САЈБЕР ПРОСТОР КАО ПОДРУЧЈЕ СУКОБЉАВАЊА: СЛУЧАЈ САД – ИРАН И СЕВЕРНА КОРЕЈА*

Дејан В. Вулетић**
Милош Р. Миленковић***
Анђелија Р. Ђукић****

Достављен: 03. 12. 2020.
Кориговано: 19. 01, 08. 02. и 05. 03. 2021.
Прихваћен: 19. 03. 2021.
Језик рада: Српски
Тип рада: Прегледни рад
DOI број: 10.5937/vojdelo2101001V

Последњих година сајбер простор све чешће представља подручје сукобљавања водећих светских и регионалних сила. У раду је приказан његов значај и укратко је описан нови концепт заједничког ратовања Сједињених Америчких Држава. Разматрани су одређени догађаји и активности у сајбер простору, у последњих неколико година, између САД са једне, односно Ирана и Северне Кореје са друге стране.

Наведени предмет истраживања је у директној вези са циљем рада који је усмерен на указивање и објашњење облика и карактеристика напада, као и одређених актера сукобљавања у сајбер простору. Основна хипотеза јесте да сајбер простор представља подручје сукобљавања светских и регионалних сила у коме оне често користе недржавне актере као посреднике, уз непрекидно усавршавање техника и метода извођења напада.

Поред општих научних метода, с обзиром на предмет и циљ истраживања, тежишно су коришћене компаративна метода којом су анализиране и упоређиване сличности и разлике реализације напада на информациону инфраструктуру страна у сукобу, као и метода анализе садржаја, имајући у виду да су као извори сазнања коришћени званични и референтни експертски извештаји, научни радови и друге публикације.

* Чланак је резултат рада на научноистраживачком пројекту „Физиономија савремених оружаних сукоба" који се реализује на основу Плана научноистраживачке делатности у МО и ВС за 2021. годину, број 2-2.

** Универзитет одбране у Београду, Институт за стратегијска истраживања, Београд, dejan.vuletic@mod.gov.rs

*** Универзитет одбране у Београду, Институт за стратегијска истраживања, Београд.

**** Универзитет одбране у Београду, Институт за стратегијска истраживања, Београд.

На основу изнете аргументације у раду, може се закључити да су инциденти у сајбер простору између САД и Ирана, односно Северне Кореје, бројни, често дуго припремани, уз активно учешће недржавних актера.

Кључне речи: *сајбер простор, сукобљавање, САД, Иран, Северна Кореја*

Увод

Већина држава има суштинске ресурсе засноване на информационо-комуникационој технологији, укључујући одрамбене системе, системе државне управе, комплексне управљачке системе и информационе инфраструктуре које обухватају контролу електричне енергије, телефонског система, токове новца, ваздушног саобраћаја, токова нафте и гаса, као и друге информационо зависне области. Друштво постаје све више зависно од информационо-комуникационе технологије,[1] што резултира његовом већом осетљивошћу, како због повећаног броја корисника, тако и због тренда међусобног повезивања рачунарских мрежа.[2] С тим у вези, заштита информационих инфраструктура намеће се као један од приоритета националне безбедности.[3]

Као резултат друштвених потреба и технолошких иновација настао је сајбер простор – нематеријални, неограничени интерактивни простор креиран од рачунарских мрежа.[4] У суштини, он представља глобално повезану информационо-комуникациону инфраструктуру.[5]

Непријатељи, било државе, групе или појединци, покушавају да угрозе критичне информационе инфраструктуре коришћењем нетрадиционалних метода. Управо такви напади могли би значајно угрозити како војну тако и економску моћ нападнуте државе. Геополитичке несугласице преливају се и у сајбер простор.[6] Државе су ангажоване на све већем надметању у сајбер простору „на нивоу испод оружаног сукоба".[7]

---

[1] Анђелија Ђукић, „Крађа идентитета – облици, карактеристике и распрострањеност", *Војно дело*, Министарство одбране РС – Медија центар „Одбрана", Београд, број 3, 2017, стр. 99.

[2] Дејан Вулетић, *Одбрана од претњи у сајбер простору*, Институт за стратегијска истраживања, Београд, 2011, стр. 5.

[3] Helen Nissenbaum, "Where computer security meets national security", *Ethics and Information Technology*, vol. 7, no. 2, 2005, p. 63.

[4] Дејан Вулетић, *Безбедност у сајбер простору*, Министарство одбране РС – Медија центар „Одбрана", Београд, 2012, стр. 21-23.

[5] Дејан Вулетић, „Употреба сајбер простора у контексту хибридног ратовања", *Војно дело*, Министарство одбране РС – Медија центар „Одбрана", број 7, 2017, стр. 310.

[6] Дејан Вулетић, „Психолошка димензија хибридног ратовања", *Војно дело*, Министарство одбране РС – Медија центар „Одбрана", број 6, 2018, стр. 274.

