САЈБЕР РАТОВАЊЕ: НОВА ВРСТА РАТОВАЊА ИЛИ ДОДАТНИ ЕЛЕМЕНТ КОНВЕНЦИОНАЛНОМ РАТОВАЊУ

Др Игор Новаковић[*]
Директор истраживања, Центар за међународне и безбедносне послове – ISAC фонд

Ирина Ризмал[*]
Самостални истраживач и студент постдипломских студија на University College of London

Апстракт: Сајбер напади представљају нову врсту безбедносне претње створену напретком на пољу информационих технологија, која има потенцијал да преокрене доминантно схватање сукоба. Како је претња релативно нова и убрзано се развија и мења, тешко је предвидети форме њеног даљег развоја и потенцијалне начине исказивања конфликтима. Међутим, треба имати у виду да је већ данас сајбер простор означен као домен ратовања од стране и Европске уније и НАТО, али и од Сједињених Америчких Држава. У чланку су размотрени начини промене конфликата са појавом овог новог домена, који се разликују од стандардних по средствима и приступима, и који практично не зависе од међународно-правних норми које се тичу оружаног сукоба, односно рата. Међутим, то не значи да је ова врста сукоба мање опасна. Иако припадају виртуелној сфери, сајбер напади могу да оставе знатне физичке последице. У чланку је примењена компаративна анализа досадашњих приступа овој тематици, а потом су и размотрене перспективе даљег развоја сајбер ратовања, односно да ли постоје могућности за даљи развој у правцу посебне гране ратовања или ће сукоби у сајбер простору остати само додатни елемент конвенционалним врстама ратовања, као што су већ постали појавом хибридног рата. Ова анализа представља прилог разматрању природе сајбер изазова у будућности, и самим тим омогућава бољи увид у потенцијалне безбедносне изазове за нашу државу данас и ближој будућности.

Кључне речи: асиметричне претње, сајбер простор, сајбер напади, сајбер рат, хибридни рат.

[*] igor.novakovic@isac-fund.org
[*] irina.rizmal@gmail.com

УВОД

Сајбер напади и сајбер ратовање су неки од најчешће коришћених термина у последњих неколико година када се говори о будућности сукоба и развијању нових приступа безбедности. Иако доносиоци одлука у већини држава које обликују модерне међународне односе „сајбер“ стављају у фокус безбедносних и одбрамбених политика, ова област још није добила довољно пажње у академским круговима. Било како било, већ скоро две деценије државе препознају сајбер „као следећу велику ствар у безбедности“, те улажу пре свега у офанзивне сајбер способности и стварање војних сајбер јединица. Са друге стране, у академској литератури фокус је усмерен на дебату око ефективности сајбер напада и да ли они представљају праву опасност у смислу новог, потпуно независног облика ратовања или не. У Србији данас, као и када су у питању друге асиметричне претње, ова дебата је тек донекле отворена, како у стручним круговима, тако и у јавности.

Шира јавност у Србији је „постала свесна“ изазова сајбер ратовања са избијањем кризе у Украјини 2014. године, када је интензивно почео да се спомиње термин „хибридни рат“. Овај термин се користи пре свега у „западним“ медијима како би се описао начин учешћа Русије у сукобу у Украјини и као један од елемената је посебно истакнуто деловање Русије у сајбер сфери које је усмерено на ширење дезинформација, као и на наношење штете стратешкој, односно инфраструктури од посебног значаја за функционисање ове државе. Северноатлантска алијанса (НАТО) дефинише хибридни рат као амалгам употребе конвенционалног и неконвенционалног, регуларног и нерегуларног, информационог и сајбер ратовања.[1] Дакле, хибридно ратовање подразумева употребу свих (или неколико) опција за вођење рата које су на располагању, и не ослања се искључиво на конвенционална средства.[2] Сајбер ратовање се у том контексту схвата као једна од опција којима се надограђује конвенционално ратовање, која доводи до тога да се сукоб између држава одвија и у сајбер простору. Међутим, питање је да ли сајбер ратовање може да постоји као самостална врста ратовања, која није зависна од конвенционалних? У овом тексту ћемо покушати да дамо одговор да ли постоје могућности за такав развој догађаја. Полазна хипотеза је да ће сајбер напади у блиској будућности највероватније остати само једно од средстава за надоградњу конвенционалног сукоба између држава, односно биће употребљавани углавном у оквиру ширег концепта хибридног ратовања. Искључиво сајбер напади биће самостално присутни у мањем броју, али ће се то дешавати у контролисаним условима, са жељом нападача да постигне одређени ефекат (паника, застрашивање, одвраћање итд.), без употребе конвенционалних снага. У сврху доказивања хипотезе сагледаћемо неколико приступа питању сајбер ратовања, пре свега у контексту односа са конвенционалним, хладноратовским облицима ратовања. Текст ће бити фокусиран искључиво на примере сајбер-напада против држава, а који су усмерени на информационе системе, мреже и

