Ненад Путник

САЈБЕР РАТ И САЈБЕР МИР

Ненад Путник
САЈБЕР РАТ И САЈБЕР МИР

Издавачи

Универзитет у Београду –
Иновациони центар Факултета безбедности

Академска мисао

Рецензенти

др Зоран Драгишић, редовни професор
Универзитет у Београду – Факултет безбедности

др Радомир Милашиновић, редовни професор
Универзитет у Београду – Факултет безбедности

др Драган Симић, редовни професор
Универзитет у Београду – Факултет политичких наука

Припрема за штампу
Владица Миленковић

Штампа
Академска мисао, Београд

Тираж
200

ISBN 978-86-7466-920-4

Ненад Путник

САЈБЕР РАТ И САЈБЕР МИР

Универзитет у Београду –
Иновациони центар факултета безбедности
Академска мисао
Београд, 2022.

Садржај

Предговор

Средином 2007. године аутор ове књиге је на Факултету безбедности Универзитета у Београду пријавио магистарску тезу под насловом „Безбедносне претње у сајбер простору са посебним освртом на проблем сајбер тероризма". Наставно-научно веће је једногласно усвојило пројекат тезе. Па ипак, накнадно, у неформалним разговорима са појединим колегама, аутор је био у ситуацији да додатно појашњава о чему он то заиста жели да пише и да аргументује научну заснованост теме. Образложење је било утемељено на тврдњи да је тема мултидисциплинарна, да она осим информатичког има и друштвено-безбедносни аспект који се огледа у последицама које испољавање сајбер претњи оставља на безбедност индивидуалних корисника ИКТ система, корпорација, друштва и државе у целини, у физичком свету, те да је, према томе, усклађена са матичношћу факултета. На срећу, проф. др Радомир Милашиновић, ментор, предложене тезе је подржао, и без трунке сумње прихватио предложени пројекат, на чему му је аутор био, и остао, неизмерно захвалан.

Данас, петнаест година касније, околности су потпуно другачије. Нико више не доводи у питање ни значај, ни актуелност, ни научну етаблираност теме. Она се изучава на Факултету безбедности кроз различите наставне предмете, и различите аспекте, на свим нивоима студија, од додипломског кратког програма студија, преко основних академских и мастер, до докторских студија. Различити аспекти ове проблематике изучавају се и на другим високошколским и научно-образовним установама, што је свакако последица глобалног повећања врста и обима сајбер напада на рачунарске системе у протклих десенију и по.

Данас је свима, макар на нивоу основних информација или пак здраворазумског или барем интуитивног поимања, јасно шта су сајбер претње и шта би могла да представља сајбер безбедност. У протеклих петнаест година десио се велики број озбиљних сајбер напада са којима је и шира јавност упозната посредством медија. Естонија је 2007. године претрпела вишенедељни напад који је назван првим случајем сајбер рата. Годину дана касније уследио је сајбер рат против

Грузије. Недуго затим вирус Стакснет је умало довео до експлозије иранских нуклеарних постројења. Потом су уследиле информационе операције на Крим и Украјину у склопу такозваног хибридног рата. У јеку пандемије коронавируса 2020. године на мети криптовируса нашле су се здравствене установе широм света. Прошле године обележено је двадесет година од терористичког напада на Куле близнакиње, напада који је планиран на основу јавно доступних информација на интернету. Осим тога, данас већина земаља има своја доктринарна и стратешка документа из домена сајбер одбране, а процењује се да више десетина држава света има и офанзивне стратегије сајбер ратовања. Билатерални односи САД и НР Кине доведени су на историјски минимум због међусобних оптужби за сајбер шпијунажу, због чега се Хенри Кисинџер залаже за нови, сајбер детант. НР Кина и Руска Федерација промовишу концепт сајбер суверенитета. Председник Руске Федерације је донео закон о интернету којим су успостављена архитектонско-технолошка решења за „нови интернет" који ће бити заснован на другачијим протоколима и који ће Русији омогућити да у случају потребе „пресече" интернет конекције са „остатком света". Овим законом су физичка и правна лица обавезана да дигиталне податке складиште на серверима који се физички налазе на територији Руске Федерације. На састанку у Женеви, 26. јуна 2021. иза затворених врата, Путин и Бајден дефинисали су црвену линију која се не сме прећи – критичну инфраструктуру која не сме бити изложена сајбер нападима.