[7] Nigel Inkster, *It's time to stabilise cyberspace – our well-being depends on it*, International Institute for Strategic Studies, Washington, 2019, p. 1.

Концепт операција у више домена

Америчка војска у ери убрзаног људског напретка налази се у ситуацији у којој различити повезани елементи оперативног окружења конвергирају, стварајући ситуацију где трендови у дипломатској, информационој, војној и економској сфери брзо трансформишу природу свих аспеката друштва, укључујући и карактер ратовања. Амерички стратези процењују да је смањена тренутна америчка компаративна војна предност и способност извођења операције против софистицираног непријатеља.

Потенцијални противници, пре свих Русија и Кина, али и Иран и Северна Кореја, предузели су бројне кораке да поремете ефикасност америчке војне моћи, што ствара неповољнију ситуацију за САД. Раст ваздухопловних, копнених и поморских способности потенцијалних противника са развијеним ударним способностима у свемиру и сајбер простору омогућавају им да се боре против америчких снага у областима у којима се већ дуго претпоставља доминација САД.[8] Посебно може бити угрожено ослањање САД на сајбер простор у процесу командовања и контроле заједничких ваздушних операција, имајући у виду чињеницу да главни противници улажу велике напоре за унапређење својих способности у том домену.

Заједничка визија 2020. (*Joint Vision 2020*) позива на доминацију пуног спектра, при чему би америчке снаге морале да воде брзе и синхронизоване операције са комбинацијама снага прилагођених специфичним ситуацијама, приступом и слободом да делују у свим доменима (копно, море, ваздушни простор, свемир и сајбер простор). Као кључни фактор доминације наглашава се способност постизања супериорности у свим доменима.[9]

Секретар одбране САД Марк Еспер (*Mark Esper*) наредио је, крајем 2019. године, одговорним службама и Заједничком штабу (*Joint Staff*) да до краја 2020. године припреме нови концепт заједничког ратовања (*Joint Warfighting Concept*) за операције у свим доменима (областима, просторима). Тај концепт треба да опише способности и атрибуте неопходне за деловање у будућности, у свим доменима, при чему се усмерава и развој Министарства одбране у наредним деценијама.

Генерал Џон Хитен (*John Hyten*), заменик начелника Здруженог штаба, током предавања 12. августа 2020. године, које је организовао Институт Худсон (*Hudson Institute*), а пренео магазин Дифенс Њуз (*DefenseNews*), говорио је о новом концепту, наглашавајући да ће највећа разлика бити у томе што у будућности неће бити линија на бојном пољу.[10]

---

[8] Према подацима Већа САД за спољне односе (*US Council for Foreign Relations*) и Центра за стратегијске и међународне студије (*Center for Strategic and International Studies – CSIS*) идентификовано је преко 250 сајбер напада на САД спонзорисаних од стране неке државе у периоду од 2005. до 2018. године. Eneken Tikk, *Cyber arms control and resilience*, SIPRI Yearbook - Armaments, Disarmament and International Security, Oxford University Press, 2019.

[9] "Joint Vision 2020", https://apps.dtic.mil/dtic/tr/fulltext/u2/a526044.pdf, 14/11/2020

[10] Hudson Institute, General John E. Hyten on Progress and Challenges Implementing the National Defense Strategy, https://www.hudson.org/events/1853-video-event-general-john-e-hyten-on-progress-and-challenges-implementing-the-national-defense-strategy82020, 16/11/2020

Убрзани, пре свега технолошки развој захтева и нове концепте, па се и сама терминологија убрзано развијала последњих година – од вишедоменске (вишедимензионалне) битке преко вишедоменске (вишедимензионалне) операције до операције у свим доменима (*Multi-Domain Battle; Multi-Domain Operations; All-Domain Operations*).

Концепт операције у више домена у основи објашњава како ће америчке снаге одвратити и победити противника у ситуацији „испод нивоа оружаног сукоба", као и у самом оружаном сукобу. Тај концепт омогућава америчким снагама да физички, виртуелно и когнитивно надјачају противнике, примењујући комбиновано оружје у свим доменима. Наводи и препоруке у вези са способностима које су потребне командантима за победу напредног непријатеља и предлаже нови оквир за боље разумевање борбеног простора 21. века. Операција у више домена неопходна је америчким снагама, заједно са савезницима и другим партнерима, како би се противници успешно одвратили и победили у будућим сукобима.

Амерички стратези процењују да се мора извршити боља интеграција свих снага како би војска САД задржала надмоћ у способностима у односу на напредне технологије и концепте непријатеља. Према процени експерата, тренутни систем не интегрише довољно све домене, као што је нпр. технолошка интеграција. Уочене су и одређене слабости у систему командовања и управљања у реалном времену.