[1]van Puyvelde, Damien. Hybrid war – does it even exist?. NATO Review. http://www.nato.int/docu/review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/ (приступљено 14. март 2017.)
[2]Ibid.

информације које се на њима налазе[3], који могу бити самостални, или део напада у ком су употребљене и конвенционалне методе.

ДЕФИНИСАЊЕ САЈБЕР РАТОВАЊА

До данас је незнатан број аутора покушао да објасни природу сајбер напада, међутим нико од њих није успео да дође до јаснијег закључка каква ће бити њихова природа у будућности.[4] Из историјске перспективе, сваки технолошки напредак довео је до стварања нових концепата који су постали веома важни за теоретичаре националне безбедности. Након авијације, нуклеарног и термонуклеарног оружја и дефинисања свемира као простора у којем могу да се одвијају сукоби, „сајбер" је постао нови популарни термин у литератури која се бави питањима безбедности. Иако су првобитни творци интернета, као глобалне мреже која је и покренула сајбер као феномен, видели само позитивне стране у смислу лакшег умрежавања и размене података, сајбер је донео и велики број нових безбедносних изазова и претњи, између осталог и претњу сукоба између држава у сајбер сфери. Постоји сагласност да сајбер напади заиста представљају праву опасност за националну безбедност, и да је у питању „савршено стратешко оружје" за државе, пошто отвара нове могућности ратовања.[5] Само површни поглед на промене приступа водећих светских сила и међународних организација овој области говори о томе да су на снази значајне припреме за потенцијалне сукобе у овој сфери. Неке процене говоре да више од 140 држава развија офанзивне сајбер способности, док велики број њих такође ствара и војне сајбер јединице.[6] Велика Бртианија је прва земља која је јавно признала да развија "широки спектар војних сајбер капацитета, укључујући и способност напада"[7]. Кларк и Кнејк (Clarke and Knake) дефинишу сајбер ратовање као „неодобрену пенетрацију у име или уз подршку владе једне државе у рачунар или мрежу друге државе, или било коју другу активност која утиче на рачунарски систем, са сврхом да дода, промени или фалсификује податке, или да изазове прекид или штету на

[3]Iasiello, Emilio. Are Cyber Weapons Effective Military Tools? *Military and Strategic Affairs* 7 no.1 (2015), 24

[4]види Libicki, Martin C. Cyber War as a Confidence Game, *Strategic Studies Quarterly* no. 5 (2011); Liff, Adam P. Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies* 35 no.3 (2012); Rid, Thomas. Cyberwar and Peace. *Foreign Affairs* 92 no.6 (2013); Iasiello, Are Cyber Weapons Effective Military Tools?; Adams, John A. Jr. *Cyber Blackout: When the lights go out-Nation at Risk* (Friesen Press, 2015)

[5]Види Geers, Kenneth. Sun Tzu and Cyber War (NATO Cooperative Cyber Defence Centre of Excellence, 2010); Libicki, Cyber War as a Confidence Game; Schmidt, Eric & Cohen, Jared. *The New Digital Age: Reshaping the Future of People, Nations and Business* (John Murray Publishers, 2013), Segal, Adam. *Cyber Blackout:When the lights go out-Nation at Risk*

[6]Iasiello, Are Cyber Weapons Effective Military Tools? 54

[7]Изјава министра одбране Велике Британије Филипа Хамонда (Philip Hammond), New cyber reserve unit created. UK Ministry of Defence. https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit (приступљено 25. мај 2017)

рачунару, мрежном уређају или на објектима које рачунарски систем контролише“[8].

