# 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*



# CYBERSPACE AS A DOMAIN OF CONFLICT: THE CASE OF THE UNITED STATES – IRAN AND NORTH KOREA*

*Dejan* V. Vuletić**
*Miloš* R. Milenković***
*Anđelija* R. Đukić****

*Достављен*: 03. 12. 2020.
*Кориговано*: 19. 01, 08. 02. и 05. 03. 2021.
*Прихваћен*: 19. 03. 2021.
*Језик рада:* Енглески
*Тип рада:* Прегледни рад
*DOI број:* 10.5937/vojdelo2101075V

In recent years, cyberspace has increasingly appeared as a domain of conflict between leading world and regional powers. The paper presents its importance and there is a brief description of the new concept of joint warfare of the United States (US). Certain events and activities in cyberspace in the last few years between the United States on the one hand and Iran and North Korea on the other have been considered.

The mentioned subject of the research is directly related to the objective of the paper, which is aimed at emphasizing and explaining the forms and characteristics of attacks, as well as certain actors of conflict in cyberspace. The main hypothesis is that cyberspace is a domain of conflict between the world and regional powers in which they often use non-state actors as intermediaries, with continuous improvement of techniques and methods of carrying out attacks.

In addition to general scientific methods, considering the subject and objective of the research, the comparative method, which analyses and compares the similarities and differences of carrying out attacks on the information infrastructure of the parties to the conflict, has been mainly used, as well as the method of content analysis, bearing in mind that official and reference expert reports, scientific papers and other

* The paper is the result of work on the scientific research project "Physiognomy of modern armed conflicts", which is conducted on the basis of the Plan of scientific research activities in the Ministry of Defence and the Serbian Armed Forces for 2021, number 2-2.

** Strategic Research Institute, University of Defence in Belgrade, Belgrade, dejan.vuletic@mod.gov.rs

*** Strategic Research Institute, University of Defence in Belgrade, Belgrade.

**** Strategic Research Institute, University of Defence in Belgrade, Belgrade.

publications have been used as sources of information. On the basis of the presented arguments in the paper, it can be concluded that the incidents in cyberspace between the US and Iran, i.e. North Korea, are numerous, often prepared for a long time, with the active participation of non-state actors.

Key words: *cyberspace, conflict, US, Iran, North Korea*

## Introduction

Most countries have substantial resources based on information and communications technology, including defence systems, public administration systems, complex management systems and information infrastructures that encompass control of electricity, telephone system, money flows, air traffic, oil and gas flows, and other information dependent fields. The society is becoming more and more dependent on information and communications technology,[1] which results in its increasing sensitivity both due to the growing number of users and due to the trend of interconnecting computer networks.[2] Therefore, the protection of information infrastructures is imposed as one of the priorities of national security.[3]

As a result of social needs and technological innovations, cyberspace has been created - an intangible, unlimited interactive space created by computer networks.[4] It is essentially a globally connected information and communications infrastructure.[5]

Enemies, whether states, groups or individuals, try to threaten critical information infrastructures using non-traditional methods. It is precisely such attacks that could significantly threaten both the military and economic power of the attacked state. Geopolitical disagreements spill over into cyberspace.[6] States are engaged in the increasing competition in cyberspace "at a level below an armed conflict".[7]

[1] Anđelija Đukić, „Krađa identiteta – oblici, karakteristike i rasprostranjenost", *Vojno delo*, Ministarstvo odbrane RS – Medija centar „Odbrana", Belgrade, Issue 3/2017, p. 99.

[2] Dejan Vuletić, *Odbrana od pretnji u sajber prostoru*, Strategic Research Institute, Belgrade, 2011, p. 5.

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

[4] Dejan Vuletić, *Bezbednost u sajber prostoru*, Ministarstvo odbrane RS – Medija centar „Odbrana", Belgrade, 2012, pp.21-23.

[5] Dejan Vuletić, „Upotreba sajber prostora u kontekstu hibridnog ratovanja", *Vojno delo*, Ministarstvo odbrane RS – Medija centar „Odbrana", Issue 7/2017, p. 310.