Концепт америчке војске у вишедоменским операцијама 2028. (*The U.S. Army in Multi-Domain Operations 2028*)[11], који је израдила Команда за обуку и доктрину (*Training and Doctrine Command – TRADOC*) 2018. године, предлаже низ решења за сукобе у различитим доменима. Основна идеја је брза и континуирана интеграција свих домена ратовања како би се противник одвратио и остварила предност у оружаном сукобу. Уколико одвраћање не би успело, војне формације, као део Здружених снага, продрле би и дезинтегрисале непријатељеве системе, користиле слободу маневра проистеклу из такве ситуације, постигле сопствене стратегијске циљеве и консолидовале добит како би се противник присилио да се врати у стање повољније за Сједињене Државе, њихове савезнике и партнере.

Значај сајбер простора за САД

Формирање америчке Сајбер команде 2009. године и добијање статуса самосталне оперативне команде у мају 2018. године (до тада је била део Стратегијске команде), говори о значају сајбер простора за Пентагон. На много начина, издвајање америчке сајбер команде из Стратегијске команде, која надгледа стратешко одвраћање, симбол је промене америчког држања у сајбер простору

[11] The U.S. Army in Multi-Domain Operations 2028, TRADOC, Virginia, 2018, https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf, 22/11/2020

од „одбране" ка „упорном ангажовању". Сједињене Државе, као још увек најистакнутија сајбер сила у свету, исказују амбиције да изврше сајбер операције на свим нивоима командовања. Сајбер команда САД има капацитете од неколико хиљада припадника који се могу ангажовати за планирање и реализацију напада. Средином 2018. године, усвојено је правило *Joint Publication 3-12 Cyberspace Operations* које регулише процену, припрему, планирање и извршавање сајбер операција.[12]

Сајбер команда представља свој циљ да САД морају унапред да се бране што ближе извору непријатељевих активности и актера пре него што они остваре тактичке, оперативне и стратегијске предности. То уверење је појачано у Националној стратегији за сајбер простор, објављеној у септембру 2018. године.[13] У њој се наводи да је циљ идентификација, супротстављање, ремећење, деградирање и одвраћање понашања у сајбер простору које је дестабилизирајуће и противно националним интересима САД, односно остваривање доминације и надмоћности САД у сајбер простору. Ако се у потпуности имплементира, стратегија би подразумевала предузимање акција против одређених актера у сајбер простору, што је био случај против Ирана због, наводног, обарања америчке беспилотне летелице.

У стратегијским документима САД посебно се наглашава право на контрамере и самоодбрану у случају сајбер напада. У ранијем периоду амерички став према сајбер простору био је дефанзивнији и усмерен, пре свега, на одвраћање потенцијалних нападача. Сједињене Државе су сматрале да би перцепција његових офанзивних способности могла одвратити противнике од напада. Концепт стратегијског одвраћања у сајбер простору се није показао као ефикасан у пракси. Ометање и узнемиравање главних конкурената у сајбер простору, за разлику од одвраћања, постали су привлачнија опција за америчке стратеге.

У августу 2018. године амерички председник Доналд Трамп (*Donald Trump*) издао је наређење (*PPD-20*) којим се поништава политика претходног америчког председника Барака Обаме (*Barack Obama*) којом је успостављена компликована процедура за међуресорни процес који се мора испоштовати пре него што би САД могле да покрену сајбер напад.

Иако амерички противници сматрају да би у случају сајбер напада на САД то довело до одговора уз познавање потешкоћа приписивања тих напада одређеним државним актерима, све чешће ангажују недржавне актере да изврше офанзиве акције против САД и њихових савезника.

Како би предупредиле могуће сајбер нападе САД све чешће подижу оптужнице против појединаца из Кине, Ирана, Северне Кореје и Русије. Процењује се да се одређени број осумњичених никада неће суочити са изручењем и кри-

[12] Joint Publication 3-12, Cyberspace operations, 8 June 2018, Joint Chiefs of Staff, Washington, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf, 20/10/2020

[13] National Cyber Strategy of the United States of America, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf, 17/10/2020

вичним гоњењем, али јавно обелодањивање њихових имена може утицати на промену одлука и одвраћање других потенцијалних нападача. Такође, САД настоје да предузимају економске санкције против појединца и организација. Више држава, укључујући и САД, објављују податке о својим сајбер способностима и спремности да их користе за националну одбрану.[14]

Однос Сједињених Држава и Ирана

Карнегијева фондација за међународни мир (*Carnegie Endowment for International Peace*) објавила је, 4. јануара 2018. године, извештај у којем је Иран означен као извор претњи у сајбер простору. Аутори наводе да су, упркос успеху Ирана везано за малвер *Shamoon*[15] и фишинг напад на компанију *Deloitte* и неколико других корпорација, ирански напади углавном лоше скривени. Као резултат тога, експерти који су се бавили истрагом догађаја нису имали много проблема да открију починиоце. Докази су указивали да су извршиоци из Ирана, како због *IP* адреса[16] тако и због појмова из персијског језика који су били садржани у малициозним програмима. Процењује се да су способности Ирана релативно мале у поређењу са Русијом и Кином, али свакако представљају претњу по САД.[17]