Намера аутора је да у овој монографији, на научно заснован начин, систематично, и у складу са епистемолошким принципима, студентима представи актуелну и сложену тематику из области широког спектра сукобљавања државних и недржавних актера у сајбер простору. Сукоби у сајбер простору се данас често и прилично слободно називају сајбер ратом.

Популарности овог израза доприносе медији који, жељни сензационализма, и у циљу повећања тиража или популарности, њиме именују различите облике сукоба у виртуелном простору – од криминала до конфронтирања држава. Такође, одређену „кривицу" сносе и секуритизујући актери – представници политичког естаблишмента али и академске јавности, који некритички и у складу са личним или општим националним опортунистичким циљевима промовишу одређене случајеве сајбер инцидената у претње националној безбедности. Оправданост употребе овог појма се може доводити у питање

и са позиција теоријске науке, будући да традиционално схваћен појам *рат* подразумева много ужи обухват и строго дефинисан садржај.

Па ипак, домети ове књиге не досежу толико далеко да она нуди коначне одговоре на питања обима и садржаја појма сајбер рат. Становиште аутора је да је употреба одређеног термина ствар језичке норме, односно договора и консензуса научника из области језика и предметне струке. Но, да би у догледној будућности дошло до терминолошког разграничења појма сајбер рат од појмова са сродним значењем (попут појмова сајбер агресија, сајбер шпијунажа, сајбер тероризам, сајбер хактивизам, сајбер криминал и слично) потребно је у првом кораку, и барем оквирно, утврдити на шта појам сајбер рат реферира или може да реферира. Исто тако, било би потребно утврдити и денотацију појмова са сродним значењем како не би долазило до њихове синонимне (зло)употребе. У том смислу, књига нуди основне терминолошке одреднице појмова *рат* и *сајбер рат*, као и покушај научне дескрипције и објашњења појава које се у савременој конфликтолошкој и безбедносној литератури подводе под овај појам. Њен допринос науци могао би се сагледати управо у покушају систематизације савремене и обимне научне и стручне мисли о актуелној појави сукобљавања у сајбер простору, као и могућностима за изналажење мира у глобалној арени у којој се сукобљавају интереси и вредности држава, војних савеза, мултинационалних корпорација, невладиних и активистичких организација, група и појединаца.

Структурну и, донекле, садржинску окосницу ове књиге представља докторска дисертација „Кибер ратовање – нови облик савремених друштвених конфликата". Но, она је узета само као полазна тачка и инспирација за један шири и потпунији приступ изучавању овог феномена, приступ који је подразумевао инкорпорирање и ажурирање најважнијих резултата и налаза ауторових истраживања у протеклих петнаест година. Резултати свих претходно објављених ауторских и коауторских истраживања који чине саставни део ове књиге јасно су назначени у циљу поштовања академске честитости.

У Београду,
14. марта 2022. године

Аутор

УВОД

Убрзани развој науке и технологије, нарочито у другој половини двадесетог века, достигао је такав темпо да су се нови технолошки и културни обрасци смењивали не више на сваки век или пола века, већ сваке деценије, а пред крај те епохе и чешће. Тешко је пронаћи адекватан заједнички атрибут за претходно столеће. У различитој публицистичкој, али и научној литератури оно је називано атомским веком, веком светских ратова, веком глобалне културе и економије, медијâ, прва свемирска ера, епоха мултиполаризма итд.

Двадесети век се сматра веком ратова јер су, у овој епохи, страдања достигла размере веће него икада раније. Процењује се да је број жртава у минулом веку био четири пута већи од броја жртава у претходна четири века. Оружане конфликте у 20. веку обележило је проширење мета на цивилне објекте и, посебно, увећање броја цивилних жртава. Број цивилних жртава у односу на војне жртве потпуно је преокренут, што је навело поједине теоретичаре на закључак да је у савременим ратовима најбезбедније бити припадник војске.

У свим досадашњим сукобима техничко-технолошки фактор је имао значајну улогу. Технолошка надмоћ значила је, у највећем броју случајева, и победу у рату. Ни данас није другачије. Тежње за освајањем нових технологија у циљу израде што деструктивнијег оружја не само да су опстале, већ су се и увећале. Може се рећи да је знање, као предуслов технолошког развоја, постало примарни и доминантни ресурс, неопходан за победу у сукобу. Технолошка креативност, дакле, није елиминисала опасности од конфликата већ их је, напротив, увећала.