[6] Dejan Vuletić, „Psihološka dimenzija hibridnog ratovanja", *Vojno delo*, Ministarstvo odbrane RS – Medija centar „Odbrana", Issue 6/2018, p.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.

## The concept of multi-domain operations

In the era of rapid human progress, the US Armed Forces are in a situation where different, connected, elements of the operational environment converge, creating a situation where trends in the diplomatic, information, military and economic sphere quickly transform the nature of all aspects of society, including the character of war. The US strategists estimate that the current US comparative military advantage and capacity to conduct operations against a sophisticated enemy is diminished.

Potential adversaries, above all Russia and China, but also Iran and North Korea, have taken numerous steps to distract the efficiency of the US military power, which creates a more unfavourable situation for the United States. The growth of air, land and naval capabilities of potential adversaries with developed strike capabilities in space and cyberspace enable them to fight the US forces in those areas where the US dominance has long been assumed.[8] The US reliance on cyberspace in the process of command and control of joint air operations can be particularly under threat, having in mind the fact that the main adversaries make great efforts to improve their capabilities in such domain.

*Joint Vision 2020* calls for full-spectrum dominance, with the US forces having to conduct fast and synchronised operations with combinations of forces tailored to specific situations, access and freedom to operate in all domains (land, sea, air, space and cyberspace). The ability to achieve superiority in all domains is emphasized as a key factor of dominance.[9]

At the end of 2019 the US Secretary of Defense, *Mark Esper*, ordered the relevant services and the *Joint Staff* to prepare a new *Joint Warfighting Concept* for operations in all domains (areas, spaces) by the end of 2020. That concept should describe the capabilities and attributes necessary for action in the future, in all domains, which directs the development of the Ministry of Defense in the coming decades.

General *John Hyten*, the Vice Chairman of the Joint Chiefs of Staff, during his lecture on August 12, 2020, organized by the *Hudson Institute* and reported by *Defense N*ews, spoke about the new concept, emphasizing that the greatest difference will be in that there will be no line on the battlefield in the future.[10]

The increased, primarily technological development, requires new concepts, so the terminology itself has developed rapidly in recent years - from multi-domain (multidimensional) battle through multi-domain (multidimensional) operation to operations in all domains (*Multi-Domain Battle; Multi-Domain Operations; All -Domain Operations*).

---

[8] According to *the US Council for Foreign Relations* and the *Center for Strategic and International Studies – CSIS* data, over 250 state-sponsored US cyber attacks in the period from 2005 to 2018 have been identified. 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

The concept of a multi-domain operation basically explains how the US forces will deter and defeat an adversary in a situation "below the level of an armed conflict", as well as in the armed conflict itself. This concept enables the US forces to physically, virtually and cognitively overpower their adversaries, using combined weapons in all domains. It also provides recommendations regarding the capabilities that commanders need to defeat an advanced enemy and proposes a new framework for better understanding of the 21st century battlefield. A multi-domain operation is necessary for the US forces together with allies and other partners in order to successfully deter and defeat adversaries in future conflicts.

The US strategists estimate that better integration of all forces has to be accomplished in order that the US Armed Forces can maintain superiority in capabilities over advanced enemy technologies and concepts. According to expert estimation, the current system does not integrate all domains enough, such as e.g. technological integration. Certain weaknesses have also been noticed in the real time command and control system.

The concept of *the U.S. Army in Multi-Domain Operations 2028*[11], developed by the *Training and Doctrine Command* (TRADOC) in 2018, proposes a range of solutions to conflicts in various domains. The main idea is the rapid and continuous integration of all domains of warfare in order to deter the adversary and gain an advantage in an armed conflict. If deterrence failed, military formations as a part of the Joint Staff, would penetrate and disintegrate enemy systems, use the freedom of manoeuvre resulting from such a situation and achieve their own strategic objectives and consolidate profit to force the enemy to return to a more favourable position for the United States, its allies and partners.