Поједини експерти сматрају да ће са развојем сајбер напада као асиметричног оружја, државе бити све више укључене. Продаја одређеног конвенционалног наоружања Ирану и Сирији указује и на могућност снабдевања и обуке када су у питању сајбер алати. Према одређеним изворима, САД и Израел су већ имали такву сарадњу која се односила на малициозни програм *Stuxnet*[18] који је ослабио иранске капацитете за обогаћивање уранијума, 2010. године.[19] Таква врста помоћи и трансфер знања дешавали су се у прошлости, пре свега у области развоја нуклеарног наоружања.[20]

---

[14] The Military Balance, Volume 119, Issue , 2019, Washington, p.8, https://www.tandfonline.com/toc/tmib20/119/1?nav=tocList

[15] Малициозни програм *Shamoon (W32.DistTrack)*, открили су, у августу 2012. године, компаније Kaspersky, Simantec и Seculert. Карактерише га, у односу на остале злонамерне програме, велика деструктивност и неопходност великих трошкова и времена опоравка циљаног система.

[16] IP адреса (*Internet Protocol address)* јединствени је тридесетдвобитни број који користе различити уређаји у међусобном комуницирању путем интернета, уз коришћење одређених протокола.

[17] Scott Stewart, "Hacking: Another Weapon in the Asymmetrical Arsenal", *Stratfor - Worldview*, January 25 2018, p.1-3, worldview.stratfor.com

[18] Stuxnet је малициозни рачунарски програм, откривен 2010. године, којим је угрожен ирански нуклеарни програм, а за који се сумња да су га израдили САД и Израел.

[19] Scott Stewart, op.cit.

[20] Ибид.

Сајбер напади неће заменити тероризам као асиметрично оружје. Многе карактеристике које чине тероризам атрактивним за извршиоце, такође се односе и на сајбер нападе. До сада изведени сајбер напади, потпомогнути одређеним државама, нису пропраћени одговарајућом негативном реакцијом, откривањем и процесуирањем починилаца. Ниски трошкови, време и напор за реализацију, несумњиво ће подстаћи више држава да се определи за ту врсту напада.[21]

Као што је мала је вероватноћа да ће Иран изазвати САД у војном сукобу великих размера, тако је и мало вероватно да ће водити директан рат у сајбер простору. Поређење сложености малициозних програма *Stuxnet* (везује се за САД и Израел) и *Shamoon* (везује се за Иран) илуструје разлику у способностима. Без обзира на ту чињеницу, САД су рањиве на сајбер нападе. Упркос тој реалности, обе стране ће наставити да се припремају за сајбер рат. Иран, као и друге државе (Кина, Русија, Северна Кореја...), и одређени недржавни актери, реализују надзор над критичном инфраструктуром САД и Запада већ дужи низ година. Такође, Американци и њихови савезници су ангажовани на извиђању иранске инфраструктуре. На Аспенском сигурносном форуму (*Aspen Security Forum*), у јулу 2018. године, директор Националне обавештајне службе САД Ден Коутс (*Dan Coats)* напоменуо је да се Иран припрема за циљање електричних мрежа, водених брана и технолошких компанија у САД, Европи и на Блиском истоку.[22]

Надзор не значи да ће се напад сигурно догодити. Као и сваки ратни план, сајбер планови се ажурирају како би се узеле у обзир промене оперативних система, рањивости, сигурносних и других мера. Наведеним активностима бави се и Иран, односно милитантне групе Хезболаха с којима сарађују. Док је сајбер рат и даље мало вероватан, ирански напади нижег нивоа против владиних институција САД, приватних компанија и организација, вероватно ће бити учесталији. Крајем 2018. године, представници италијанске компаније за нафтне услуге *Saipem* изјавили су да су угрожени сајбер нападом, односно малициозним програмом који представља варијанту малвера *Shamoon*, што указује да су починиоци вероватно из Ирана. Највећи клијент компаније *Saipem* је национална нафтна компанија *Saudi Arabian Oil Co.*, конкурентска фирма иранској, што је вероватно био разлог за напад на италијанску фирму. Поред тога, лондонска фирма *Certfa*, која је специјализована за праћење иранске активности у сајбер простору, објавила је извештај који указује на фишинг нападе Ирана усмерене на финансијску инфраструктуру САД. Напади су усмерени и према Организацији за светску међубанкарску финансијску телекомуникацију (*Society for Worldwide Interbank Financial Telecommunication – SWIFT*) са седиштем у Бриселу, која олакшава глобалне финансијске трансакције.[23]

[21] Ибид.

[22] Scott Stewart, "How Iran's Cyber Game Plan Reflects Its Asymmetrical War Strategy", *Stratfor - Worldview*, December 18 2018, p. 1-2, worldview.stratfor.com

[23] Ибид.