Чини се, ипак, да је ова дефиниција преширока, и да се не могу сви сукоби држава у сајбер простору сматрати за рат, пошто варирају како у поступку, тако и по намерама, интензитету и свакако последицама. Сингер и Фридман (Singer, Friedman) као паралелу наводе да су, приликом писања повеље УН разматрани „прекиди поштанских, телеграфских и радио и других врста комуникације“, и да, иако су ти напади сматрани озбиљним, ипак нису дефинисани као акт ратовања.[9] Џозеф Нај (Nye) сматра да се сајбер ратовањем могу сматрати искључиво они сукоби који „имају ефекте који појачавају или су једнаки кинетичком (конвенционалном) насиљу“[10]. Сингер и Фридман су става да постоје два критеријума по којима се одређује да ли се одређени напад може сматрати елементом ратовања. Први критеријум је да ли је у нападу употребљен одговарајући ниво силе који одговара конвенционалном рату, док је други критеријум постојање усмерености и мерљивости, односно постојање „усмерене и намерне везе између узрока и последице“. Другим речима, мора да постоји јасан доказ да је дати напад део приступа одређене државе која жели њиме да угрози функционисање система државе која је мета, укључујући и безбедност њених грађана, као и да је приликом напада употребљена количина силе која одговара конвенционалном рату.

Међутим, и када се испуне ови критеријуми, питање је да ли је то довољно да би ступиле на снагу одредбе међународног права, које је врло тешко применити на сукобе у сајбер простору. Ако пођемо од Повеље Уједињених нација (УН) која се према сукобима између држава односи као према кршењу територијалног интегритета и суверенитета једне државе од стране друге или више њих, у случају сукоба у сајбер простору одмах наилазимо на проблем примењивости ове дефиниције. Сајбер сукоби не подразумевају нужно употребу физичке силе, нити се нужно дешавају искључиво на одређеном географском простору (иако могу оставити последице).[11] Неки аутори дефинишу различите начине када се сајбер напад може окарактерисати као рат, односно када се међународно право може применити. Најпознатији је пример „Талинског приручника за сајбер ратовање“ који су израдили стручњаци за међународно право из НАТО Кооперативног центра за изузетност за област сајбер одбране, а након познатог сајбер напада на Естонију 2007. године. Међутим, иако постоји овакав документ, не постоји воља на међународном нивоу да се прнципи које он предлаже прихвате. Важно је схватити да је сајбер још увек нова област у којој државе и даље експериментишу и истражују капацитете и могућности које она отвара, посебно у офанзивном домену, представљајући тако, „нову врсту барута“ двадесет првог века.[12] Државе

---

[8]Clarke, Richard A. & Knake, Robert K. *Cyber War. The Next Threat to National Security and What to Do About It,* (Harper Collins e books, 2010) 109

[9] Singer, Peter W. & Friedman, Allan. *Cybersecurity and Cyberwar. What everyone needs to know,* (Oxford University Press, 2014) 124

[10]Nye, Joseph S. Jr, Nuclear Lessons for Cybersecurity. *Strategic Studies Quarterly* 5 no.4 (2011) 21

[11]Singer & Friedman, *Cybersecurity and Cyberwar. What everyone needs to know* 124

[12]Питер Раунд (Peter Round) директор за капацитет, наоружање и технологију Европске одбрамбене агенције у обраћању посланицима Европског парламента, цитиран у Cyber security directive held up in face of “Wild West”. Euractiv.

не желе да деле информације о својим капацитетима и активностима у сајбер простору и због тога је јако тешко мобилисати политичку вољу на међународном нивоу да се употреба сајбер простора значајније регулише, барем у блиској будућности. Са друге стране, неке државе, попут Русије су активни заговорници међународне регулације сајбер простора, односно склапања нових споразума којима би се активности у овом простору регулисале, док су, како тврде Кларк и Кнејк, Сједињене Америчке Државе (САД) главни противник оваквог процеса.[13] Докле год сајбер простор остане нерегулисан, биће тешко дефинисати у међународним односима специфичне врсте сајбер напада - а који су изведени самостално, без употребе других метода ратовања - као конкретне покушаје сајбер ратовања.

