционисање система једне организације резултовала је настанком нових ризика у виду сајбер напада. Под оваквом врстом активности подразумевају се сви подухвати у дигиталном простору који за циљ имају ометање, уништење или манипулацију подацима или комуникационим каналима (Wilde, 2024). Међутим, сајбер ратовање, као појам ширег обухвата од сајбер напада, различито се дефинише у доктринама великих сила, пре свега у односу на питање – да ли сајбер ратовање овухвата и манипулисање наративима? Русија и Кина не раздвајају сајбер ратовање од операција манипулација информацијама у непријатељском јавном простору (енг. Foreign Information Manipulation and Interference), посматрајући их заједно као део једног ширег концепта информационог рата (Grzegorzewski, Marsh, 2024: 17; Harknetta, Smeetsb, 2022: 549; Wilde, 2025: 4), док Сједињене Државе сајбер ратовање третирају техницистички, ограничавајући се на наношење штете рачунарској мрежи (Wilde, 2022). Дистинкција у дефинисању шта јесте „сајбер" игра важну улогу у томе како се спроводе малициозни напади, као и то шта је њихова мета. Док је циљ сајбер ратовања, у ужем смислу, наношење штете рачунарским мрежама и подацима, информациони рат обухвата и психолошку димензију утицања на популацију кроз контаминацију информационе сфере лажним и конспиративним наративима који поткопавају поверење грађана у органе власти и етаблиране медије.

Сајбер напади представљају идеалан инструмент за вођење асиметричне борбе и достизања стратешке предности која би у својој коначници требала резултовати другачијом прерасподелом моћи у међународном поретку. Потенцијална способност оваквих напада да проузрокују промене на стратешком нивоу, без потребе за коришћењем силе и започињања оружаних сукоба, чине их врло подесним средством спољне политике, посебно оних актера који теже урушавању тренутног

међународног поретка. Ричард Харкнета (енг. Richard J. Harknetta) и Макс Смитс (енг. Max Smeets) исправно уочавају да стратешке последице сајбер напада нису изазивање тренутне парализе државног апарата, већ утицање на изворе моћи супарника без потребе за нападом у физичком простору (2022: 535).

Иако су поједини напади имали за последицу незанемарљиву материјалну штету (као што су израелско-амерички StuxNet напад на иранско нуклеарно постројење Натанз 2010. године и руски NotPetya напад на Украјину 2017. године) и парализу државних органа, знатно чешћа употреба сајбер средстава јесте у активностима које привлаче мање пажње као што су шпијунирање или крађа података. Такве активности не треба посматрати изоловано, као појединачна догађања, већ као део сајбер операција и сајбер стратегија које државе спроводе једне против других (Oppenheimer, 2024: 38) Међутим, у литератури су присутна два виђења сајбер операција и стратегија која зависе од аспекта сајбер бобре који се посматра. Тако Дејан Вулетић и Ерик Чабров (енг. Eric Chabrow) сајбер операције и стратегије посматрају у контексту оружаног сукоба: стратегије подразумевају сајбер нападе као додатни вид ратовања у већ постојећем сукобу у физичком простору, док сајбер операције обухатају све сајбер нападе према другом актеру, без обзира на постојање оружане борбе (Vuletić, 2017: 343–344; Chabrow, 2009). С друге стране, Метју Монте (енг. Matthew Monte), као и Харкнет и Смитс, сајбер операције и сајбер стратегије посматрају у конткесту различитих нивоа анализе: сајбер операција је усмерена на испуњавање непосредних оперативних циљева, док се сајбер стратегије, које садрже више операција, спроводе с циљем достизања стратешке предности (Harknetta, Smeetsb, 2022: 541; Matthew Monte, 2015).

Упркос најавама с почетка века да би сајбер простор могао изједначити мале и велике државе, стварајући окружење у коме су сви рањиви, бројни фактори, пре свега у погледу људских и материјалних ресурса, довели су до пресликавања ситуације из физичког простора у виртуелни, у коме поново доминирају велике силе (Chabrow, 2009; R.T. Stimpson, 2015: 4). Међутим, и велике силе суочавају се са ограничењима као што су мањак људства или питање имица у међународном окружењу, што их је навело да у своје сајбер операције почну интегрисати недржавне

актере, успостављајући различите модалитете сарадње са њима. Иако су хакерске групе у прошлости биле расцепкане и са мало ресурса, временом је дошло до њиховог укрупњавања и професионализације чиме су оне постале врло потентан актер у надметању у сајбер простору (ENISA, 2024: 20).

Степен њихове интеграције може значајно варирати – од врло блиског где држава има формализовану сарадњу и непосредно делегира задатке, до прећутног толерисања криминалних радњи када су мете друге државе (Maurer, 2018: 268; Grabosky 2015: 10). Најопасније међу њима јесу управо оне групе најближе државама због чега је понекад тешко и утврдити дистинкцију између њих. Њихови напади су сложени, технолошки напредни, изведени након дугих припрема и најчешће бивају усмерени ка крађи података, шпијунажи и ометању рада институција држава или важнијих недржавних актера (ENISA, 2024: 20). Обимна сарадња између државних и недржавних актера указује да владе препознају корист од таквог вида борбе у „сивој зони", пре свега у могућности негирања одговорности. Координишући и штитећи различите хакерске групе уз одбијање прихватања одговорности омогућава појединим државама да уживају бројне бенефите које пружа овакав вид ратовања (Canfil, 2022: 1). Државе се изузетно ретко одлучују да прихвате одговорност за напад, чак и у оним околностима када је сасвим јасно одакле је он потекао. Додатно, званичници одбијају и да демантују такве наводе бирајући пребацивање одговорности на друге, без одбацивања навода о сопственој умешаности (енг. Non-denial denial), или одбијајући да се уопште и да коментар (Brown, Fazal, 2021: 402). Тиме је креирано окружење у коме државе тешко могу одговорити на овакве нападе без кршења сопствених прописа, као што је то случај са САД, где је линија разграничења између државних сајбер снага и илегалних хакера много јасније одређена (Shwedo, 2025).