Иран често користи милитантне заступнике, као што је Хезболах, да раде „прљав посао" уместо њих и да Техерану пруже могућност порицања. На сличан начин може их снабдевати и обучавати за деловање у сајбер простору. Иран је убрзано побољшао способности за деловање у сајбер простору, па се процењује да ће наставити тај тренд. То је и један од одговора Ирана на санкције и напоре САД да се Иран ослаби.[24]

Медијски рат САД и Ирана одразио се и на одређена дешавања у сајбер простору. Неименовани амерички безбедносни званичници упозорили су, 20. јула 2018. године, америчку телевизијску мрежу *NBC News* да се Иран спрема да покрене дистрибуирани напад одбијања услуга (*Distributed Denial of Service – DDoS*) на инфраструктуру САД. Такође, компанија Симантек (*Symantec Corp.*) упозорила је, 25. јула 2018. године, на нову иранску хакерску групу под називом *Leafminer*. Група се ослањала на добро успостављену тактику циљања на стотине јавних и приватних организација широм Блиског истока, Азербејџана и Авганистана.[25]

Иран има добро документовану историју употребе фишинг напада. Фишинг подразумева убеђивање циља за отварање одређене датотеке у електронској пошти, чиме се малициозни програм уноси у одређени уређај или мрежу и тиме омогућава нападачима приступ или контролу. У 2016. години Иран је поново дистрибуирао малвер *Shamoon*, који је 2012. године довео до уништења хиљада компјутерских терминала *Saudi Aramco*. Малвер је уништио податке и пореметио организације широм Средњег истока. Анализа напада у 2017. години, коју је израдио *IBM*, показује да је малициозни програм дистрибуиран слањем биографија, пропратних писама и других материјала за пријаву на посао, који садрже скривене злонамерне скрипте у наизглед безопасним *Microsoft Word* документима.[26]

И у 2017. години, иранска група названа *APT33* (скраћеница за напредну упорну претњу) слала је материјале са злонамерним програмима запосленима у сектору авијације у Саудијској Арабији. . Према подацима из марта 2018. године, једна иранска сајбер операција компромитовала је 8.000 налога од приближно 100.000 циљаних академских радника. Иако је стопа успеха од 8% релативно ниска, она може дати велике бројеве када је циљна група довољно велика. У наведеном случају, академски радници из 21 земље примили су електронску пошту у којој се изражава заинтересованост за њихов рад. Поруке су садржале линкове на *web* сајтове које опонашају страницу за пријаву на њихов универзитет. Информације добијене на такав начин могле су се користити за приступ легитимним универзитетским *web* страницама, откривајући електронске поруке, истраживачке резултате и контакт-листе.[27]

[24] Ибид.

[25] Ben West, "When It Comes to Cyberattacks, Iran Plays the Odds", *Stratfor - Worldview*, July 31 2018, p. 1-2, worldview.stratfor.com

[26] Ибид.

[27] Ибид.

Иста група која је оптужена за циљање академске заједнице компромитовала је рачуне у 36 америчких и 11 страних компанија једноставним скенирањем корпоративних *e-mail* налога и коришћењем неких од најчешћих лозинки. Најмање 47 запослених користило је изузетно слабе лозинке (123456789, или чак „лозинка"). *Leafminer* група је, такође, користила ту тактику. Мало софистицираније тактика укључује скенирање база података и покушај повезивања претходно компромитованих корисничких имена и лозинки са сличним корисничким именима на другим налозима.[28]

Једна од најактивнијих сајбер група у Ирану, под именом *Charming Kitten* („шармантни мачић"), повезана је са најмање два напада правећи лажне *web* странице. Компромитоване су *web* странице либанске владе, саудијске здравствене службе и азербејџанског универзитета. *Charming Kitten* је осмислио и *web* странице са адресама које опонашају легитимне. Немачки информативни сервис *Deutsche Welle* компромитован је додавањем поддомена „нет" на име домена како би се обманули посетиоци и навели их да мисле да су посетили легитимну страницу. Поред тога, израдили су фиктивну *web* страницу британске новинске агенције (*British News Agency*) како би намамили посетиоце да посете страницу и преузму злонамерни софтвер.[29]

Неименовани високи амерички званичници саопштили су да ирански хакери имају способност да изврше софистициране сајбер нападе на америчку и европску инфраструктуру и приватне компаније. Немачка обавештајна агенција је такође известила о све већој учесталости напада, у последњих неколико година, који су вероватно пореклом из Ирана.[30]

Неравнотежа моћи спречиће Иран да уђе у директни војни сукоб са САД и њиховим савезницима, али се очекује веће деловање асиметричним арсеналом као што су нпр. сајбер напади.[31] Међутим, да би се развиле напредне сајбер способности, држави је потребно много ресурса: снажан систем високог образовања, улагање у истраживање и развој, јавно-приватна сарадња итд. Мале су могућности да ће земље као што су Иран и Северна Кореја имати све ресурсе и привлачити сајбер експерте светске класе. Оно што им недостаје у ресурсима, оне надокнађују амбицијом и великом жељом, као што је био случај са нуклеарним оружјем. Уз мало спољне експертизе могли би превазићи своја ограничења и постати много озбиљнија претња.[32]

Однос Сједињених Држава и Северне Кореје

У јулу 2018. године је, наводно, примећено да Исламска република Иран игра игру бројева у сајбер простору, користећи релативно једноставне технике приступа рачунарским системима, циљајући на хиљаде корисника у нади да ће

[28] Ибид. p. 4.