## Significance of cyberspace for the United States

The establishment of the US Cyber Command in 2009 and obtaining the status of an independent operational command in May 2018 (until then it was a part of the Strategic Command), shows the significance of cyberspace for the Pentagon. In many ways, the exclusion of the US Cyber Command from the Strategic Command, which monitors strategic deterrence, is a symbol of the change in the US attitude in cyberspace from "defence" to "persistent engagement." The United States, still being the most prominent cyber power in the world, has expressed ambitions to carry out cyber operations at all levels of command. The US Cyber Command has the capacity of several thousand members, who can be engaged in planning and carrying out attacks. In mid-2018, the *Joint Publication 3-12 Cyberspace Operations* Regulation, which defines the evaluation, preparation, planning and execution of cyber operations, was adopted.[12]

The Cyber Command presents its objective that the United States has to defend themselves as close as possible to the source of enemy activities and actors before

[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

[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

they achieve tactical, operational and strategic advantages. This belief is reinforced in the National Cyber Strategy published in September 2018.[13] It states that the objective is to identify, counter, distract, degrade and deter behavior in cyberspace that is destabilising and contrary to the national interests of the United States, i.e. achieving the US dominance and supremacy in cyberspace. If fully implemented, the Strategy would involve taking actions against certain actors in cyberspace, which was the case against Iran for allegedly shooting down the US drone.

The US strategic documents emphasize the right to countermeasures and self-defence in the case of a cyber attack. In the previous period the US attitude towards cyberspace was more defensive and aimed primarily at deterring potential attackers. The United States has believed that the perception of their offensive capabilities could deter adversaries from attack. The concept of strategic deterrence in cyberspace has not proven to be effective in practice. Distracting and harassing major competitors in cyberspace, as opposed to deterrence, have become a more attractive option for the US strategists.

In August 2018, the US President *Donald Trump* issued the order (*PPD-20*) repealing policies of the former US President *Barack Obama*, which established a complicated procedure for the interdepartmental process that has to be followed before the United States could launch a cyber attack.

Although the US adversaries believe that in the case of a cyber attack on the United States, this would lead to a response, knowing the difficulties of attributing those attacks to certain state actors, they are increasingly engaging non-state actors to carry out offensive actions against the United States and its allies.

In order to improve deterrence, the United States is increasingly bringing charges against individuals from China, Iran, North Korea and Russia. It is believed that a number of suspects will never face extradition and prosecution, but public disclosure of their names could change their decisions and deter other potential assailants. Moreover, the United States endeavours to impose economic sanctions against individuals and organisations. Several countries, including the United States, publish data on their cyber capabilities and readiness to use them for national defence.[14]

## US-Iran relationship

On January 4, 2018, the *Carnegie Endowment for International Peace* published a report in which Iran was identified as a source of threats in cyberspace. The authors state that despite Iran's success with the *Shamoon* malware[15] and the phishing attack

[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

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

[15] The *Shamoon* malware (*W32.DistTrack*) was discovered in August 2012 by Kaspersky, Simantec and Seculert. In relation to other malicious programmes, it is characterised by great destructiveness and the necessity of high costs and recovery time of the target system.

on *Deloitte* and several other corporations, the Iranian attacks are mostly poorly concealed. As a result, the experts investigating the event did not have much trouble finding the perpetrators. The evidence indicated that the perpetrators were from Iran, both because of the IP addresses[16] and the Persian language terms in the malicious programmes. Iran's capabilities are estimated to be relatively small compared to Russia and China, but they certainly pose a threat to the United States.[17]

Some experts believe that with the development of cyber attacks as asymmetric weapons, states will become more involved. The sale of certain conventional weapons to Iran and Syria also indicates the possibility of supply and training when it comes to cyber tools. According to certain sources, the United States and Israel have already had such cooperation related to the malicious programme Stuxnet[18], which weakened Iran's uranium enrichment capacity in 2010.[19] This kind of assistance and knowledge transfer has happened in the past, primarily in the field of the development of nuclear weapons.[20]