Са друге стране, пракса интеграције проксија у сајбер стратегије и операције има последице које се могу негативно одразити на мале државе са лимитираним ресурсима. Пре свега, државе су у стању да, барем привремено, мобилишу огроман број хакера: Украјини је подршку у њеном сајбер рату против Русије пружило око 400.000 хакера изводећи нападе на њене институције и компаније (Bloomberg, 2022). Поред тренда

омасовљавања, државе су започеле и са пролиферацијом знања у домену сајбер технологија (CyberPeace Institute, 2023: 16). Такође, тренд који је у претходне две године постао изразито актуелан на бројним илегалним форумима јесте пролиферација софистицираних малициозних програма ка технички мање вештим интернет криминалцима, начин пословања познат као „рансомвер као услуга" (енг. Ransomware as a Service) (Martin, Whelan, 2023: 10). У процес пролиферације малвера укључене су и државне сајбер трупе, чиме се додатно отежава одређивање одговорности за напад (De Stercke, Petrovska & Janssens, 2024: 36).

Сајбер простор отворио је нову димензију за надметања између великих сила у коме је извођење напада испод прага започињања оружаног сукоба постао учестао приступ. Ангажујући сопствене сајбер ресурсе у виду делова оружаних снага и обавештајних агенција, државе, а пре свега велике силе као субјекти са највише расположивих ресурса, почеле су спроводити различите врсте активности с циљем прикупљања осетљивих података о противницима (како институција тако и грађана и привредних субјеката) и саботажом елемената критичне инфраструктуре. Временом, у овај окршај почеле су се укључивати и различите групе сајбер криминалаца које су, вођене бројним мотивима (новац, идеологија, патриотизам), почеле улазити у различите аранжмане сарадње са државама, постајући њихов прокси у глобалном сајбер рату.

Раст напетости између великих сила додатно су интензивирали окршај у „сивој зони" који је значајно добио на интензитету са руском инвазијом на Украјину. Акције усмерене на уништење рачунарске мреже и поверљивих докумената, крађу осетљивих података и утицање на ставове јавног мњења кроз манипулације у информационој сфери постали су главне особине тренутног сајбер окршаја који се одвија између status quo и ревизионистичких држава. У таквом надметању су, услед глобалне умрежености, невољно укључене и западнобалканске државе које се налазе пред значајним изазовима које представљају сајбер напади.

Искуство балканских држава: између државних хакера и сајбер криминалаца

Паралелно са првим нападима у зору 24. фебруара 2022. године, сајбер простор Украјине био је преплављен активностима руских хакера усмерених ка крађи осетљивих података, онеспособљавању сателитских комуникација и уништењу рачунарске мреже (SSSCIP, 2022:7). Велики сајбер напори које је Русија уложила током првих неколико месеци, а који су представљали преседан по њиховом обиму и разноврсности (Bateman, 2022: 42–46), ипак нису донели прижељкиване резултате (Wilde, 2024: 7; Bateman, 2022). Дугогодишња припрема инфраструктуре и људства, искуство са ранијим нападима, али и издашна помоћ западних партнера допринели су да Кијев преброди критичну фазу рата (Krasznay, 2024: 4). Помоћ Запада, као и немогућност наношења трајне штете Украјини, подстакли су Москву да, неколико месеци након почетка сукоба, прилагоди свој приступ тренутним околностима рата. Промене су биле усмерене на ангажовање како државних (El Pais, 2024) тако и недржавних хакера, као и интензивирање напада на савезнике Украјине који су слабије припремљени за нову врсту борбе.

Владе држава Западног Балкана сусреле су се са значајним изазовом у виду различитих државних сајбер снага и проксија, првенствено пореклом из Русије и Ирана, с циљем утицања на јавност, крађе података, стицања финансијске добити и омогућавања даљих напада на западне државе. Најчешће мете биле су државне институције, електроенергетска инфраструктура и велике компаније као што су трговински ланци и банке. Овакве акције могу изазвати двоструке губитке по државе и компаније. Првенствено, напади могу изазвати непосредну штету кроз физичко оштећење и нарушавање начина функционисања уређаја што узрокује потребу за непосредном санацијом штете (Салій, 2024: 332). С друге стране, значајно опаснији јесу индиректни губици који се могу манифестовати кроз успорен или обустављен рад система, финансијске издатке потребне за унапређење њихове заштите, губитак поверења корисника и цурење поверљивих информација (2024: 332).