[29] Ибид.

[30] International Institute for Strategic Studies, Growing cyber threat from Iran, https://www.iiss.org/blogs/cyber-report/2018/07/cyber-report-20-to-26-july, 17/9/2020

[31] Scott Stewart, "How Iran's Cyber Game Plan Reflects Its Asymmetrical War Strategy", op.cit.

[32] Scott Stewart, "Hacking: Another Weapon in the Asymmetrical Arsenal", op.cit.

макар мали проценат угрожених постати и жртве. Представници Министарства правде САД су више пута оптуживали Северну Кореју за сличне инциденте.[33]

Одређени извори наводе да је Северна Кореја највероватнији починилац напада на *Sony Pictures* 2014. године, *Bangladesh Bank* 2016. године, *WannaCry* 2016. и 2017. године и десетине других напада. Операције које изводе Северна Кореја и Иран имају много заједничког у смислу циљања и тактике, али постоји кључна разлика како те две земље приступају својим сајбер кампањама. Док Иран има тенденцију да игра игру великих бројева, Северна Кореја, припрема нападе месецима или понекад годинама.[34]

Иранске и севернокорејске операције су сличне у одабиру циљева, планирању и експлоатацији напада. Обе државе циљају америчке компаније које раде за систем одбране и финансијске институције. Ирански *DDOS* напади на финансијске институције САД од 2011. до 2013. године коштале су америчке компаније милионе долара, док су трошкови Ирана били минимални. Низ севернокорејских напада на финансијске институције широм света наводно је проузроковао штету која се мери стотинама милиона долара.[35]

Обе земље предузимају различите варијанте фишинг напада, покушавајући да преваре своје жртве у преузимању злонамерног софтвера представљајући га као легитимни линк или датотеку. Наводна крађа Северне Кореје од 81 милион долара из централне банке Бангладеша, слањем малициозног програма скривеног као биографије и пропратна писма послата електронском поштом запосленима, представља њен „највећи успех" у сајбер простору. И док је Иран обично имао мотив само да изазове прекид или сметње у функционисању финансијских институција, мотив Северне Кореје био је и финансијски, али и политичка одмазда. Обе државе су показале склоност ка предузимању разорних напада. *WannaCry* напад 2017. године, за који се сматра да је одговорна Северна Кореја, прикривен као *ransomware*[36] напад, имао је за циљ прекид функционисања система.[37]

Међутим, разлике између Северне Кореје и Ирана јављају се у њиховим приступима надгледању система. Неинтрузивним надзором (*non-intrusive surveillance*), нападачи често проводе пасивна надгледања циљане мреже, док интрузивним надзором они илегално приступају циљаној мрежи како би пратили активност изнутра. Улазак у мрежу често претходи главном нападу, чији би циљеви могли бити крађа информација или новца, дистрибуција малициозног

[33] Ben West, "North Korea's Hackers Play the Long Game", *Stratfor - Worldview*, September 18 2018, p. 1-2, worldview.stratfor.com

[34] Ибид.

[35] Ибид.

[36] *Ransomware* је врста малициозног софтвера која ограничава приступ рачунарским системима или похрањеним датотекама те се од жртве тражи откупнина ради добијања параметара за приступ њима.

[37] Ben West, "North Korea's Hackers Play the Long Game", op.cit.

софтвера и друго. Одређени откривени инциденти указују на то да Северна Кореја посвећује много више времена спровођењу инвазивног надзора пре реализације напада.[38]

У спровођењу својих бројних напада, севернокорејски нападачи, ради смањења трошкова и повећања ефикасности, често користе исту инфраструктуру напада. Наравно, нападачи замагљују свој идентитет користећи *proxy* (помоћне) сервере, виртуелне приватне мреже (*Virtual Private Network – VPN*) итд. Коришћење истих адреса електронске поште, уређаја, *IP* адреса и другог, указује на чињеницу да Северна Кореја стоји иза одређених напада у сајбер простору. Може се очекивати да ће у будућности модификовати своје алате и тражити друге циљеве на територији САД и земаља са којима оне гаје „блиске односе".[39]

Сајбер способности постају моћан инструмент националне моћи. Да би нека држава била суперсила у двадесет првом веку мора имати респектабилне способности за сајбер ратовање.[40] Поред САД, Русије, Ирана и Северне Кореје, према проценама експерата са сајбер безбедност, постоји између 20 и 30 држава које имају респектабилне способности за сајбер ратовање.[41, 42] Меру способности за ову врсту ратовања, експерти Кларк и Кнејк (*Clarke u Knake*) дали су на бази процене офанзивне моћи, одбрамбених способности и зависности од рачунарских система. Зависност се односи на критичне информационе системе који немају праву замену, а који су зависни од сајбер простора.[43]