САЈБЕР РАТОВАЊЕ У ОДНОСУ НА КОНВЕНЦИОНАЛНЕ СУКОБЕ ХЛАДНОРАТОВСКЕ ЕРЕ

Највећи изазов за проучавање феномена сајбер ратовања је чињеница да су примери напада на државе у сајбер простору до данас били прилично ретки. Најчувенији су свакако следећи: напад на интернет странице владе и финансијских институција у Естонији 2007; израелски напад на сиријски систем противваздушне одбране, односно војне контроле ваздушног саобраћаја, исте године; руски напад на владине и медијске сајтове и финансијске институције у Грузији 2008; наводно америчко-израелски напад на иранска нуклеарна постројења путем „црва“ Стакснет (Stuxnet) 2010; севернокорејски напади 2009, 2011 и 2013. на Јужну Кореју; и руски напад на украјинску електричну мрежу 2015. године. То нам оставља мало материјала за детаљнију анализу. Једини могући начин на који тренутно можемо да испитамо природу сајбер ратовања је кроз упоређивање одређених параметара конвенционалног ратовања из последњег периода пре развоја сајбер оружја (условно речено хладноратовског) са карактеристикама познатих сајбер напада који су у медијима били окарактерисани као сајбер ратовање. Ти параметри су следећи: атрибуција, односно могућности идентификације нападача; сигнализирање и одвраћање; одрицање од прве употребе; и време трајања сукоба.

Атрибуција. Пружање „доказа“ да је једна држава покренула сајбер напад још увек је готово немогуће учинити са сигурношћу, па је и атрибуција, односно откривање починиоца сајбер напада, неретко компликован задатак. Нападач има на располагању много могућности да свој „траг“ на мрежи сакрије. Напади се обично врше преко мреже рачунара над којима је успостављена контрола путем вируса или црва, тзв. ботнет (botnet) мреже уређаја (зомби мрежа) који се углавном не налазе на територији нападача и који нису ни „свесни“ да у нападу учествују. Такође, државе још увек развијају капацитете за сајбер ратовање углавном у тајности и у релативној тајности и спроводе нападе на друге државе, тако да је тешко утврдити ко је нападач, осим ако сама држава не преузме

https://www.euractiv.com/section/digital/news/cyber-security-directive-held-up-in-face-of-wild-west-internet/ (приступљено 25. мај 2017.)

[13]Clarke & Knake, *Cyber War: The Next Threat to National Security and What to Do About It* 106

одговорност. До сада, већина држава за које се сумња да су извршиле сајбер нападе су порицале да су у њима и учествовале, и тек детаљно дигитално „форензичко“ испитивање може да пружи ограничене назнаке и углавном посредне доказе. На пример, приликом сајбер напада на Естонију априла 2007. године, цео контекст је сугерисао да је нападач била Русија. Наиме, фебруара исте године у Талину је избио спор између радикалних Естонаца и етничких Руса око очувања споменика совјетској армији у центру овог града, који је кулминирао крајем априла 2007. Споменик није срушен, већ је дислоциран, међутим спор је изазвао озбиљне тензије са Русијом, која није благонаклоно гледала на такву врсту ревизије прошлости. Током кулминације кризе, интернет странице стотине кључних институција, организација и јавних пружаоца услуга у Естонији – која је иначе једна од најумреженијих нација у Европи и свету – биле су преплављене захтевима за приступ у толикој мери да су поједини сервери престали са радом и угасили се, односно на њих је изведен тзв. ДДОС (Distributed Denial of Service) напад.[14] Утврђено је да је у нападу учествовало преко милион рачунара, што је био највећи ДДОС напад који је до тада виђен. Естонија је позвала у помоћ НАТО, чији су стручњаци покушали да утврде са киме „инфицирани рачунари“ комуницирају приликом напада. „Дигитална форензика“ је утврдила да се централни рачунар који је управљао ботнет мрежом налази у Русији и да је програмски код написан на „ћириличној тастатури“.[15] Иако је естонска Влада, већ на самом почетку јавно посумњала на Русију, и иако су стручњаци закључили да је епицентар напада у Русији, директних последица није било пошто „су политички лидери НАТО закључили да ови сајбер напади нису били акт рата“[16]. Москва је негирала умешаност у напад у Естонији, док су поједини званичници владе, након сазнања да су стручњаци утврдили да је напад дошао из Русије, признали да је могуће да су „патриотски настројени Руси, разјарени оним што је Естонија учинила, узели ствари у своје руке“. Већ ова епизода говори колико је тешко недвосмислено утврдити одговорност у случају сајбер напада. И свакако, услед изостанка атрибуције, одмазда ван сајбер сфере је практично немогућа, пошто је готово немогуће створити политичке услове да једна земља буде означена као кривац за одређени сајбер напад, а поготово за тумачење да је напад представљао случај сајбер ратовања.