Cyber attacks will not replace terrorism as an asymmetric weapon. Many characteristics that make terrorism attractive to perpetrators can also be related to cyber attacks. The cyber attacks that have been carried out so far, aided by certain states, have not been accompanied by an appropriate negative reaction, detection and prosecution of the perpetrators. Low costs, time and effort to implement, will undoubtedly encourage more states to opt for this type of attack.[21]

Just as it is unlikely that Iran will provoke the United States in a large-scale military conflict, it is also unlikely that it will wage a direct war in cyberspace. The comparison of the complexity of the malicious programmes *Stuxnet* (related to the US and Israel) and *Shamoon* (related to Iran) illustrates the difference in capabilities. Despite that fact, the United States is vulnerable to cyber attacks. Despite that reality, both sides will continue to prepare for a cyber war. Iran, as well as other countries (China, Russia, North Korea, etc.), and certain non-state actors, have been monitoring the critical infrastructure of the United States and the West for many years. Furthermore, Americans and their allies are engaged in reconnaissance of Iranian infrastructure. At the *Aspen Security Forum* in July 2018, the director of the US National Intelligence Service, *Dan Coats*, noted that Iran is preparing to target electrical networks, water dams and technological companies in the US, Europe and the Middle East.[22]

---

[16] IP address (*Internet Protocol address*) is a unique 32-bit number used by various devices to communicate with each other over the Internet, using certain protocols.

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

[18] Stuxnet is a malicious computer programme, discovered in 2010, which endangered Iranian nuclear programme and it is suspected to have been made by the United States and Israel.

[19] Scott Stewart, op.cit.

[20] Ibid.

[21] Ibid.

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

Surveillance does not mean that an attack will happen for sure. Like any war plan, cyber plans are updated in order to take into account changes in operating systems, the vulnerability of security and other measures. Iran, i.e. the Hezbollah militant groups with which it cooperates are also engaged in these activities. While cyber warfare is still unlikely, lower-level Iranian attacks against the US government institutions, private companies and organisations are likely to increase. At the end of 2018, the representatives of the Italian oilfield services company *Saipem* said that they were endangered by a cyber attack, i.e. a malicious programme that is a variant of the *Shamoon* malware, which indicates that the perpetrators are probably from Iran. The *Saipem's* greatest client is the national oil company *Saudi Arabian Oil Co*., a competitor to the Iranian company, which is probably the reason why the Italian company was attacked. In addition, the London company *Certfa*, which specializes in monitoring Iranian activities in cyberspace, has published a report that indicates Iranian phishing attacks aimed at the financial infrastructure of the United States. The attacks are also aimed at the Brussels-based *Society for Worldwide Interbank Financial Telecommunication - SWIFT)*, which facilitates global financial transactions.[23]

Iran often uses militant lawmakers such as Hezbollah to do "dirty work" for them and give Tehran the opportunity to deny it. In a similar way, it can supply and train them to operate in cyberspace. Iran has rapidly improved its capabilities to operate in cyberspace, so it is estimated that it will continue this trend. That is one of Iranian responses to the US sanctions and their efforts to weaken Iran.[24]

The media war between the United States and Iran has also affected certain events in cyberspace. On July 20, 2018, unnamed US security officials warned the US television network *NBC News* that Iran was preparing to launch the *Distributed Denial of Service - DDoS* attack on the US infrastructure. Moreover, on July 25, 2018, *Symantec Corp.* warned of a new Iranian hacker group called *Leafminer*. The group relied on the well-established tactics to target hundreds of public and private organisations across the Middle East, Azerbaijan and Afghanistan.[25]

Iran has well-documented history of phishing attacks. Phishing involves persuading a target to open a certain file in an email, allowing a malicious programme to enter a specific device or network, thus allowing attackers access or control. In 2016, Iran redistributed the *Shamoon* malware, which led to the destruction of thousands of *Saudi Aramco* computer terminals in 2012. The malware destroyed data and disrupted organisations across the Middle East. An analysis of the 2017 attack by *IBM* shows that the malicious programme was distributed by sending resumes, cover letters and other job application materials, which contain hidden malicious scripts in seemingly harmless *Microsoft Word* documents.[26]

[23] Ibid.

