

# 10

► љићања

## О САЈБЕР РАТУ И РАТНИЦИМА

„дигитална коцка“  
је бачена

**С**ветла се гасе, вода престаје да тече, возови искачу из шина, банке остају без података, авиони падају с неба, улицом влада руља, људи гину док идентитет нападача остаје тајна.“ Свакодневно ратује свако са сваким и свако против свакога на поприштима с краја на крај планете. Да ли је „дигитална коцка“ већ бачена или није?

За Гаја Јулија Цезара, храброг римског војсковођу и потоњег властодршца, поуздано зnamо да је то учинио и прегазио малу реку Рубикон. Човечанство је без објаве закорачило у Трећи светски рат, у чијим се окршајима гине до последњег бајта! (Бајт представља један знак, као што су слово, цифра или интерпункција.)

Магазин „Економист“ је 2010. на корицама крупним словима исписао „Сајбер рат“, уметнувши иза атомску печурку да читалац не остане у недоумици. Насупрот томе, култни часопис „Вајред“ је обзнатио да предстоји жестока битка за душу интернета „ако се настави са сејањем страха и пометње“. Кome се приволети?

Доскорашњи челник ЦИА (Централна обавештајна агенција), Леон Панета, почетком 2011.

упозорио је на следећи амерички Перл Харбур у сајбер (кибер) простору, девет година након предвиђања познате РАНД корпорације да „сајбер рат долази“.

Томас Рид, професор с Краљевског колеџа у Лондону, чијим смо живописним описом започели казивање, изјавио је пре две године да је то уобразиља која никада неће постати збиља. Највећи број напада у привидним (виртуелним) свето-

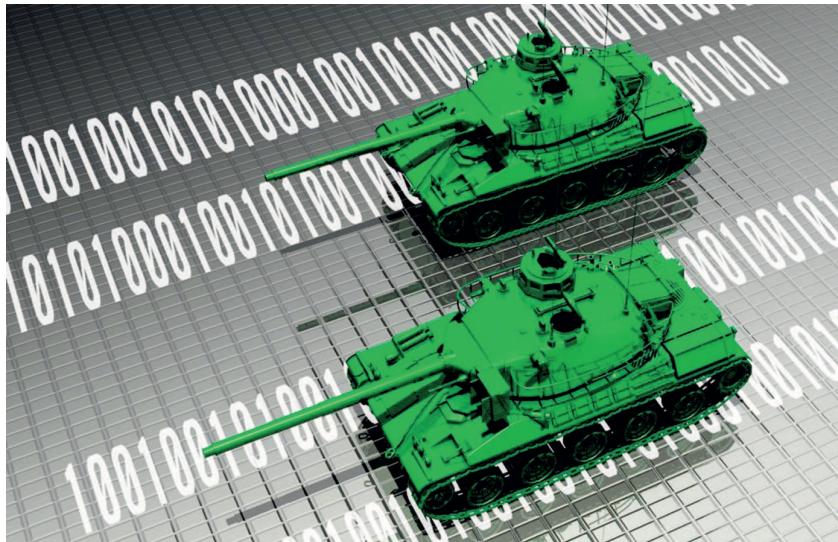


Томас Рид

вима су, наставља он, обичне подвале иза којих стоје овејани преваранти. Саботажа и шпијунажа постоје, али никада нису прерасле у ратовање. И нема доказа да је на електронском бојном пољу изгубљен бар један људски живот. Терористи су користили интернет само за пропаганду и ништа више, а себе су жртвовали у самоубилачким препадима.

Шта је са иранским постројењем за обогаћивање уранијума у Натанцу, наводно првој победи у сајбер ратовању, које су онеспособили израелски и амерички програмери злочестим рачунарским првићем „стакснетом“ (Stuxnet)?

Није српски народ без разлога сковоа крилатицу „Где има дима, има и ватре“. Зашто да бауљамо задимљеним пределима привидне стварности, ако можемо да се позовемо на тумачење проф. др Радомира Михајловића из Њујоршког института за технологију: „Сајбер простор је простор



Бојно поприште у рачунарима

## Милиони жртава, ниједан мртав!

Светски сукоб је 1993. најавила америчка РАНД корпорација, прилично упућена у војна збивања.

Битке се бију до последњег бајта у сваком рачунару с краја на крај планете, умреженом или неумреженом.

Доскорашњи први човек ЦИА упозорио је да Америци прети нови Перл Харбур, а Србији?



Радомир Михајловић

са свим рачунарским машинама и програмима, умреженим и неумреженим“. Без пасоша и граница, то је савршено царство за све оне који желе да незаконито стекну новац, преотму нечије личне податке, украду пословне и државне тајне.

Наш саговорник је у различитим академским звањима предавао на многим универзитетима у свету и у земљи. Бави се кибернетском (сајбер) безбедношћу дуже од десет година. Докторат је одбранио на Политехничком институту Њујоршког универзитета, где је имао прилике да учествује у пројектима „Рата звезда“.