Сигнализирање и одвраћање. Што се тиче сигнализирања и одвраћања, могућности држава су ограничене, услед неколико очигледних препрека за успешну примену ових приступа на начин на који је то било могуће са конвенционалним и нуклеарним оружјима током Хладног рата. Прва препрека је свакако та што се у већини случајева процес стварања капацитета за вођење рата у сајбер простору спроводи у тајности. Друга препрека је та да у случају сајбер напада не постоји свест о томе колико су такви напади потенцијално опасни, односно још увек не постоји

[14]Clarke & Knake, *Cyber War. The Next Threat to National Security and What to Do About It,* 14
[15]Ibid.
[16]Singer & Friedman, *Cybersecurity and Cyberwar. What everyone needs to know* 122-123. Међутим, директна последица је било стварање претходно споменутог „Талинског приручника“ и, како кажу аутори, Одељење за јавну дипломатију НАТО је о овом догађају направило кратки филм под називом „Рат у сајберпростору“

„демонстрациони ефекат“ као што је то било у случају нуклеарног оружја и употребе над Хирошимом и Нагасакијем.[17] Како грађани углавном нису свесни опасности које долазе из сајбер сфере, потенцијално је тешко употребљавати и сигнализирање и одвраћање, односно тешко је убедити их да би оваква врста конфликта „била скупа“.[18] Самим тим, свест јавности о ризицима и опасностима потенцијалних будућих сукоба у сајбер простору је ниска, па притисак јавности на доносиоце одлука, делом неопходан за успех тактике одвраћања, још увек изостаје. Трећа препрека је чињеница да сајбер оружја углавном могу да се искористе једанпут, односно да је противничка страна након првог напада једним сајбер оружјем углавном способна да развије одбране од тих оружја[19], надоградњом и ажурирањем сопствених система (и да их подели са другима). Стога, државе не желе да користе најсофистицираније и вероватно и најопаснија сајбер оружја која поседују, а која би им у случају пуног рата, уз конвенционална средства, могла потенцијално донети предност. Четврта препрека је да је у случају сајбер оружја тешко и предвидети ефекат које ће оно постићи у евентуалном сукобу (што је кључни аспект комуникације за сигнализацију и одвраћање) и то из два разлога. Први је свакако питање каквим дефанзивним односно офанзивним капацитетима држава која је потенцијална мета располаже, односно, да ли је довољно дефанзивно снажна да одбије или умањи снагу напада, и у којој мери њени офанзивни капацитети могу да нанесу штету нападачу током потенцијалног противудара. Развој капацитета у сајбер простору отвара и неслућене нове могућности за мале државе, као релативно јефтинији и лакше доступан извор релативне моћи у односу на конвенционалне врсте напада. Ово омогућава војно слабије развијеним државама да развију капацитете којима могу значајно да науде државама које су веће од њих. Због свега наведеног, напади у сајбер сфери су (још увек) углавном слабијег интензитета (и уколико су усмерени на државе, реч је пре свега о одмазди за политичке одлуке и потезе у физичком свету), док државе више припремају терен и „сеју“ оружја која могу потенцијално бити употребљена у случају „озбиљнијег сукоба“. Други разлог је у томе што одбрана једне државе не зависи само од стварања домаћих дефанзивних капацитета, већ и од „умрежености“ државе као такве. Другим речима, за разлику од конвенционалних оружја чији ефекат употребе може јасно да се предвиди, пошто углавном свуда делује једнако (док последице свакако зависе од одбране нападнутих и припремљености за напад), у случају сајбера постоји значајна разлика између држава у контексту примењивости сајбер напада на њу саму. Што је држава „умреженија“ то је већа могућност да ће сајбер напад деловати, и самим тим сигнализација и одвраћање имају смисла. Дакле, сајбер ратовање је као софистицирана грана ратовања најупотребљивије против држава које су у великој мери „умрежене“, односно где су кључни системи – како војни тако и цивилни – аутоматизовани и зависни од управљања преко мрежа. Према томе, сва је прилика да државе које имају највеће сајбер капацитете могу пре постати мете, иако је за очекивати да ће исте највише