Сједињене Државе, према мишљењу Кларка и Кнејка , немају способност да се дисконектују са остатка сајбер простора, што представља негативан аспект по питању безбедности. Поред наведеног, САД у великој мери зависе од сајбер простора, док Северна Кореја има мали број система зависних од сајбер простора, па евентуални сајбер напад не би довео до озбиљнијих последица. Према мишљењу наведених аутора, од анализираних држава највеће способности за сајбер ратовање има Северна Кореја, затим Иран, па САД. Данас су САД много рањивије на сајбер нападе од Ирана и Северне Кореје, па се може рећи да евентуални сајбер рат у овом тренутку представља недостатак за САД.[44]

---

[38] Ибид., p. 3.

[39] Ибид., p. 2-5.

[40] Marcus Willett, *Cyber instruments and international security*, International Institute for Strategic Studies, Washington, 2019, p. 1.

[41] Cristopher Paul, *Information Operations – Doctrine and Practice*, Praeger Security International, London, 2008, p. 121-122.

[42] Richard A. Clarke, Robert K. Knake, Cyber War – The next treat to National Security and What to do about it, HarperCollins e-books, 2010, p. 59.

[43] Мање зависна држава добија већи број бодова приликом рангирања. Мера способности за сајбер ратовање разматраних држава приказана је према следећем:

– САД – сајбер напад = 8, сајбер зависност = 2, сајбер одбрана = 1; укупно: 11.

– Иран – сајбер напад = 4, сајбер зависност = 5, сајбер одбрана = 3; укупно: 12.

– С. Кореја – сајбер напад = 2, сајбер зависност = 9, сајбер одбрана = 7; укупно: 18.

[44] Richard A. Clarke, Robert K. Knake, op.cit, p. 127-128.

Закључак

Војно присуство у сајбер простору је несумњиво. Инциденти између држава су све бројнији и озбиљнији. Наведени примери показују да су неке активности припремане годинама и уз подршку одређених државних органа. Без обзира на то што је покренута истрага против одређених група, које су најчешће спонзорисане од држава, мало је вероватно да ће то одвратити земље као што су Северна Кореја и Иран од даљих активности и представљаће све већу претњу по безбедност САД.

Геополитичка неслагања и различити интереси одразиће се и на дешавања у сајбер простору. Претње у том подручју су у сталној еволутивности и несумњиво ће у будућности бити све софистицираније, опасније и све чешће спонзорисане од стране државе. Будућност карактерише и све више „озбиљних играча" у сајбер простору који ће наведено подручје користити једни против других. Дигитална револуција је произвела ново подручје у којем се шпијунира, саботира и на различите начине угрожавају одређени сегменти друштва. У том смислу, нарочито осетљиве биће критичне информационе инфраструктуре, које су у великом проценту у приватном власништву, а од којих друштво значајно зависи.

Дигитална револуција створила је нови домен у коме ће се несумњиво и даље шпијунирати, саботирати или сукобљавати на различите начине. Будући непријатељи, било државе, групе или појединци, могу покушавати да угрозе информационе инфраструктуре коришћењем нетрадиционалних метода, а управо такви напади могли би знатно угрозити и војну и економску моћ нападнуте државе. Информациона револуција и повезане организационе и функционалне промене мењају чак и природу сукоба, посебно међу државама, као и начин њиховог решавања. Односи између светских и регионалних сила у сајбер простору зависиће, у великој мери, од односа тих држава у реалном свету.

Литература

[1] Анђелија Ђукић, „Крађа идентитета – облици, карактеристике и распрострањеност", *Војно дело*, Министарство одбране РС – Медија центар „Одбрана", Београд, број 3, 2017.

[2] Ben West, North Korea's Hackers Play the Long Game, *Stratfor - Worldview*, September 18 2018, worldview.stratfor.com

[3] Ben West, When It Comes to Cyberattacks, Iran Plays the Odds, *Stratfor - Worldview*, July 31 2018, worldview.stratfor.com

[4] Cristopher Paul, *Information Operations – Doctrine and Practice*, Praeger Security International, London, 2008.

[5] Дејан Вулетић, *Безбедност у сајбер простору*, Министарство одбране РС – Медија центар „Одбрана", Београд, 2012.

[6] Дејан Вулетић, *Одбрана од претњи у сајбер простору*, Институт за стратегијска истраживања, Београд, 2011.

[7] Дејан Вулетић, „Психолошка димензија хибридног ратовања", *Војно дело*, Министарство одбране РС – Медија центар „Одбрана", број 6, 2018.

[8] Дејан Вулетић, „Употреба сајбер простора у контексту хибридног ратовања”, *Војно дело*, Министарство одбране РС – Медија центар „Одбрана”, број 7, 2017.