У даљем тексту биће анализирани неки од значајнијих случајева који илуструју претњу коју представљају сајбер напади повезани са великим

силама. Важно је нагласити да приликом проучавања сајбер инцидената постоје бројне непознанице, пре свега у погледу броја извршених напада, починилаца, мотива и нанете штете (Oppenheimer, 2024: 29). До јавности допре тек један део информација јер, поред обзнањених напада, постоје и успешни напади о којима нападачи нису публиковали никакве податке, а за које жртва не зна ни да су се догодили или напади за које жртва не жели да објави информације (2024: 29). И поред тога што значајан број сајбер инцидената остаје „позната непознаница" (2024: 31), доступне информације указују да се западнобалканске државе налазе пред великим ризиком од оваквих претњи које ће се у будућности само повећавати.

Пример паралишућег сајбер напада на државне институције Црне Горе августа 2022. године јасно показује ризике с којима се суочавају мање државе у сајбер простору. Напад који је, судећи према доступним подацима, изведен изнутра (не)намерним поступањем запослених (Balkan Insight, 2022a), паралисао је различите институције, онемогућавајући њихово нормално функционисање. Одговорност за напад преузела је хакерска група номинално означена као организација са искључивим лукративним циљевима – Куба Рансомвер (енг. Cuba Ransomware) (Bank Info Security, 2022). Ипак, због својих активности у украјинском сајбер простору, ова група је означена као организација са одређеним степеном повезаности са руским обавештајним агенцијама (TechCrunch, 2023). Брза реакција савезника у оквиру НАТО спречила је даље ширење малициозних програма, умањујући штету која је могла настати (CSIS, 2024), демонстрирајући значај међународне сарадње у превазилажењу сајбер претњи.

Значајно драматичније последице изазвала је серија напада на рачунарску инфраструктуру државних органа Албаније од стране иранских хакера. Почевши у јулу 2022. године, хакерска група Правда отаџбине (енг. Homeland Justice), која је директно повезана са државним структурама у Техерану, почела је са нападима који су резултовали уништењем података и публиковањем поверљивих информација као што су идентитети албанских обавештајаца или садржај мејлова директора обавештајних агенција (Oghanna, 2023). Даљи напади навели су Тирану да септембра исте године повуче радикалан потез прекидајући дипломатске односе са Техераном (Al Jazeera, 2022), што је била само

последња фаза у односима који су постали натегнути 2016. године када је Влада Албаније одлучила да прихвати више хиљада чланова иранске опозиционе групе Муџахедин-е-Халк (енг. Mujahedin-e-Khalq), што се и узима као повод за нападе (Zaimi, 2023).

Прекид дипломатских односа није значио и крај малициозних акција: у октобру су нападнути полицијски органи што је изазвало цурење података који садрже информације о око сто хиљада грађана Албаније које Министарство унутрашњих послова сумњичи за извршење противзаконитих дела, што је изазвало велику забринутост у јавности (Balkan Insight, 2022b). Ирански хакери деловали су синхронизовано са руским прокси хакерским групама које су у истом периоду нападале рачунарске мреже институција Црне Горе, Бугарске, Северне Македоније и самопроглашене државе Косова (Oghanna, 2023). Такође, покрадени подаци са албанских сервера примарно су се налазили на руским сајтовима и телеграм групама (Oghanna, 2023), што додатно упућује на постојање сарадње ове две државе у сајбер простору с циљем унапређења шанси за успех операција.

Случајеви Црне Горе и Албаније указују на способности сајбер актера да проузрокују значајну штету институцијама онемогућавајући њихов рад и делећи осетљиве податке са јавношћу или црном тржишту, чиме се креира атмосфера неповерења у способност власти да очува своју безбедност и својих грађана. С друге стране, серија напада на ове две државе показују да постоје актери који имају дефинисану сајбер стратегију у дигиталном простору (поремећај рада државних органа и креирање атмосфере неповерења према властима), али и сајбер операције којима теже да постигну своје циљеве (напади на институције, симултани напади на више држава, објављивање осетљивих података). Иако владе у Подгорици и Тирани нису промениле своје спољнополитичке позиције, сајбер напади су дефинитивно негативно утицали на њихову стабилност и функционисање наметањем додатних трошкова.

Још једна врста операција којима су таргетиране западнобалканске државе јесте покушај утицања на јавност кроз манипулације у информационој сфери. Борба за контролу над наративима између великих сила већ дуго је присутна у контексту њиховог надметања, али коришћење сајбер инструмената у те сврхе представља важан новитет

који креира додатне друштвене тензије. Иако је случај румунских председничких избора привукао значајну пажњу светске јавности управо због питања утицаја сајбер манипулација на исход избора (BBC, 2024), присуство координисаних активности лажних налога на друштвеним мрежама било је присутно и током последњих хрватских председничких избора одржаних децембра 2024, односно јануара 2025. године.

На друштвеним мрежама идентификовани су лажни налози који су делили одређене карактеристике: радикално леви или десни ставови који промовишу проруске, анти-ЕУ и анти-НАТО поруке, фотографије генерисане вештачком интелигенцијом, генеричне поруке и описи налога и повезаност налога кроз међусобно дељење садржаја (Center for international resilience, 2025). Овакав садржај био је дистрибуиран на више језика, а посебно висока фреквентност порука подршке председнику Милановићу уследиле су након његове изјаве противљења могућем учешћу Хрватске у сукобу у Украјини (Center for international resilience, 2025). Покушаји утицања на доминантне наративе представља део шире стратегије Москве која ставља у фокус савезнике Кијева у Европи, с циљем умањење подршке помоћи Украјини (ENISA, 2024: 95). Као што је раније истакнуто, коришћење манипулација информацијама је саставни елемент руске сајбер стратегије која је у односу на почетак рата 2022. године доживела еволуцију пребацујући тежиште током 2023. године са Украјине на њене партнере, међу које се сврстава и Хрватска (ENISA, 2024: 95).