Са социолошког аспекта посебно је значајан развој информационе и комуникационе технологије након Другог светског рата, јер је довео до важних промена у начину организовања и функционисања друштва. Настанак комуникационих инструмената, попут телевизије, првих генерација рачунара и сателита, не само да је повећао брзину и могућности за размену информација, већ је утицао и на промене у свим сферама друштвених активности. Настанак персоналних

рачунара и стварање, прво, технолошки неусавршених локалних рачунарских мрежа, а затим и „глобалне мреже" – интернета – утицали су на културну, економску и политичку сферу друштвеног живота скоро свих технолошки напреднијих држава света.

Ни са војног и безбедносног аспекта наведене промене нису од мањег значаја. Савремене оружане снаге се у својим активностима изузетно много ослањају на најновија технолошка достигнућа на пољу информационо-комуникационих технологија. Информациона револуција је значајно трансформисала начин на који се воде ратови у информационом добу. Она је изазвала промене, не само у начину на који оружане снаге воде оружани сукоб (у смислу борбене технике, средстава и тактике) већ и у начину на који друштва долазе у конфликт, у начину на који се „препарира јавно мњење" и задобија домаћа и међународна подршка за агресију.

Осим наведених улога, информационо-комуникациона технологија је почела да се злоупотребљава и на један специфичан начин. Интернет је промовисан у ново бојно поље, а рачунари и рачунарске мреже су попримили улоге средстава за извршење напада и самих мета напада. Информатичко ратовање је постало нови, све заступљенији облик друштвених сукоба, који се због специфичних карактеристика битно разликује од досадашњих врста ратовања. Оно се води истим средствима, методама и техникама као и сајбер криминал, сајбер обавештајне активности и сајбер тероризам. У њему учествују оружане снаге, друштвене групе, корпорације али и индивидуални корисници рачунарских технологија. Из наведених разлога, научна и стручна јавност још увек није постигла сагласност по питању дефиниције овог специјалног вида ратовања.

Експанзија информатичког ратовања почиње у последњој деценији 20. века са развојем савремених информационо-комуникационих технологија или, прецизније речено, са пуштањем интернета у комерцијалну употребу. Основна специфичност ових активности јесте да бојиште није физички, већ виртуелни свет. Информатичко ратовање се, према томе, може дефинисати као подврста информационог ратовања, којој није потребно традиционално бојно поље, већ се одвија у сајбер простору. На сајбер простор може утицати било која група која поседује рачунаре и приступ интернету. Сајбер напади могу бити усмерени на намерно убацивање дезинформација на одређене интернет платформе или могу бити усмерени на саботажу рачунарских мрежа и система. Онемогућавање нормалног функцио-

нисања информационих система, у савременом друштву које је постало од њих зависно, може имати врло озбиљне последице на све сфере друштвеног живота. Последице могу бити чак и фаталне уколико се угрозе критичне информационе инфраструктуре као што су системи за контролу копненог и ваздушног саобраћаја, хидро-брана, нуклеарних електрана, безбедносних и здравствених служби или, пак, системи за дистрибуцију електричне енергије. Арсенал сајбер напада (оружје које се користи за изазивање дисфункције информационе инфраструктуре) веома је разноврстан и специфичан – он подразумева примену различитих информатичких инструмената, програма, и техника. Предуслов за извођење сајбер напада је, дакле, поседовање информатичког знања.

Modus operandi информатичког ратовања, према томе, проширен је у односу на конвенционално информационо ратовање низом активности, усмерених на софтверско угрожавање информационе инфраструктуре, док је пропагандни аспект информационог ратовања попримио форму злоупотребе интернета као средства масовне комуникације. Сајбер простор, „виртуелни свет", на тај је начин постао не само циљ напада већ и моћно средство у рукама високообразованих „информатичких ратника". У прилог овој тези можемо навести и чињеницу да је у савременим војним доктринама сајбер простор стекао статус петог борбеног простора, заједно са копном, водом, ваздухом и космосом. Све више аутора сматра да је „инфосфера" простор где би се могле водити примарне борбе у будућности, а поједине државе се увелико припремају за такав концепт вођења ратова.

У битно обележје информатичког ратовања можемо још сврстати и тенденцију његовог померања изван војних граница на индивидуалну, друштвену и комерцијалну раван. Док је некаашње појмовно одређење информационог ратовања истицало његову војну димензију, добар део савремене литературе истиче аспект његовог проширења ван војних области. Проширење делокруга информационог ратовања изван војних активности је, у техничком смислу, омогућено дифузном и децентрализованом структуром глобалне рачунарске мреже – интернета. Суштински, феномен сукобљавања у сајбер простору помоћу оружја које нуди сам сајбер простор, и његово преливање у сфере „цивилног" света узроковано је противречном природом процеса глобализације и идеолошким, политичким, културним и социјалним диспаритетима које овај процес носи.

