Ванредни професор

Универзитет у Београду

Факултет безбедности

E-mail: n.putnik@fb.bg.ac.rs

UDK: 327:004.738.5(73)(510)

COBISS.SR-ID: 67037449

DOI: 10.18485/fb_givs_sbmd.2022.ch9

Број страница: 139–149

АМЕРИЧКО-КИНЕСКИ СТРАТЕШКИ РИВАЛИТЕТ У САЈБЕР ПРОСТОРУ

Проф. др Ненад Путник

Апстракт:

Последњих година Кина у знатној мери утиче на преобликовање међународних односа и испољава највећу експанзију спољнополитичких и економских циљева. Сајбер простор је од есенцијалног оперативног значаја у тим активностима, као и у модерним сукобима, нарочито у асиметричном ратовању. У сајбер простору највеће ривалство данас је присутно између САД и Кине. У овом раду приказана су истраживања која то потврђују, као и теоријски приступи односима ове две земље, који објашњавају узроке тињајућег конфликта међу њима. Описана актуелна филозофија сајбер конфликата и начини њиховог манифестовања могу представљати основу за даље подробније анализе, имајући у виду да је сајбер простор попримио стратешки значај за испољавање антагонизама између великих сила.

Кључне речи:

конфликти, сајбер простор, сајбер напад, сајбер шпијунажа, САД, Кина

Увод

Конфликти међу државама (па и унутар њих) присутни су од њиховог настанка; кроз време су се мењали главни означени унутрашњи и спољни непријатељи (групе и субгрупе, војно-политички савези) и модалитети њиховог постојања и испољавања (оружани и неоружани сукоби, отворени и прикривени). Чини се да је падом Берлинског зида, а затим и распадом СССР-а и савеза који је ова политичка идеологија окупљала, у извесној мери смањена опасност избијања светског рата – дуго је војно и економски био доминантан једино НАТО и водеће државе у оквиру њега, пре свега САД. Међутим, почетком XXI века многе државе, различитог друштвено-политичког уређења, почињу економски, али и војно да снаже и креирају и остварују своје интересе изван националних, па и континенталних граница, међу којима пре свих Русија, Кина, а затим и Турска. Дугогодишња економска и војна слика света почиње да се мења, а успостављање „нове равнотеже" пре свега САД су виделе као опасност по своје интересе. Међународни односи преобликовани су услед моћних трендова, од којих су неки створени захваљујући новим технологијама, неки јаком реакцијом на Америчку хегемонију (Lewis 2018: 15).

Чини се да је највећу експанзију спољнополитичких и економских циљева испољила Кина – држава снажне комунистичке оријентације, контролисане друштвене отворености према свету и значајног капитала, путем којег жели да остварује своје интересе, пре свега у Европи. Њен пројекат „Појас и пут" (много савременија и комплекснија верзија „Пута свиле") на Конгресу Комунистичке партије Кине означен је као стратешки циљ дипломатије. Управо је овај пројекат финансијски и инфраструктурно оријентисан ка европском простору, чије се западне државе (пре свега) сматрају деценијским савезницима САД. Својеврсна конфронтација, каква је постојала између САД и СССР-а, данас Русије, јавља се и између Америке и Кине, при чему се савремено „бојно поље" не ствара само на светском економском тржишту већ и у војној сфери. У погледу војних доктрина и дефинисања опасности не само ове две већ и многе друге државе акценат све више стављају на неоружане сукобе, који се могу водити у такозваном сајбер простору. Конфликти међу државама добиће нове форме и сајбер операције биће њихов важан сегмент (Lewis 2015: 16). И поред енормних издвајања у војне буџете и производње савременог оружја, отворени ратни сукоб ипак представља велики ризик чак и за најмоћније државе – уместо класичних борбених дејстава, којима се губе бројни људски животи и који изискују велике финансијске издатке, много учинковитији биће такозвани сајбер напади и ратови. Иако милитантне претње константно упућују многе земље, пре свега Русија, САД, Кина и Северна Кореја,

нарочито реферишући на локалне и регионалне интересне сфере, отворене сукобе свакако избегавају. Национална снага данас се све више показује у сајбер простору.