[17]Clarke & Knake, *Cyber War. The Next Threat to National Security and What to Do About It* 92
[18]Segal, *The Hacked World Order: How nations fight, trade, maneuver and manipulate in the digital age* 29
[19] Clarke & Knake, *Cyber War. The Next Threat to National Security and What to Do About It* 94

и улагати у сајбер одбрану. Ограничена могућност коришћења сајбер ратовања , искључиво на „умреженим“ територијама, значајно лимитира и његову употребну вредност као потенцијално кључне или чак самодовољне гране ратовања. Самим тим и сигнализирање и одвраћање имају веома малу употребну вредност, осим када је реч од дефанзивним капацитетима.

Са тим у вези, у последње време је приметно да постоје и нови трендови када је реч о сигнализирању и одвраћању, те да представници држава, уместо да комуницирају о развијању конкретних сајбер оружја и последицама које она могу да нанесу, говоре пре свега о јачању дефанзивних сајбер способности. Како је навео заменик секретара за одбрану САД, Вилијем Лин III (William Lynn III) „одвраћање ће неизбежно морати да буде засновано више на ускраћивању било каквих добитака нападачима, него на наметању цене (за напад) кроз одмазду“[20].

Међутим, сајбер напади могу бити искоришћени да одврате противнике од активности у другим областима, ван сајбер сфере. Пример за то је претпостављени америчко-израелски напад 2010. године Стакснет „црвом“ на иранска постројења за обогаћивање уранијума који су тада готово уништени, а јасна порука Ирану да одустане од овог програма послата овим чином. Већ споменути руски напад на Естонију такође се може тумачити као врста одвраћања, али не од напада директно на Русију, већ од сукоба са етничким руским становништвом у Естонији. Овакви напади, уколико су успешни, могу да пошаљу јак сигнал којим ће се поједине државе одвратити од специфичних активности, али то је свакако прилично далеко од употребе стратегије сигнализације и одвраћања у случају сајбер ратовања.

Употреба оружја пре осталих. Коначно, оно што су сајбер напади донели је поновна реевалуација улоге држава као унитарних актера. Иако се међународне организације попут УН, ЕУ, НАТО и ОЕБС-а труде да креирају заједничке одговоре на изазове сајбер ратовања, саме државе све више развијају сопствене војне сајбер команде и улажу у стварање сопствених, независних, офанзивних сајбер способности. Овде је развој области и значаја сајбер сфере поновно преокренуо садашње приступе безбедности у правцу „свака држава искључиво делује за себе“. Уместо да разматрања неке врсте декларације „о одустајању од употребе оружја пре осталих“, као што смо видели, државе су фокусиране управо на овај први ударац у сајбер сфери, који може значајно да ослаби противника и неутралише системе који би у супротном могли бити употребљени у контра-нападу.