Информационо-комуникационе технологије на глобалном нивоу увећавају улогу држава, организација, мултинационалних компанија, невладиних организација, транснационалних криминалних организација и, чак, појединаца у међународној арени. Савремене технологије омогућавају ширење информације али и дезинформације, фаворизују културну и економску интеграцију (или дезинтеграцију) и дају видљивост и хитност догађајима, где год да се они дешавају у „глобалном селу". Природа сајбер простора је таква да се токови информација могу тешко ограничити и контролисати. Може се рећи да сајбер простор не познаје политичке и географске границе – две тачке су увек близу без обзира на дистанцу која их раздваја. То са једне стране узрокује интензивирање односа између међународних актера, а са друге, лаку дистрибуцију нежељених информација. Из тог разлога неке владе су, чак, одлучиле да усвоје рестриктивне политике или да својим грађанима онемогуће приступ интернету.

Државе које се ослањају на информационе технологије изложеније су и рањивије на било који облик штетне преправке, прекида или уништења технологија од којих зависе информациони токови као што су, на пример, индустријска друштва рањивија од аграрних друштава по питању континуираног снабдевања енергијом.

Безбедносне претње у савременим околностима су, дакле, асиметричне. Земље са нижим нивоом зависности од нових технологија не само да су мање рањиве, већ могу да искористе рањивост развијенијих земаља за достизање својих стратешких циљева. Могућност извршавања деструктивних акција је, са економске тачке гледишта, све доступнија. Развијање офанзивних стратегија сукобљавања у сајбер простору не захтева високе инвестиције, попут оних неопходних за конвенционално ратовање и, изнад свега, ове стратегије доступне су великом броју актера. За разлику од технолошки софистицираног оружја, сајбер оружје могу развијати појединци или групе за шта су им једино потребни знање и мотивација. То омогућава државама или актерима којима до сада није придаван значај у стратешком контексту, да теже другачијој позицији у сајбер простору, где знање одређује равнотежу моћи пре него количина војног арсенала.

Осим тога, у сајбер простору је мање изражена веза између безбедности и територије. Геополитичка позиција која је одувек била централни, средишњи, елемент безбедносне политике државе постепено губи свој значај. Данас није више неопходно физичкиући у

неку територију, нити је напасти кинетичким оружјем. Дакле, комплетна контрола физичких ентитета као што су ваздушни или копнени простор није довољна да гарантује безбедност једној држави. Војна надмоћ не значи безусловно и сигурност у сајбер простору где је неопходно развити нове стратегије одбране критичне информационе инфраструктуре.

Претња сајбер нападом није лако уочљива нити се актери претње могу лако категоризовати. Првенствено, не постоји јасна идентификација актера – сваки члан „електронске друштвене заједнице" је потенцијални противник. Непријатељске државе, војни савези, терористи, незадовољни радници, обесни појединци, комерцијална или индустријска предузећа, политички активисти и криминалне организације само су примери могућих актера. Сваки од ових актера мотивисан је различитим циљевима, ограничен различитим нивоима ресурса, сопственим могућностима и могућностима система да се брани. Тешко је пронаћи евидентне доказе у вези са непријатељским намерама могућих нападача и проценити њихове реалне способности да изведу напад на тако широком нивоу да угрозе безбедност државе.

Различити видови конфронтације у сајбер простору промовисали су феномен такозваног сајбер ратовања у друштвено питање. Појам сајбер ратовање се, у актуелним научним тематизацијама ове појаве, употребљава као збирни термин за описивање широког распона активности на индивидуалном, друштвено-социјеталном, корпоративно-економском и војном нивоу. Под ове активности могу се сврстати, на пример, хактивизам (Hactivism), фишинг (Phishing), покретање напада усмерених на дистрибуирану опструкцију услуга (Distributed denial of service – DDoS) као и развијање војних дефанзивних и офанзивних оперативних способности.

Употреба израза сајбер ратовање за описивање савремених сукоба у сајбер простору може се чинити непримереном у односу на традиционално поимање рата као организованог, интензивног конфликта између држава, савеза држава, етничких и верских група или класа средствима оружаног насиља у циљу остваривања одређене политичке, војне и друге добити. Тешко је говорити о стварном рату уколико такве операције немају конкретне последице у смислу физичке штете или губитка људских живота.