[9] Eneken Tikk, *Cyber arms control and resilience*, SIPRI Yearbook - Armaments, Disarmament and International Security, Oxford University Press, 2019.

[10] Hudson Institute, General John E. Hyten on Progress and Challenges Implementing the National Defense Strategy, https://www.hudson.org/events/1853-video-event-general-john-e-hyten-on-progress-and-challenges-implementing-the-national-defense-strategy82020, 16/11/2020

[11] Helen Nissenbaum, „Where computer security meets national security”, *Ethics and Information Technology*, vol. 7, no. 2, 2005.

[12] International Institute for Strategic Studies, Growing cyber threat from Iran, https://www.iiss.org/blogs/cyber-report/2018/07/cyber-report-20-to-26-july, 17/9/2020

[13] Joint Publication 3-12, Cyberspace operations, 8 June 2018, Joint Chiefs of Staff. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf, 20/10/2020

[14] Joint Vision 2020, https://apps.dtic.mil/dtic/tr/fulltext/u2/a526044.pdf, 14/11/2020

[15] Marcus Willett, *Cyber instruments and international security*, International Institute for Strategic Studies, Washington, 2019.

[16] National Cyber Strategy of the United States of America, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf, 17/10/2020

[17] Nigel Inkster, *It's time to stabilise cyberspace – our well-being depends on it*, International Institute for Strategic Studies, Washington, 2019.

[18] Richard A. Clarke, Robert K. Knake, *Cyber War – The next treat to National Security and What to do about it*, HarperCollins e-books, 2010.

[19] Scott Stewart, Hacking: Another Weapon in the Asymmetrical Arsenal, Stratfor - Worldview, January 25 2018, worldview.stratfor.com

[20] Scott Stewart, How Iran's Cyber Game Plan Reflects Its Asymmetrical War Strategy, Stratfor - Worldview, December 18 2018, worldview.stratfor.com

[21] The Military Balance, Volume 119, Issue 1 (2019), https://www.tandfonline.com/toc/tmib20/119/1?nav=tocList

[22] The U.S. Army in Multi-Domain Operations 2028, TRADOC, 2018, https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf, 22/11/2020

Сајбер простор као подручје сукобљавања: случај САД – Иран и Северна Кореја

Савремено друштво критички зависи од информација, као стратешког ресурса и информационо-комуникационих технологија, које врше њихов пренос, обраду и размену. Информационо-комуникационе технологије су створиле ново окружење, сајбер простор, у којем су тензије, неслагања и инциденти све чешћи. Последњих година наведена област се све више појављује као

подручје домена сукоба између водећих светских и регионалних сила. У раду се даје кратак опис концепта операција у неколико домена и елемената новог концепта заједничког ратовања оружаних снага САД. На важност сајбер простора за САД указано је прегледом организационих промена и усвајањем одређених стратешких и доктринарних докумената. Рад представља одређене догађаје и активности у сајбер простору последњих година између САД с једне стране и Ирана и Северне Кореје с друге стране.

Америчка Сајбер Команда (USCYBERCOM) је створена 2009. године. Наведена Команда је у мају 2018. године подигла свој статус на пуну и независну обједињену команду. То указује на важност сајбер простора за Пентагон. На много начина, одвајање Америчке Сајбер Команде од стратешких команди, која надгледа стратешко одбијање, представља симбол промене става САД у сајбер простору од „одбрамбеног" до „константног ангажовања". Сједињене Државе су и даље најјача сила у сајбер простору и показују амбицију за спровођење сајбер операција на свим нивоима командовања.

Мало је вероватно да ће Иран испровоцирати Сједињене Државе на војни сукоб великих размера и директан рат у сајбер простору. Иран је брзо усавршио своју способност да делује у сајбер простору и процењује се да ће се овај тренд наставити. Неравнотежа може спречити Иран да уђе у директан војни сукоб са Сједињеним Државама и њиховим савезницима. Очекује се појачано деловање са асиметричним арсеналом какви су нпр. сајбер напади.

Иранске и севернокорејске операције су сличне у избору циљева, планирању и експлоатацији напада. Обе земље предузимају различите облике *phishing* напада покушавајући да преваре своје жртве да преузму злонамерни софтвер представљајући га као легитимни линк или датотеку. И док је Иран обично имао мотив само да изазове поремећај у функционисању финансијских институција, мотив Северне Кореје био је и финансијска и политичка одмазда. Одређени откривени инциденти указују да Северна Кореја много више времена посвећује спровођењу инвазивног надзора пре извођења напада. Бројни примери показују да су се неке активности припремале током година и уз подршку одређених државних органа.

Без обзира што је покренута истрага против одређених група, које најчешће спонзоришу државе, мало је вероватно да ће то одвратити земље попут Северне Кореје и Ирана да одустану од даљих активности и представљаће све већу претњу америчкој безбедности.

Кључне речи: *сајбер простор, сукоб, САД, Иран, Северна Кореја*