У најспецифичнијој позицији у односу на све друге државе Западног Балкана налази се Србија, као актер који је сачувао неутралност у односу на руско-украјински сукоб. Толерисање односа са Москвом од стране Запада захтевало је одређене уступке Београда, пре свега у погледу продаје оружја Украјини и осуди инвазије у Генералној Скупштини УН. Овакви потези учинили су Србију рањивом на сајбер претње са Истока, док ју је њена неутралност лишила помоћи споља, која је у случају Црне Горе била пресудна у одбрани. У таквом сплету околности, Србија је постала рањива на сајбер претње, на шта указују и подаци компаније Касперски (енг. Kaspersky): током 2022. године Србија је била на 13. месту држава које су трпеле највише напада на своју критичну инфраструктуру (Cord, 2023).

Највише је претрпела Електропривреда Србије (ЕПС) која се нашла у фокусу руске сајбер групе Квилин (енг. Qilin), глобално познате по високософистицираним акцијама који таргетирају западне компаније и институције (Balkan Insight, 2024). Циљ напада било је извлачење података за које би се могао тражити откуп или који би се могли продати на црном тржишту (Balkan Insight, 2024). Поред тога што је отежано функционисање ЕПС-а, хакери су, према оценама експерата, могли доћи и до личних података грађана које компанија поседује или података о самом систему електроснабдевања (Balkan Insight, 2024). Посебно осетљив случај је хидроелектрана „Бајина Башта", чију су рачунарску мрежу хакери компромитовали што је довело до крађе пословне документације, личних карата запослених, па чак и архитектонских цртежа и планова читавог комплекса (Radio Slobodna Evropa, 2024).

Убрзо је откривено да су и друге институције компромитоване, па су се на црним тржиштима могли наћи креденцијали за налоге запослених Поште Србије, Србијагаса или Националне службе за запошљавање што отвара простор за даље акције (BIRN, 2023b). Контрола над мејл адресама запослених у институцијама омогућило би малициозним актерима да имају увид у електронску пошту, али и да започну фишинг нападе кријӯћи се иза званичних налога. Поред државних компанија и институција, на удару се нашао и ланац продавница Гигатрон, одакле су такође преузети подаци који могу угрозити безбедност грађана (BIRN, 2023a). Иако ови напади нису изазвали велику директну материјалну штету као што су то били неки од напада на Украјину у периоду пре 2022. године, овакве акције имају за циљ стварање секундарних трошкова у виду угрожавања безбедности података грађана или институција, као и урушавања поверења јавности у способности државних органа да сајбер нападаче спрече у таквим намерама. Одговор надлежних органа било је ћутање (Radio Slobodna Evropa, 2024), односно негирање постојања било какве штете, покушавајући тиме да одврате пажњу са случајева, умање штету и последично заташкају одговорност и пропусте. За разлику од других држава Западног Балкана, где је питање починиоца било отворено одмах након почињеног напада, означавање кривца за нападе на српске компаније и институције је изостало.

Наведени случајеви сајбер напада на државе Западног Балкана, као и бројни други који нису сврстани овде (као што су напади на Министарство пољопривреде и Фонд здравственог осигурања у Северној Македонији (BIRN, 2023a), Парламентарне скупштине Босне и Херцеговине (BIRN, 2023a) и Републички геодетски завод Србије (BIRN, 2022)), указују на постојање проблема у погледу сајбер безбедности међу свим овим државама који би могли бити спречени предузимањем одређених превентивних корака. Крађа података и њихова накнадна продаја или уништење не представљају ризик искључиво за институције већ и за саме грађане, због чега је изградња отпорности како на нивоу организација тако и на нивоу појединаца врло важна за колективну сајбер безбедност.

Будућност балканских држава у сајбер простору – постоји ли решење за рањивост

Растући број напада, све затегнутији односи између различитих полова моћи у глобалној арени, технолошки напредак у виду вештачке интелигенције, све замагљенија линија између државе и сајбер криминала и манипулације у информационој сфери представљају главне трендове са којима се суочавају државе у дигиталном простору. Посебно значајно надметање одвијаће се у информационом простору где су борбе за поседовање тачних информација и контролу наратива постали основни елементи савремене политике великих сила, што се може уочити и у тренутном рату у Украјини (ENISA, 2024: 91). У таквим околностима, употреба сајбер средстава представља један од важнијих инструмената којим велике силе могу утицати на расподелу моћи у међународном поретку.

На све ове изазове неопходно је одговорити проактивним и превентивним мерама како би се умањили ризици које носи дигитални простор. Да сајбер одбрана није унапред изгубљена и да адекватна припрема може пружити позитивне резултате јесте Украјина. Након сукоба у Донбасу 2014. године и серије врло деструктивних сајбер напада, Кијев је уложио значајне напоре у изградњу својих одбрамбених капацитета адекватном обуком људства, ангажовањем приватних компанија специјализованих за сајбер одбрану и кооперацијом са другим

државама (Krasznay, 2024: 2). Резултат је био успешна одбрана критичне инфраструктуре и опстанак Украјине у сајбер простору и након три године од почетка сукоба.