Временска димензија и сукоб. Што се тиче временске димензије сукоба, сајбер сукоби и сајбер ратовање се не могу сагледати у контексту класичних сукоба, где се може повући јасна граница између ратног стања, односнотрајања сукоба и мира. Сваки од горе побројаних напада је био само врхунац серије активности које су се највероватније одвијале далеко пре него што је сукоб почео, да би се коначна манифестација десила након

[20] Цитирано у Segal, *The Hacked World Order: How nations fight, trade, maneuver and manipulate in the digital age* 83

контекстуализације проблема. Односно, антиципирајући проблем у будућности, државе које су извршиле сајбер напад, вероватно су далеко пре „манифестационе фазе“ напада извршиле пенетрацију „непријатељског система“ и похраниле вирусе, црве или логичке бомбе. У моменту избијања кризе, односно у моменту употребе, ова средства су активирана, или је њихово дејство појачано до максимума, како би се дошло до жељеног ефекта. Стога сајбер ратовање заправо омогућава ситуацију у којој смо, како је рекао Џоел Бренер (Joel Brenner), бивши шеф контраобавештајног сектора у Сједињеним Америчким Државама, „(…) у константном сукобу између нација који ретко прелази у отворени рат (…) и морамо да се навикнемо да смо са неким државама, са којима сигурно нисмо у рату, попут Кине, у интензивном сајбер конфликту“[21]. Дакле, сукоби у сајбер простору се одвијају константно и у датом моменту немају нужно озбиљне негативне импликације на односе између држава. Њихова права сврха је (сем обавештајних активности и послова индустријске шпијунаже) стварање предуслова за моменат избијања конфликта, када би се област сајбера искористила као један од домена где би се сукоб одвијао и где постоји могућност да би једна страна добила кључну предност.

ХИБРИДНИ СУКОБИ И САЈБЕР РАТОВАЊЕ

Коришћење сајбер оружја је много видљивије и сврсисходније уколико се употребљава паралелно са другим кинетичким, односно конвенционалним, наоружањима. У овим случајевима напади у сајбер сфери користе се пре свега за онеспособљавање дела или целокупног одбрамбеног система и конвенционалне и сајбер одбране, сејањем пропаганде нападом (који може бити различите врсте) на интернет странице институција и медија, застрашивањем цивилног становништва путем уништавања или онеспособљавања критичне цивилне инфраструктуре итд. Тако је, на пример, израелски сајбер напад у Сирији 2007. искоришћен за онеспособљавање противваздушне одбране, услед чега ваздушни напад на постројења за која се сумњало да служе за развој нуклеарног наоружања који је уследио сутрадан није наишао ни на какав отпор. Штавише, био је у потпуности неочекиван.[22] Исто тако, руски напад 2008. током рата у Грузији, који је текао симултано са конвенционалним сукобом, учинио је много на сејању пропаганде и панике нападом на медије и на владине интернет странице. У оба примера, сајбер је био користан сегмент за једну од страна у сукобу, и довео је до жељеног исхода у оба случаја. Сама употреба је била релативно безболна, пошто ни једна ни друга влада, због текућег сукоба, нису имале потребу да прикривају своје акције. То значи да ће сајбер ратовање у сваком случају готово сигурно наставити да се манифестује кроз хибридне сукобе.

[21] Цитирано у Singer & Friedman, *Cybersecurity and Cyberwar. What everyone needs to know* 121

[22] Clarke & Knake, *Cyber War. The Next Threat to National Security and What to Do About It* 10

ЗАКЉУЧАК

Као што смо видели из текста, сукоби између држава који се искључиво одвијају у сајбер сфери се за сада одвијају паралелно са нормалним, свакодневним односима између држава. Карактеристика сајбера као паралелне димензије омогућава лимитиране сукобе у сајбер простору, наспрам истовремено неометане политичке и економске сарадње у физичком свету. Они не прерастају у рат, нити се суштински рачунају у такав, пошто је, и поред углавном оправдане сумње, врло тешко извршити атрибуцију. Сајбер оружја се углавном не користе за стратегије сигнализације и одвраћања, пре свега јер државе нису сигурне у сопствену снагу, нити у снагу противника у сајбер сфери, и што је најважније, ретко постоји свест грађана супарничких држава о могућим последицама сајбер напада, и колико озбиљне могу да буду. Међутим, јасно је да ће сајбер напади сигурно остати један од елемената надоградње конвенционалног ратовања, значајно га допуњујући и увећавајући његове ефекте, пре свега у односу на цивилно становништво, али само у одређеној мери. Другим речима, веома је мала вероватноћа да ће сајбер постати кључна или чак самостална грана ратовања у скоријој будућности, већ ће се пре свега користити као допунска снага у текућим сукобима. Ако се и десе напади, они ће пре свега бити демонстративног карактера (сигнализирање и одвраћање) за ограничене, индиректне циљеве.