Сајбер напади

Сајбер нападе можемо посматрати као средство за постизање одређених економских, политичких или војних циљева, што подразумева употребу специфичних алата, али и поседовање знања и специфичних вештина. За спровођење ефикасног сајбер напада потребно је знање, технологија и одабир тренутка, када ће и како напад на непријатељски систем произвести жељене ефекте, било да се ради о поремећају рада неке инфраструктуре или сервера, преузимању/крађи података и тајни или сајбер шпијунажи. Зависно од коришћених метода напади могу бити спроведени у циљу преузимања контроле над апликацијама, (зло)употребе или оштећења података, или, пак, водити делимичном или потпуном уништењу поставки система. Готово сви сајбер напади, без обзира на то да ли су дело појединаца, група или саме државе, врше се због неких од следећих циљева:

- онеспособљавање противничких система и преузимање даљинске контроле над њима;
- крађа, брисање или измена важних и тајних података;
- пресретање комуникације и размене информација;
- саботажа, фишинг и/или компромитовање привредних и војних индустрија и организација како би се стекла стратешка предност над противником.

Влада САД је 2011. године потенцијалне сајбер нападе на критичну инфраструктуру декларисала као акте сличне ратним акцијама и дала себи за право да на њих одговори и традиционалним кинетичким нападом на државу са чије је територије атак потекао (Valeriano and Maness 2014: 348). Таквих оружаних одговора на сајбер нападе до сада није било, но сајбер простор је у стратешким и доктринарним документима не само САД већ и других великих сила одавно попримио статус петог борбеног простора, уз копно, ваздух, море и свемир. Битке у сајбер пољу данас се сматрају регуларним методама у конфликтима. Џозеф Нај је, у том смислу, као актере сајбер конфликата апострофирао владе, организације и појединце[55].

[55] Опширније видети: Nye 2011: 18-38.

Сајбер простор је од есенцијалног оперативног значаја у модерном ратовању, војници су од њега у све већој мери зависни, а на стратешком нивоу слабости и снаге једне државе на овом пољу могу се искористити у сврху одвраћања или утицања на баланс моћи (Magnus 2011: 2). Оспособљеност држава за активности у сајбер простору одвраћа друге од потенцијалних напада, омогућава вршење сајбер шпијунаже – војне или економске – и стицање предности у тим сферама. Једна од посебних „погодности" јесте то што сајбер нападе не морају изводити званичне државне институције већ недржавни ентитети, чиме се, из перспективе међународног ратног права, избегава одговорност државе за напад.

Долажење у посед информација које су власништво неке корпорације (пословне тајне) често је од кључног значаја у спречавању производње и дистрибуције робе или услуге коју њена конкуренција не може да произведе довољно квалитетно (Akoto 2021: 2). Што је објект напада сложенији и стратешки важнији (попут великих корпорација, владиних тела, војних индустрија), ефекат успешно спроведеног сајбер напада је значајнији – не само у смислу остваривања стратешке предности над противником (војне, економске, политичке) већ и у пропагандном. Успешно изведен напад показује да постоје рањивости и најзаштићенијих ИКТ система, али и изазива забринутост, некада и панику у јавности (о чему, на пример, сведочи DDoS напад на Естонију 2007. године). Луис (2018) сматра да је мало вероватно да би водеће земље света извршиле сајбер нападе на финансијску инфраструктуру, с обзиром на то да у глобалној ери такав напад може имати негативан ефекат по целокупно светско тржиште и берзе.

Конфликт САД и Кине у сајбер простору

САД су у погледу традиционално схваћене војне моћи неоспорно испред Кине, вероватно и у технолошкој оспособљености за извођење офанзивних сајбер операција. Међутим, њихове одбрамбене могућности у сајбер простору нису на задовољавајућем нивоу.

Слабост америчке одбране у сајбер простору огледа се, прво, у немогућности да искључи интернет, друго, у израженој међуповезаности критичних инфраструктура (банкарски сектор, финансије, саобраћај, снабдевање енергентима, јавна управа, хитне службе итд.) и, треће, у условљености рада наведених критичних инфраструктура од електроенергетске и телекомуникационе инфраструктуре. За разлику од САД, земље попут Кине, Сирије и Египта имају могућност гашења интернета, што их чини мање рањивима на сајбер нападе, док је Руска Федерација 2019. године донела закон о

интернету којим су успостављена архитектонско-технолошка решења за „нови суверени интернет" који ће бити заснован на другачијим протоколима и који ће Русији омогућити да у случају потребе „пресече" интернет конекције са „остатком света". Овим законом су, између осталог, физичка и правна лица обавезана да дигиталне податке складиште на серверима који се физички налазе на територији Руске Федерације (Савезни закон бр. 90-ФЗ 2019).