Најважнија, али уједно и најслабија, карика у одбрани у сајбер простору јесу сами корисници (Gorgulenko, 2024: 19) и њихова едукација о ризицима неадекватног коришћења рачунара игра кључну улогу у подизању нивоа безбедности (De Stercke, Petrovska & Janssens, 2024: 40). Коришћење нелиценцираних програма, а посебно оперативних система преузетих са пиратских сајтова, може бити извор небезбедности у рачунарској мрежи (Федієнко, 2023: 148). Према резултатима истраживања које је спровео NALED са 144 јединице локалне самоуправе, 29% њих се у више од половине случајева користе пиратским програмима (NALED, 2023). Посећивање непоузданих интернет адреса, интеракција са мејловима сумњивог порекла и садржаја и откривање осетљивих података непознатим лицима само су неки од начина на који појединац може угрозити интегритет рачунарске мреже.

Најдиректнији начин за сузбијање надеведних проблема јесу континуиране едукације и кампање за подизање свести међу запосленима, где је такође неопходно показати већу проактивност. Тек трећина јединица локалних самоуправа има најмање једну особу која је у последње три године похађала неки вид обуке из области сајбер безбедности (NALED, 2023). Тестови пенетрације (надгледана симулација сајбер напада с циљем оцене нивоа безбедности рачунарске мреже и обучености запослених) и програми подстицаја лицима која пронађу грешке у апликацијама такође су се показали као адекватна средства за подизање дефанзивних капацитета (Holt et al., 2023: 843). Иако су ове праксе знатно учесталије у приватном сектору (Kranenbarg et al., 2018: 10), поједине државе као што су САД и Украјина (Тетєвін, 2024: 265) почеле су активно користити ове мере како би додатно тестирале и заштитиле своје критичне секторе економије и администрације.

Сарадња са глобалним лидерима на пољу заштите рачунарских мрежа показала се врло ефикасном у борби против софистицираних сајбер напада: њихова експертиза и способност да идентификују и спрече малициозне акције надилази капацитете и највећих држава, што их чини једним од виталних актера глобалне сајбер одбране (Krasznay, 2024: 3).

Ипак, приватно-јавно партнерства са иностраним компанијама за демократска друштва носе и ризике, пре свега у погледу способности одржавања контроле над спољном и безбедносном политиком. Због тога је важно претходно дефинисати у којим околностима и у каквим аранжманима је неопходно посезати за експертским знањима иностраних компанија (Bateman, Beecroft & Wilde, 2022).

Поред сарадње са приватним сектором, државе Западног Балкана могу рачунати и на до сада неискоришћени потенцијал међународне кооперације, пре свега на регионалном плану. Ниједна држава није способна да се самостално носи са свим сајбер претњама, нити је спремна да у потпуности преузме на себе одговорност за борбу против хакера (Haner, Knaker, 2021: 6), што даје додатан импулс за унапређење сарадње у сајбер сфери (Тетевін, 2024: 265–266). Искуство Црне Горе указује да управо такви видови кооперације могу бити пресудни за умањивање штете или потенцијално одвраћање даљих напада. Правни и финансијски оквири за унапређење сајбер безбедности који постоје у НАТО и ЕУ могу пружити снажан подстрек за повећање регионалне и европске сарадње у овом све важнијем пољу (Krasznay, 2024: 4).

Закључак

Сајбер напади постали су неизоставан инструмент спољне политике у савременом међународном окружењу, омогућавајући државним и недржавним актерима да врше нападе на своје противнике без употребе физичке силе. Развој дигиталних технологија, оружани сукоби као што је онај у Украјини и интеграција хакерских група у државне сајбер снаге довели су до пораста броја напада чији је циљ ометање рада институција, манипулисање јавним мњењем и прикупљање осетљивих података. Овај тренд је посебно видљив на Балкану, где се хакерски напади често користе као вид притиска на државе услед одређених спољнополитичких потеза, као што су подршка Кијеву или иранској опозицији.

Примери напада на западнобалканске државе у претходних неколико година илуструју ризике са којима се ове државе суочавају: напад на Црну Гору паралисао је институције и приморао државу да се ослони на међународну помоћ; ирански напади на Албанију резултирали су штетом

која је довела и до прекида дипломатских односа, док су напади на Србију и њен електроенергетски сектор указали на рањивост критичне инфраструктуре на сајбер претње. Ови инциденти наглашавају улогу сајбер напада као средства за вршење политичког притиска и пројекцију моћи великих сила, али и на недостатке са којима се ове државе суочавају. Пре свега, оне појединачно не поседују довољно развијене капацитете за превенцију и одбрану од сложених сајбер напада. Недостатак финансијских и људских ресурса чини их посебно осетљивим, док недовољна регионална сарадња додатно отежава одбрану од сајбер инцидената. Низак ниво свести о значају сајбер безбедности међу институцијама и грађанима представља додатни ризик, јер велики број напада користи технике социјалног инжењеринга како би заобишао техничке мере заштите. Решења за ове изазове морају укључивати улагање у сајбер безбедност, јачање сарадње са међународним партнерима и унапређење домаћих капацитета за заштиту критичне инфраструктуре. Примери квалитетно припремљене сајбер одбране, попут Украјине, показују да је могуће изградити ефикасан одбрамбени систем кроз комбинацију техничких мера, едукације и међународне подршке.