[24] Ibid.

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

[26] Ibid.

In 2017 an Iranian group called *APT33* (abbreviation for Advanced Persistent Threat) sent materials with malware to the employees in the aviation sector in Saudi Arabia. According to the March 2018 data, an Iranian cyber operation compromised 8,000 accounts of approximately 100,000 targeted academics. Although the success rate of 8% is relatively low, it can give great numbers when the target group is large enough. In the mentioned case, academics from 21 countries received an e-mail expressing an interest in their work. The messages contained links to the *web*sites that mimicked their university application page. The information obtained in this way could be used to access legitimate university *web*sites, revealing emails, research results and contact lists.[27]

The same group accused of targeting academia has compromised the accounts in 36 US and 11 foreign companies by simply scanning corporate *e-mail* accounts and using some of the most common passwords. At least 47 employees have used extremely weak passwords (123456789, or even "password"). The *Leafminer* group has used this tactic, as well. A slightly more sophisticated tactic involves scanning databases and trying to link previously compromised usernames and passwords to similar usernames on other accounts.[28]

One of the most active cyber groups in Iran called *Charming Kitten* is associated with at least two attacks by making fake *web*sites. The *web*sites of the Lebanese government, the Saudi health service and the University of Azerbaijan have been compromised. *Charming Kitten* has also designed *web*sites with addresses that imitate the legitimate ones. The German news service *Deutsche Welle* has been compromised by adding a "net" subdomain to the domain name to deceive visitors and make them think they have visited a legitimate site. In addition, they have created a fictitious *web*site of the *British News Agency* with the aim of enticing visitors to visit the site and download malicious software.[29]

Unnamed senior US officials say the Iranian hackers have the ability to carry out sophisticated cyber attacks on the US and European infrastructure and private companies. The German intelligence agency has also reported an increasing frequency of attacks in recent years, which are probably of the Iranian origin.[30]

The imbalance of power will prevent Iran from a direct military conflict with the United States and their allies, but greater action by an asymmetric arsenal such as e.g. cyber attacks is expected.[31] However, in order to develop advanced cyber capabilities, the state needs many resources: a strong high education system, investment in research and development, public-private cooperation, etc. There is little chance for the states such as Iran and North Korea to have all the resources

[27] Ibid.

[28] Ibid., p. 4.

[29] Ibid.

[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.

and attract world-class cyber experts. What they lack in resources, they make up for with ambition and great desire, as it was the case with nuclear weapons. With some external expertise, they could overcome their limitations and become a far more serious threat.[32]

## US-North Korea relationship

In July 2018, it was reportedly spotted that the Islamic Republic of Iran was playing a number game in cyberspace, using relatively simple techniques to access computer systems, targeting thousands of users in the hope that at least a small percentage of those at risk would become victims. The US Justice Department officials have repeatedly accused North Korea of similar incidents.[33]

Certain sources state that North Korea is the most likely perpetrator of the attacks on *Sony Pictures* in 2014, *Bangladesh Bank* in 2016, *WannaCry* in 2016 and 2017, and dozens of other attacks. The operations carried out by North Korea and Iran have a lot in common in terms of targeting and tactics, but there is a key difference in how the two countries approach their cyber campaigns. While Iran tends to play a game of large numbers, North Korea prepares attacks for months or sometimes years.[34]

Iranian and North Korean operations are similar in target selection, planning and exploitation of attacks. Both states target the US companies working for the defence system and financial institutions. Iranian *DDOS* attacks on the US financial institutions from 2011 to 2013 cost the US companies millions of dollars, while Iranian costs were minimal. A series of North Korean attacks on financial institutions around the world have allegedly caused damage amounting to hundreds of millions of dollars.[35]

Both states undertake different variants of phishing attacks in an attempt to deceive their victims into downloading malicious software by presenting it as a legitimate link or file. The alleged $81 million theft of North Korea from the Central Bank of Bangladesh, by sending a malicious programme hidden as resumes and cover letters sent by e-mail to employees, represents its "greatest success" in cyberspace. While Iran used to have a motive only to cause disruption or disturbance to the functioning of financial institutions, North Korean motive was both financial one and political retaliation. Both states have shown a propensity to launch devastating attacks. The 2017 *WannaCry* attack, which is believed to be conducted by North Korea, disguised as a *ransomware*[36] attack, was aimed at shutting down the system.[37]

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

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

[34] Ibid.