Управо због слабости америчке одбране Кина је претходних година успела да изведе бројне успешне сајбер нападе на САД. Привредни и војни раст Кине био је запажен, али очигледно потцењен када је бивши секретар за одбрану САД Роберт Гејтс 2007. године изјавио да ову земљу не види као стратешког непријатеља, већ као респектабилног партнера, с једне и респектабилног конкурента, с друге стране (Lowther et al. 2013: 21). Међутим, само неколико година касније ова слика сарадње и „здраве" конкуренције значајно се мења, и то управо, и прво, на пољу сајбер простора. Војна стратегија Кине назначава да је оспособљеност у сајбер сфери оно у шта Народноослободилачка армија (ПЛА) треба да инвестира и да обилато користи (Magnus 2011: 4). Оспособљеност за вођење сукоба у сајбер простору Кина види као моћну алатку асиметричног ратовања и средство за спровођење стратегије одвраћања. Аутори посвећени проблематици односа САД и Кине истичу да је потребно разумети да се, пре свега, филозофија и поглед на свет ове источне земље и земаља Запада дијаметрално разликују. Пре него што се крене у интерпретацију њихових активности и дугорочних амбиција, морају се разумети основна културолошка начела стратегије Кине (Lowther et al. 2013: 24). Ова група аутора истиче да су утицај хеленске филозофије, јудаизам и хришћанство, вођени америчком „изузетношћу" и искуствима у ратовима, обликовали стратегију САД која подразумева директно суочавање са непријатељем, велика борбена дејства и потпуно уништење противника. С друге стране, стратегију Кине граде филозофија Конфучија, моралност и метафизика, класична војна дела кинеских аутора и национализам. Ова учења Кину воде дефанзивним/одбрамбеним активностима, не првенствено нападачким. Позивање на учења древне Кине данас имају утемељење у чињеницама да ова земља своје унутрашње и спољне интересе није градила и бранила војном силом и нападачким ратовима. Међутим, како се глобални, али и унутардруштвени изазови мењају, и сама Кина почиње да спроводи експанзионистичке мере, управо кроз пројекат „Појас и пут", али и кроз покретање асиметричних ратова. Иако је претраживач Google „изашао" из Кине 2010. године као одговор на нерешена питања крађе ауторства, статистички подаци показују да употреба интернета ипак расте – становници 60 највећих градова Кине проводе 70% свог

слободног времена претражујући управо веб-странице корпорација и влада западних земаља, пре свега америчких[56]. Фебруара 2007. гласило Министарства одбране Кине *China National defense News* дефинисало је сајбер бојно поље као употребу мреже, технологије и метода у борби за информације које ће дати предност на пољу политике, економије, војних питања и технологије (Iasiello 2016: 46). Након обелодањивања неколико кинеских сајбер напада, амерички званичници мењају помирљив тон и указују на ову земљу као на главну опасност по њихов виртуелни простор.

Америчка компанија за сајбер безбедност „Mandiant" објавила је 2013. године извештај у коме је кинеску војску оптужила за сајбер шпијунажу[57]. Након објављивања извештаја амерички званичници, укључујући и тадашњег председника Обаму, почињу јавно да оптужују Кину за спровођење сајбер шпијунаже (Iasiello 2016: 48). Бивши директор Америчке националне агенције за безбедност (NSA) генерал Кит Александер изнео је процену да је сајбер шпијунажа нанела штету САД у износу од 338 милијарди долара, истичући да је не потпуно, али у највећој мери та активност потекла од Кине[58]. Новински извештаји објављују да су кинески хакери такође „украли" на десетине података о америчком војном програму, нарочито о ракетном систему Patriot и ратним бродовима морнарице (Segal 2013: 39).