Западнобалканске државе морају посветити већу пажњу својој сајбер безбедности како би одговориле на растуће изазове у дигиталном простору. Убрзани технолошки развој и све већа интеграција сајбер операција у геополитичке стратегије указују да ће сајбер напади у будућности постати још интензивнији и деструктивнији. Само кроз систематску припрему, регионалну сарадњу и међународну подршку могуће је изградити одрживу одбрану од сајбер претњи и очувати стабилност и безбедност у дигиталном окружењу.

Литература

Al Jazeera. (2022). Albania cuts diplomatic ties with Iran over cyberattack. Preuzeto: 25. 1. 2025. sa https://www.aljazeera.com/news/2022/9/7/albania-cuts-diplomatic-ties-with-iran-over-cyberattack.

Balkan Insight. (2022). Iranian Hackers Leak Database of Albanian Criminal Suspects. Preuzeto: 20. 1. 2025. sa https://balkaninsight.com/2022/10/03/iranian-hackers-leak-database-of-albanian-criminal-suspects/.

Balkan Insight. (2022). Montenegro Sent Back to Analog by Unprecedented Cyber Attacks. Preuzeto: 19. 1. 2025. sa https://balkaninsight.com/2022/09/01/montenegro-sent-back-to-analog-by-unprecedented-cyber-attacks/.

Balkan Insight. (2024). Latest Cyber-Attacks in Serbia Raise Fresh Questions about Defence Katarina Baletic. Preuzeto: 20. 1. 2025. sa https://balkaninsight.com/2024/01/16/latest-cyber-attacks-in-serbia-raise-fresh-questions-about-defence/.

Bateman, J. (2022). Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications. Carnegie Endowment for international peace. Preuzeto: 14. 1. 2025. sa https://carnegie-production-assets.s3.amazonaws.com/static/files/Bateman_Cyber-FINAL21.pdf.

Bateman, J., Beecroft, N. & Wilde, G. (2022). What the Russian Invasion Reveals About the Future of Cyber Warfare. Carnegie Endowment for International Peace, Preuzeto: 11. 1. 2025. sa https://carnegieendowment.org/2022 /12/19 /what-russian-invasion-reveals-about-future-of-cyber-warfare-pub-88667.

BBC. (2024). Romania hit by major election influence campaign and Russian cyber-attacks. Preuzeto: 21. 1. 2025. sa https://www.bbc.com/news /articles/cgq18w507dko.

BIRN. (2022). Hakeri imali pristup mejlovima zaposlenih u katastru Srbije: Stručnjaci kažu da opasnost još nije prošla. Preuzeto: 20. 1. 2025. sa https://birn.rs/hakeri-imali-pristup-mejlovima-zaposlenih-u-katastru-srbije-strucnjaci-kazu-da-opasnost-jos-nije-prosla/.

BIRN. (2023). Battle for Balkan Cybersecurity: Threats and Implications of Biometrics and Digital Identity. Preuzeto: 18. 1. 2025. sa https://balkaninsight.com/2023/06/30/battle-for-balkan-cybersecurity-threats-and-implications-of-biometrics-and-digital-identity/.

Bloomberg. (2022). Ukraine Says 400000 Volunteers Aid Hacking Against Russia. Preuzeto: 17. 1. 2025. sa https://www.bloomberg.com/news/articles/2022-03-04/ukraine-s-hacker-army-said-to-be-helped-by-400-000-supporters.

Brown, J. M., Fazal T. M. (2021). "#SorryNotSorry: Why states neither confirm nor deny responsibility for cyber operations". European Journal of International Security, Cambridge, Vol 6 (4), 401–417. DOI: 10.1017/eis.2021.18.

Canfil, J. K. (2022). "The illogic of plausible deniability: why proxy conflict in cyberspace may no longer pay". Journal of Cybersecurity, Oxford, Vol 8 (1), 1–16. DOI: 10.1093/cybsec/tyac007.

Center for International Resilience. (2025). Inauthentic & Malign Influence Activity Croatian Presidential Runoff. Preuzeto: 2. 2. 2025. sa https://www.info-res.org/app/uploads/2025/01/Inauthentic_Behavior_-Croatian_Presidential_Runoff_v2.pdf.

Center for Strategic and International Studies (CSIS). (2024). Russia Aims at Montenegro. Preuzeto: 17. 1. 2025. sa https://www.csis.org/analysis/russia-aims-montenegro.

Chabrow, E. (2009). "Conventional War Strategy Doesn't Work in Cyberspace". GovInfoSecurity. Preuzeto: 18. 1. 2025. sa https://www.govinfosecurity.com/conventional-war-strategy-doesnt-work-in-cyberspace-a-1924.

Cord. (2023). Focused On Cyber Security. Preuzeto: 21. 1. 2025. sa https://cordmagazine.com/sector-in-focus/hi-tech/goran-stojadinovic-a1-serbia-focused-on-cyber-security/.