[35] Ibid.

[36] *Ransomware* is a type of malicious software that restricts the access to computer systems or stored files, and a ransom is demanded from a victim in order to obtain the parameters to access them.

However, differences between North Korea and Iran arise in their approaches to monitoring the system. Using *non-intrusive surveillance*, attackers often conduct passive surveillance of the target network, while by intrusive surveillance they illegally access the target network to monitor an activity from the inside. Entering the network often precedes the main attack, whose goals could be the theft of information or money, distribution of malicious software, etc. Certain, discovered incidents indicate that North Korea devotes much more time to conducting invasive surveillance before carrying out attacks.[38]

In carrying out their numerous attacks, North Korean attackers often use the same attack infrastructure in order to reduce costs and increase efficiency. Attackers, of course, obscure their identity using *proxy* servers, *Virtual Private Networks - VPNs*, etc. The use of the same e-mail addresses, devices, *IP* addresses, etc., indicates the fact that North Korea is responsible for certain attacks in cyberspace. It can be expected that in the future, it will modify its tools and look for other targets in the US and the states with which they cultivate "close relations".[39]

Cyber capabilities are becoming a powerful instrument of national power. For a state to be a superpower in the 21st century, it should have respectable capabilities for cyber warfare.[40] In addition to the United States, Russia, Iran and North Korea, according to cyber security experts' assessment, there are between 20 and 30 countries that have respectable capabilities for cyber warfare.[41],[42] The experts *Clarke and Knake* have given a measure of capability for this type of warfare on the basis of the evaluation of offensive power, defence capabilities and dependence on computer systems. Addiction refers to critical information systems that do not have an adequate replacement, and that are dependent on cyberspace.[43]

According to Clarke and Knake, the United States does not have the ability to disconnect from the rest of cyberspace, which is a negative aspect in terms of security. In addition, the United States is heavily dependent on cyberspace while North Korea has a small number of systems dependent on cyberspace, so a potential cyber attack would not cause more serious consequences. According to the mentioned authors, North Korea has the greatest capabilities for cyber warfare

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

[38] Ibid., p. 3.

[39] Ibid., pp. 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, pp. 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] A less dependent country gets a greater number of points when being ranked. The measure of cyber warfare capability of the considered countries is shown according to the following:

– US – cyber attack = 8, cyber addiction = 2, cyber defence = 1; total: 11.

– Iran – cyber attack = 4, cyber addiction = 5, cyber defence = 3; total: 12.

– N. Korea – cyber attack = 2, cyber addiction = 9, cyber defence = 7; total: 18.

among the analysed countries, followed by Iran and the United States. Today the United States is far more vulnerable to cyber attacks than Iran and North Korea, so possible cyber warfare is currently a disadvantage for the United States.[44]

## *Conclusion*

The military presence in cyberspace is unquestionable. Incidents between countries are becoming more numerous and serious. These examples show that some activities have been prepared for years and with the support of certain state authorities. Despite the fact that an investigation has been launched against certain groups, which have been most often sponsored by states, it is unlikely that this will deter countries such as North Korea and Iran from further activities and it will pose an increasing threat to the US security.

Geopolitical disagreements and different interests will be reflected in the events in cyberspace, as well. Threats in such a space are constantly evolving and they will undoubtedly be more sophisticated, dangerous and more frequently sponsored by states in the future. The future is also characterised by more "serious players" in cyberspace, who will use this field against each other. The digital revolution has produced a new area in which certain segments of society are being spied on, sabotaged and threatened in various ways. In that sense, critical information infrastructures, which are in a large percentage in private ownership, and which the society significantly depends on, will be particularly sensitive.