Кинеске власти препознале су да даљи економски раст могу остварити експанзијом својих идејних инфраструктурних и финансијских решења изван непосредног територијалног окружења, а такав уплив свакако носи са собом и политички утицај на глобалном нивоу. Такав финансијски и војно-политички уплив САД су остварile управо на тлу Европе након Другог светског рата. Америка, и поред бројних рецесија и војнодипломатских ризичних иступа по свету, и даље представља најмоћнију силу, али јој тај положај делимично може преузети Кина, и то не агресивном милитаризацијом и оружаним сукобима, већ управо преузимањем идеја, патената и интелектуалне својине путем сајбер операција. У прилог томе говори и званична објава америчке фирме за производњу соларних панела „SolarWorld", која је објавила губитак од 120 милиона долара узрокован сајбер шпијунажом пословних тајни ове компаније од

[56] Опширније видети: Atsmon and Magni 2010.

[57] APT 1: Exposing one of China's Espionage Units, dostupan na: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (Mandiant, 2013).

[58] Опширније видети: NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History', Foreign Policy: The Cable, 09. 07. 2012. dostupno na: http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatesttransfer-of-wealth-in-history/ (Alexander, 2012).

стране кинеских произвођача 2012. године (Akoto 2021: 2). Један од главних начина борбе против америчке надмоћи за Кину јесте да уплови у сајбер операције у циљу да преузме информације из дипломатских, економских и сектора одбрамбене индустрије (Isasiello 2016: 58). Основни циљеви Комунистичке партије, која суверено влада Кином, јесу одржање режима, државног и друштвеног уређења, али и, како је то у „Појасу и путу" дефинисано, стратешким постављањем ове земље за регионалног и једног од глобалних светских лидера. Један од начина постизања тог циља јесте и перфидна шпијунажа у сајбер простору. С друге стране, САД су такође извршиле више сајбер напада на Кину и ове две земље се тренутно сматрају највећим ривалима у сајбер сфери. О интензитету ових напада и степену антагонизма између ових држава довољно говори иницијатива Хенрија Кисинџера за спровођење новог детанта – сајбер детанта (Putnik and Milošević, 2018).

Ривалство се може дефинисати као дугорочни конфликт кога карактерише трајније непријатељство (Valeriano and Maness 2014: 349). Оно може бити и компетиција, али и анимозитет и сукоб. Желећи да утврде највећа ривалства управо у сајбер сфери, Валериано и Манес спровели су опсежно истраживање сајбер напада у свету, иза којих јавно или прикривено стоје државе. Резултати су показали да поред познатих конфликата између Русије и Украјине, Пакистана и Индије, као и Израела и Ирана, прво место заузимају ипак Америка и Кина – ове земље учествовале су у 53 инцидента у сајбер простору, највише једна према другој, а најчешћи иницијатор инцидената и спорова била је Кина[59].

Закључак

Односи САД и Кине прешли су пут од такмичења и чак сарадње до отворених оптуживања за сајбер шпијунажу и наношење економске штете. С обзиром на то да у временима које, сведоци смо, карактерише неизвесност коју може изазвати и изненадна пандемија, улог у одржању и увећању финансијске и политичке моћи постаје све већи. Након ужасних људских губитака и разарања након Другог светског рата улог моћи водио је трци у наоружању (конвенцијалном и нуклеарном), енормној производњи оружја и оштрој медијској пропаганди, па и прогонима и убиствима неистомишљеника. Да ли садашње ривалство САД и Кине води сличном сценарију, у коме ће се методе, овога пута сајбер ратовања, усложњавати и имати све штетније последице по државе и друштва? Да ли треба

[59] Опширније видети: Valeriano and Maness 2014: 347-360.