CyberPeace Institute. (2023). Cyber Dimensions of the Armed Conflict in Ukraine – Q3 2023. CyberPeace Institute. Preuzeto: 23. 1. 2025. sa https://cyberpeaceinstitute.org/wp-content/uploads/2023/12/Cyber-Dimensions_Ukraine-Q3-2023.pdf.

D'Cunha, S., Ferraro, T., & Rodenhäuser, T. (2025). "'Hybrid threats, 'grey zones', 'competition', and 'proxies': When is it actually war?". EJIL:Talk!. Preuzeto: 20. 1. 2025. sa https://www.ejiltalk.org/hybrid-threats-grey-zones-competition-and-proxies-when-is-it-actually-war/.

De Stercke, C., Petrovska, O., & Janssens, J. (2024). "Cybercrime & cyber warfare: entering the grey zone". Freedom from Fear Magazine. United Nations Interregional Crime and Justice Research Institute, Vol 19, 31–41.

El Pais. (2024). Ukraine claims Russia uses its cooperation with China to carry out cyberattacks. Preuzeto: 21. 1. 2025. sa https://english.elpais.com/international/2024-02-12/ukraine-claims-russia-uses-its-cooperation-with-china-to-carry-out-cyberattacks.html.

Gorgulenko, V. (2024). "Cyber warfare in modern military conflicts: best practices, trends and patterns of development", Modern information

technologies in the field of security and defense . Kyiv, 50(2), 11–28. DOI: 10.33099/2311-7249/2024-50-2-11-28.

Grzegorzewski, M., Marsh, C. (2024). "A Strategic Cyberspace Overview: Russia and China". Great Power Cyber Competition: Competing and Winning in the Information Environment. Routledge, London, 6–25.

Haner, J. K., Knake R. K., (2021). "Breaking botnets: A quantitative analysis of individual, technical, isolationist, and multilateral approaches to cybersecurity". Journal of Cyber Security, Vol. 1 (15), 1–15. DOI: 10.1093/cybsec/tyab003

Harknetta, R. J., Smeetsb, M. (2022). "Cyber campaigns and strategic outcomes". Journal of Strategic Studies. Taylor and Francis, London, Vol 45 (4), 534–567. DOI: 10.1080/01402390.2020.1732354.

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, Vol. 22, 825–848. DOI: 10.1111/1745-9133.12646.

Krasznay, C. (2024). "The Role of Civilian Cybersecurity Companies in Military Cyber Operations". Land Forces Academy Review, Sibiu, Vol 29 (113), 1–10. DOI: 10.2478/raft-2024-0001.

Martin, J., Whelan, C. (2023). "Ransomware through the lens of state crime: Conceptualizing ransomware groups as cyber proxies, pirates, and privateers". State Crime Journal, Pluto Journals, London, Vol 12 (1), 1–25. DOI: 10.13169/statecrime.12.1.0001.

Maurer, T. (2018). Cyber Mercenaries. Cambridge, Cambridge University Press, Cambridge.

Monte, M. (2015). Network Attacks and Exploitation: A Framework. Wiley, Hoboken.

NALED. (2023). Interni podaci (Excel format). Preuzeto: 26. 1. 2025.

Novaković, I. & Rizmal, I. (2017). Cyber warfare: new type or warfare or additional element of conventional warfare. ISIKS 2017: Asymmetry and Strategy. Beograd.

Oghanna, A. (2023). "How Albania Became a Target for Cyberattacks". Foreign Policy. Preuzeto: 21. 1. 2025. sa https://foreignpolicy.com/2023/03/25/albania-target-cyberattacks-russia-iran/.

Oppenheimer, H. (2024). "How the process of discovering cyberattacks biases our understanding of cybersecurity". Journal of Peace Research. SAGE Publications, London, Vol. 61 (1), 28–43. DOI: 10.1177/00223433231217687.

Radio Slobodna Evropa. (2024). Hakersko 'ogoljavanje' poslovanja Hidroelektrane Bajina Bašta u Srbiji. Preuzeto: 22. 1. 2025. sa https://www.slobodnaevropa.org/a/hidroelektrana-bajina-basta-hakerski-napad/33026495.html.

Shwedo, B. J. (2025). Gostujuće predavanje 7. i 8. marta. Vojna akademija.

State Service of Special Communications and Information Protection of Ukraine (SSSCIP). (2022). Russia's Cyber Tactics: Lessons Learned. SSSCIP, Kyiv.

Stimpson, R. T. (2015). Cyberwarfare Will Not Replace Conventional Warfare. Joint Command and Staff Programme, Canadian Forces College, Toronto.

TechCrunch. (2023). Cybercriminals who targeted Ukraine are actually Russian government hackers, researchers say. Preuzeto: 22. 1. 2025. sa https://techcrunch.com/2023/05/15/cybercriminals-who-targeted-ukraine-are-actually-russian-government-hackers-researchers-say/.

The European Union Agency for Cybersecurity (ENISA). (2024). ENISA Threat Landscape 2024. ENISA. Athens. DOI: 10.2824/0710888.

Vuletić, D. (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. DOI: 10.5937/vojdelo1707308V.

Wilde, G. (2024). Russia's Countervalue Cyber Approach: Utility or Futility?. Carnegie Endowment for international peace. Preuzeto. 24. 1. 2025. sa https://carnegieendowment.org/research/2024/02/russias-countervalue-cyber-approach-utility-or-futility?lang=en.