Међутим, уколико се осврнемо, сајбер се као нови облик међународних сукоба појавио на сцени тек пре нешто више од две деценије, да би се 2007. године показао у пуном светлу. За тако кратак период постојања, овај потенцијални вид сукоба је више него исказао могућности да постане много озбиљнији полигон за ратове будућности него што је то данас.

ЛИТЕРАТУРА

1. Adams John, A. Jr. *Cyber Blackout: When the lights go out - Nation at Risk* (Friesen Press, 2015)
2. Clarke, Richard A. and Knake, Robert K. *Cyber War. The Next Threat to National Security and What to Do About It* (HarperCollins e books, 2010)
3. "Cyber security directive held up in face of "Wild West" Internet". Euractiv. https://www.euractiv.com/section/digital/news/cyber-security-directive-held-up-in-face-of-wild-west-internet/ (приступљено 25. мај 2017.)
4. Geers, Kenneth. *Sun Tzu and Cyber War* (NATO Cooperative Cyber Defence Centre of Excellence, 2011)
5. Iasiello, Emilio. Are Cyber Weapons Effective Military Tools? *Military and Strategic Affairs* 7 no.1 (2015)
6. Libicki, Martin C. Cyber War as a Confidence Game. *Strategic Studies Quarterly* no. 5 (2011)
7. Liff, Adam P. Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies* 35 no.3 (2012)
8. "New cyber reserve unit created". UK Ministry of Defence (2013). https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit (приступљено 25. мај 2017.)

9. Nye, Joseph S. Jr. Nuclear Lessons for Cybersecurity. *Strategic Studies Quarterly* 5 no.4 (2011)
10. Rid, Thomas. Cyberwar and Peace. *Foreign Affairs* 92 no.6 (2013)
11. Schmidt, Eric and Cohen, Jared. *The New Digital Age: Reshaping the future of people, nations and business* (John Murray Publishers, 2013)
12. Segal, Adam. *The Hacked World Order: How nations fight, trade, maneuver and manipulate in the digital age* (Public Affairs, 2016)
13. Singer, Peter and Friedman, Allan. *Cybersecurity and Cyberwar. What everyone needs to know* (Oxford University Press, 2014)
14. van Puyvelde, Damien. Hybrid war – does it even exist? NATO Review. http://www.nato.int/docu/review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/ (приступљено 14. март 2017.)

CYBER WARFARE: NEW TYPE OR WARFARE OR ADDITIONAL ELEMENT OF CONVENTIONAL WARFARE

Igor Novaković*
International and Security Affairs Centre – ISAC fund, Belgrade,
Republic of Serbia

Irina Rizmal*
Masters candidate at the University College of London,
Great Britain

Abstract: Cyber-attacks represent a new type of security threats, arising as a result of advancements in the field of information technologies, having the potential to change the dominant perception of conflicts. Since this threat is relatively new, and continues to evolve and change, it is difficult to foresee its future forms of development and potential manifestations of its use in conflicts. However, one should bear in mind that both the EU and NATO, as well as the USA, have already defined cyber space as a new military domain. The article discusses how conflicts are changing with the rise of this new domain, differing from conventional ones in both methods and means, and independent of norms of international law regarding the armed conflict/war. However, that does not mean that this new type of conflict is any less dangerous. Although belonging to the virtual sphere, cyber-attacks can leave considerable physical consequences. This article employs a comparative analysis of approaches to this topic, and then considers the perspectives of further developments in the cyber warfare, namely if there are possibilities for cyber to become a separate branch of war-waging, or, if it will remain only an additional element of conventional warfare, as it has already become with the advent of the so-called "hybrid warfare". This analysis represents a contribution to the discussion on the challenges of cyber in the future, providing a better insight into the potential challenges for our state in the present day and in the near future.

Key words: asymmetric threats, cyber space, cyber-attacks, cyber warfare, hybrid warfare

* igor.novakovic@isac-fund.org
* irina.rizmal@gmail.com