Међутим, ризик од ескалације ове врсте конфликта се увећава те га не би требало потцењивати. На ову чињеницу прво су указали

DDoS напади na Естонију 2007. године, а затим и Грузију 2008. године. Након тога, сајбер напади су постали пратилац свих традиционалних сукоба који се воде широм планете.

Из историјске перспективе посматрано, преокрет у перцепцији сајбер претњи наступио је оног тренутка када су рачунарски напади почели да погађају SCADA системе који су „срца" критичне инфраструктуре, и друге системе специјане намене (као што су системи за контролу процеса у нуклеарним реакторима – случај напада на Иран малициозним кодом Стакснет).

Сајбер ратовање је стога, у дословном значењу термина, постало реалност. Процењује се да више десетина држава света развија капацитете за овај вид сукобљавања, као и Северноатланска алијанса. Многе државе и војни савези данас имају разрађене војне доктрине и стратегије сајбер ратовања.

Реално сагледавање феномена сајбер ратовања отежано је ограниченим приступом информацијама – истраживачи се могу ослонити само на јавно доступне изворе, али и „сликом" коју стварају медији. У медијском етру расправа о овим питањима поприма алармантан и сензационалистички тон. Уопштено, можемо констатовати да се концепту сајбер рата у водећим Западним мас-медијима, али све чешће и код нас, придаје врло велики значај и када је реч о онима који га афирмишу и када се говори о онима који су жртве. Реторичка драматизација удружена са секуритизацијом се често користи и даје општи утисак да претња сајбер ратом постаје све већа и опаснија.

Проблем несигурности сајбер простора постао је, почетком 21. века, једна од важних тема научне, стручне али и шире јавности у свим технолошки развијеним земљама. У прилог овој тврдњи говоре све учесталије научне тематизације овог проблема, али и спроведене законодавне реформе у одређеним земљама, затим семинари, пројекти и скупови на националном и међународном нивоу, као и бројне јавне дебате о потреби редефинисања стратегија за заштиту сајбер простора. На основу претходно реченог може се констатовати да је претња сајбер ратом веома актуелан друштвени проблем који захтева свестрану научну анализу.

С обзиром на уочену фрагментарност досадашњих истраживања, недовољну развијеност теоријског оквира и непостојање јасно дефинисаних основних појмова, у спроведеном истраживању смо се усредсредили на исцрпну дескрипцију и класификацију манифестних облика овог феномена са аспекта безбедносних наука у циљу

синтетизовања полазне грађе за будуће теоријске и емпиријске радове који ће се бавити овом тематиком.

На основу прегледа научне и стручне литературе (од 1990. до 2022. године), могу се уочити одређене, битне, тенденције сукобљавања у сајбер простору. Стога се предмет спроведеног истраживања може одредити као идентификација, дескрипција и класификација савремених облика сукобљавања у сајбер простору и анализа могућности за постизање трајнијег мира.

Предмет истраживања, са временског аспекта, обухвата период од настанка глобално умреженог друштва до данас. За почетак глобалног умрежавања узима се 1994. година када је World Wide Web претворио интернет у инструмент масовне комуникације.

Предмет истраживања тематски припада већем броју научних дисциплина. Он обухвата сазнања и проблеме социологије, наука безбедности, информационих и математичких наука и њихових посебних дисциплина (као што су криптографија и криптоанализа), војних, правних, криминалистичких и криминолошких наука, што несумњиво упућује на његов интердисциплинарни карактер.

Научни циљ спроведеног истраживања био је научно објашњење феномена сајбер ратовања. Научно објашњење ове актуелне друштвене појаве подразумевало је систематизацију досадашњих сазнања о сукобима у сајбер простору што је претпостављало сагледавање, дескрипцију и исцрпну класификацију различитих облика сукобљавања у виртуелном простору.

Надамо се да ће спроведена анализа допринети разјашњењу појмовног и терминолошког корпуса ове специфичне области, као и да ће на практичном нивоу резултати истраживања допринети бољем разумевању ове проблематике, што је од великог значаја за развијање стратегија превенције, сузбијања и управљања безбедносним ризицима у сајбер простору не само на националном већ и корпоративном нивоу.

Брз улазак „информационих конфликата" унутар цивилних и корпоративних оквира, тј. експанзија сајбер ратовања у комерцијални свет, представља озбиљан проблем лицима одговорним за заштиту и безбедност националне и корпоративне информационе инфраструктуре. Стога се подизање нивоа безбедносне културе и свести о последицама које сајбер напади могу произвести у физичком свету мора схватити као императив информационог доба. Ова студија је покушај доприноса том циљу.