Weulen Kranenbarg, M., Holt, T. J. & van der Ham, J. (2018). "Don't shoot the messenger! A criminological and computer science perspective on coordinated vulnerability disclosure". Crime Science, Vol. 7 (16), 7–16. DOI: 10.1186/s40163-018-0090-8.

Zaimi, G. (2022). "Iran's Balkan front: The roots and consequences of Iranian cyberattacks against Albania." Middle East Institute. Preuzeto: 22. 1. 2025.

sa https://mei.edu/publications/irans-balkan-front-roots-and-consequences-iranian-cyberattacks-against-albania.

Салій, А. Я. (2024). „Особливості відповідальності за кібератаки в країнах ЄС". Науковий вісник Ужгородського національного університету, Серія: Право, Uzhhorod, Vol. 81 (2), 330–334. DOI: 10.24144/2307-3322.2024.81.2.51.

Тетєвін, М. С. (2024). „Досвід України в галузі міжнародного співробітництва в галузі кібербезпеки". Науковий вісник Ужгородського національного університету, Серія: Право, Uzhhorod, Vol. 82 (3), 263–266. DOI: 10.24144/2307-3322.2024.82.3.41.

Федієнко, О. П. (2023). „Загрозливі тенденції використання державою-агресором шкідливого програмного забезпечення в умовах правового режиму воєнного стану". Інформація і право, Kiev, Vol. 3 (46), 142–153. DOI: 10.37750/2616-6798.2024.1(48).

CYBERATTACKS AS A STRATEGIC INSTRUMENT OF FOREIGN POLICY: THE WESTERN BALKANS IN THE ERA OF HYBRID WARFARE

Aleksandar BOGIĆEVIĆ*
University of Defence – Strategic Research Institute

Abstract: Raising tensions between the United States, the dominant power in the existing international order, and its challengers, mainly China, Russia, and Iran, deteriorated the stability of the global order and, consequently, international security. The role of cyber threats in fostering such an unsafe atmosphere is constantly increasing. They become increasingly common among states, inflicting damage to other actors and influencing their political

* E-mail: aleksandar.bogicevic@mod.gov.rs, ORCID: https://orcid.org/0009-0006-7450-5193.

The paper was created as part of the Ministry of Defence project titled "Security Challenges of Western Balkan Countries within the European Security Paradigm", No. ISI/DH1/24–25, implemented by the research team and the Regional Security Research Group of the Strategic Research Institute, along with an external contributor, during the period 2024–2025.

decision-making processes. The lack of conclusive evidence about perpetrators of cyberattacks and the possibility of denying and deflecting responsibility for them make cyberspace an ideal place for state and non-state actors to focus on conducting operations in a „grey area". An additional challenge for European states was created with the beginning of the war in Ukraine, starting a new phase in cyberspace war, characterised by an increasing number of attacks and sophistication. To increase their capacity for conducting cyber operations while maintaining the possibility of denying responsibility for them, the growing importance in cyberspace is given to hacker groups that cooperate to some extent with states, thereby taking on the role of cyber proxies. Such a complex and increasingly unstable international order also affects the Western Balkans states, which are alarmingly exposed to sophisticated cyberattacks from foreign actors to which they cannot respond. The reasons behind these attacks can be linked to the foreign policies and positions of these states on significant international issues, including backing the Iranian opposition, preserving military and political neutrality, and aiding Ukraine's war efforts. These attacks, which focus on critical infrastructure such as state institutions, state-owned enterprises, and citizens' data, pose a significant security risk to the entire society, underscoring the urgent need for enhanced cybersecurity measures. This paper aims to identify and analyse the strategic utilisation of cyberattacks by other states, primarily great powers, focusing on implications for the Western Balkans states. After the beginning of the war in Ukraine in February 2022, several sophisticated cyberattacks by non-state cyber proxy actors aimed at the Western Balkan countries did severe damage to government institutions in several cases (Montenegro, Albania, and North Macedonia, especially), while Serbia was hit with a combination of attacks on institutions and state enterprises. In all cases, attacks interrupted the work of institutions (in the case of Montenegro, for several months), leaked undisclosed state documents (as in Albania and Serbia) or endangered citizens' data. These attacks have shown several important trends in global cybersecurity: first, cyberattacks became a popular option for „punishing „states for their political stances on specific questions; second, everybody can be a potential target, so everybody must be vigilant and ready for defence; and last, trying to punish perpetrators of attacks is almost impossible, particularly if we take into account the fact that attackers are cyber proxies under the protection of other governments, giving them immunity from persecution. Because retaliation is impossible, the Western Balkan states must find different solutions to upgrade their cyber

defence. The template for conducting a strong defence in cyberspace can be seen in Ukraine, which survived for more than three years in the digital space, despite powerful Russian cyberattacks. Building international cooperation with state and non-state actors could represent a key element of defence in the digital world. Besides, building internal capacities by raising awareness through education must become a crucial aspect of cyber defence, particularly when most attacks target individuals as the weakest link in the cyber defence network. No indicator suggests that the future will bring fewer attacks by cyber proxies, especially with the introduction of artificial intelligence, so countries must be prepared for an even more unstable cyber world and more sophisticated cyber threats.

Keywords: cyber warfare, hybrid warfare, foreign policy, cybersecurity, Western Balkans.