The digital revolution has produced a new domain in which there will undoubtedly continue to be spying on, sabotaging or clashing in various ways. Future enemies, whether states, groups or individuals, may attempt to threaten information infrastructures using non-traditional methods, and precisely such attacks could significantly threaten both the military and economic power of the attacked state. The information revolution and related organisational and functional changes are changing even the nature of conflict, especially between states, as well as the way they are resolved. The relations between world and regional powers in cyberspace will largely depend on the relations of those countries in the real world.

## *References*

[1] Anđelija Đukić, „Krađa identiteta – oblici, karakteristike i rasprostranjenost", Vojno delo, Ministarstvo odbrane RS – Medija centar „Odbrana", Beograd, 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

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

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

[5] Dejan Vuletić, *Bezbednost u sajber prostoru*, Ministarstvo odbrane RS – Medija centar „Odbrana", Belgrade, 2012.

[6] Dejan Vuletić, *Odbrana od pretnji u sajber prostoru*, Strategic Research Institute, Belgrade, 2011.

[7] Dejan Vuletić, „Psihološka dimenzija hibridnog ratovanja", *Vojno delo*, Ministarstvo odbrane RS – Medija centar „Odbrana", broj 6, 2018.

[8] Dejan Vuletić, „Upotreba sajber prostora u kontekstu hibridnog ratovanja", *Vojno delo*, Ministarstvo odbrane RS – Medija centar „Odbrana", broj 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

# Cyberspace as a Domain of Conflict: the Case of the United States – Iran and North Korea

Modern society is critically dependent on information as a strategic resource and information and communications technology, which carries out its transmission, processing and exchange. Information and communications technology has created a new environment, cyberspace, in which tensions, disagreements and incidents are becoming more frequent. In recent years, the mentioned area has increasingly appeared as a domain of conflict between the leading world and regional powers. The paper gives a brief description of the concept of operations in several domains and elements of the new concept of joint warfare of the US Armed Forces. The importance of cyberspace for the US has been pointed out with a review of organizational changes and the adoption of certain strategic and doctrinal documents. The paper presents certain events and activities in cyberspace, in recent years, between the United States on the one hand, and Iran and North Korea on the other.

The United States Cyber Command (USCYBERCOM) was created in 2009. USCYBERCOM was elevated to the status of a full and independent unified command in May 2018. It indicates the importance of cyberspace for the Pentagon. In many ways, the separation of USCYBERCOM from Strategic Commands, which oversees strategic rejection, is a symbol of the change in the US attitude in cyberspace from "defensive" to "persistent engagement." The United States is still the strongest force in cyberspace and shows ambition to carry out cyber operations at all levels of command.

It is unlikely that Iran will provoke the United States into a large-scale military conflict and wage a direct war in cyberspace. Iran has rapidly improved its ability to operate in cyberspace, and it is estimated that this trend will continue. The imbalance can prevent Iran from a direct military conflict with the United States and its allies. Greater action is expected with an asymmetric arsenal such as e.g. cyber attacks.

Iranian and North Korean operations are similar in target selection, planning and exploitation of attacks. Both countries undertake different variants of phishing attacks in an attempt to deceive their victims into downloading malicious software by presenting it as a legitimate link or file. Whereas Iran usually had a motive only to cause disruption to the functioning of financial institutions, North Korean motive was both financial and political retaliation. Certain discovered incidents indicate that North Korea devotes much more time to conducting invasive surveillance before carrying out attacks. Numerous examples show that some activities have been prepared over the years and with the support of certain state bodies.

Regardless of the fact that an investigation has been launched against certain groups, most often sponsored by states, it is unlikely that this will deter countries such as North Korea and Iran from giving up further activities and will pose an increasing threat to the US security.

Key words: *cyberspace, conflict, US, Iran, North Korea*