размишљати о сценарију у коме заоштравање конфликата може водити извођењу сајбер напада који би дестабилизацијом или урушавањем неке критичне инфраструктуре изазвали енормне последице, не само по власти и корпорације већ и по здравље и животе људи? САД, за разлику од Кине, праве извесну разлику између сајбер шпијунаже у подручју политике и војне индустрије и напада који су усмерени према привреди. Мајкл Хауден, бивши директор Агенције за националну безбедност (NSA) и Централне обавештајне агенције (CIA), изјавио је: „Ви шпијунирате, ми шпијунирамо, али ви сте једноставно украли нешто што нисте смели" (Faesen et al. 2020). По угледу на договоре Америке и Русије о смањењу нуклеарних бојевих глава и трке у наоружању, ове две и још 23 друге земље (укључујући и Кину) оформиле су 2018. године Групу владиних експерата за унапређење одговорног понашања држава у сајбер простору у контексту националне безбедности. Једна од најзначајнијих декларација ове групе јесте да државе не би требало да спроводе сајбер нападе на критичну инфраструктуру друге државе у време мира, као и да пружају уточиште сајбер криминалцима који врше нападе на друге државе. Разматрање ове проблематике и колективно јавно помирљиво иступање можда указују на повећање свести о озбиљности сајбер напада и њихових последица. Међутим, и у овом случају, као што је то било и са многим другим споразумима, све може остати само на прокламованој доброј вољи, с обзиром на нарастајуће националне безбедносне изазове у XXI веку и потребу за очувањем државне стабилности и социоекономског стања у друштву, упркос глобалним проблемима.

Библиографија

Савезни закон бр. 90-ФЗ, доступно на: http://publication.pravo.gov.ru/Document/View/0001201905010025

Akoto, William. 2021. „International trade and cyber conflict: Decomposing the effect of trade on state-sponsored cyber attacks". *Journal of Peace Research* 1-15/na internetu: 58 (5): 1083-1097.

APT 1: Exposing one of China's Espionage Units, Mandiant, доступно на: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Atsmon, Yuval and Max Magni. 2010. „China's Internet Obsession". *McKinsey Quarterly* 3:1-3.

Axelrod, Robert and Rumen Iliey. 2014. "Timing of cyber conflict". *Proceedings of the National Academy of Sciences of the United States of America* 111(4): 1298-1303.

Faesen, Louk, Tim Sweijs, Alexander Klimburg, Conor MacNamara and Michael Mazarr. 2020. *Responding to Chinese Economic Espionage*. Hague: Hague Centre for Strategic Studies.

Hjortdal, Magnus. 2011. „China's use of cyber warfare: Espionage meets strategic deterrence." *Journal of Strategic Security* 4(2):1-24.

Lewis, James Andrew. 2018. *Rethinking Cybersecurity*. Washington D.C.: Center for Strategic and International Studies (CSIS).

Lowther, Adam, John Geis, Panayotis Yannakogeorgos, and Chad Dacus. 2013. „Chinese-US relations: moving toward greater cooperation or conflict?" *Strategic Studies Quarterly* 7(4): 20-45.

NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History', Foreign Policy: The Cable, 09.07.2012, доступно на: http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatesttransfer-of-wealth-in-history/

Nye, Joseph S. 2011. „Nuclear lessons for cyber security?" *Strategic Studies Quarterly* 5(4): 18-38.

Putnik, Nenad and Mladen Milošević. 2018. Trends in Peace Research - Can Cyber Détente Lead to Lasting Peace? In: *Handbook of Research on Examining Global Peacemaking in the Digital Age*, edited by B. Cook, 1-19. Hershey: IGI Global.

Segal, Adam. 2013. „The code not taken: China, the United States, and the future of cyber espionage." *Bulletin of the Atomic Scientists* 69(5) : 38-45.

Valeriano, Brandon and Ryan C. Maness. 2014. „The dynamics of cyber conflict between rival antagonists, 2001–11." *Journal of Peace Research* 51(3): 347-360.

US-CHINESE STRATEGIC RIVARLY IN CYBERSPACE

Nenad Putnik

Abstract:

In recent years, China has significantly influenced the reshaping of international relations and has shown the greatest expansion of foreign policy and economic goals. Cyberspace is of essential operational importance in these activities, as well as in modern conflicts, especially in asymmetric warfare. In cyberspace, the biggest rivalry today is between the United States and China. This paper presents research that confirms this, as well as theoretical approaches to the relations between the two countries, which explain the causes of the simmering conflict between them. The current philosophy of cyber conflicts and the ways of their manifestation are described in this article, which can be the basis for further detailed analyzes, bearing in mind that cyberspace has acquired strategic importance for the manifestation of antagonisms between great powers.

Key Words:

Conflicts, cyberspace, cyber-espionage, US, China