**1. Биће да је ненадмашни Никола Тесла наслутио сајбер рат. Како изгледа овај нејављени обрачун, назван Трећим светским ратом?**

Тесла је, свакако, ненадмашан, а предвидео је да ће будуће генерације људи ратовати помоћу 3

контролисаних интелигентних уређаја. Он је 1898. у Медисон сквер гардену у Њујорку практично извео прву бежичну комуникацију и приказао први дрон (беспилотна летелица), најављујући, по његовим речима, епоху телаутоматизације. Далеко пре свих предвидео је технолошко ратовање. Моје је мишљење да је Трећи светски рат информатички и да се само неке од операција одвијају и одвијаће се у сајбер простору. Да будем одређен, Трећи светски рат је започео хладним ратом и није завршен тријумфом Роналда Регана и прослављеним речима у Берлину: „Господине Горбачов, срушите овај (Берлински) зид“. На рушевинама Берлинског зидаје информациски и информатички рат притисака и претњи физичком силом настављен.

Сајбер простор је нови правац надметања у коме су се, по свему судећи, Руси и Кинези за сада боље снашли. Руси су победили у интелектуалном одмеравању, а Кинези у индустријској шпијунажи и копирању резултата врло скупих развојно-истраживачких пројеката, углавном финансиралих од америчких компанија и америчке државе. Многи указују на то да Америка успешно води Трећи светски рат на свим пољима, али не и у сајбер простору.

## 2. У окршајима се гине, песнички казано, до последњег бајта. Која се оружја користе? На којим попрштима се битке воде?

Честе алармантне вести указују да се ратна попришта и сукоби међу војним силама померају из физичког у логички простор, уоквирен у сајбер суперпростор. Наместо да грувају топови и да се крстареће ракете провлаче планинским гудурама и булеварима метропола, пакети бајтова пробијају одбрамбене „огњене зидове“ и праве хаос на непријатељским рачунарима (серверима). У шали бих питање малчице променио: битке се не воде до последњег бајта, већ до последњег слога; до последњег пакета бајтова, можемо да кажемо до последњег килобајта.

## 3. Леон Панета, доскорашњи шеф ЦИА, најавио је следећи амерички Перл Харбур у сајбер простору. Сматрате ли ово упозорење сувише злослутним?

Леон Панета је ову бомбастичну изјаву дао да би убрзо одлуку америчких законодаваца да се што пре крене са улагањем новца у сајбер одбрамбене системе. Што се тиче Перл Харбура у верзији 2, такав догађај је апсолутно немогућ и у физичком и у логичком простору. Ту бих цитирао недавну изјаву руског председника Владимира Путина који је, отприлике, рекао да је сваки напад на НАТО или САД могућ само у сновима лудака. Ни будном лудаку таква одлука не би пала на памет. Из овакве изјаве некима се чини да стоји мирољубива политика Русије, а ја бих рекао да је у питању немерљива војна супериорност Америке у односу на цео свет, на све земље заједно. Посебно је изражена у сајбер простору. Упозорење Леона Панете није злослутно, већ на неки начин поучно. Сајбер Перл Харбур је немогућ, али су мањи напади више него могући.

## 4. Није ли то разлог што су САД на чело Сајбер команде поставиле генерала Кита Александера, директора Националне агенције за безбедност?

Генерал Кит Александер је 2010. добио четврту звездицу када је постављен за првог команданта Сајбер команде. Заменио га је адмирал



Пролаз у сајбер свет

„Никола Тесла је далеко ће предвидео свих џревида шехнолошко ратовање“, стајара проф. гр Радомир Михајловић, из Њујоршког институута за шехнолођу, који се сајбер безбедношћу бави дуже од десет година



Кит Александар

Мајкл Роцерс 2014, а сада је вршилац дужности (ВД команданта) генерал пуковник Џон Дејвис. Пре доласка на чело Сајбер команде, Кит Александер је био директор Националне агенције за безбедност (NSA). С таквим искуством био је убедљиво најкомпетентнији човек за место главнокомандујућег. Своју компетентност је у више наврата јавно демонстрирао. Можемо да кажемо да је он покренуо обједињавање информационих система свих индивидуалних војних родова, војних, цивилних и приватних информационих система ради што успешније одбране од могућих напада и, по његовим речима, што успешнијег противнапада. Слажем се с поруком у питању да је важност сајбер одбране јасно одсликана у избору најбољег могућег човека.

## 5. Ни друге земље нису оклевале. Има ли потврде да су први успешни напад извели Израелци онеспособивши иранско нуклеарно постројење?

Поред САД, колевке интернета, одакле је сајбер простор почeo да се шири, све развијеније и средње развијене земље настојe да развију безбедносну инфраструктуру у сајбер простору. Израел је по свим мерилима једна од најактивнијих земала у офанзивно-дефанзивним операцијама у сајбер простору. Увео је изванредно образовање у свим узрастима, а једно је земља с највећим бројем новооснованих високотехнолошких компанија по квадратном километру. У савршеној војној синхронизацији са свим земљама НАТО-а и с врхунском глобалном обавештајном мрежом, Израел је био способан, и још јесте, да изведе сајбер напад невиђене убојитости. У случају одбране од будућег могућег нуклеарног напада из Ирана, у јуну 2010. је, највероватније, преко физичког оперативца (тзв. сникер-нет) убацио вирус „стакснет“ у рачунарску мрежу која је контролисала иранска нуклеарна постројења. Напад је био и успешан и неуспешан. Разлог неуспешности огледа се у одмазди иранских сајбер снага које су објавиле програмски код „стакснет“ вируса и тако омогућиле многобројним злонамерним хакерима да се тиме евентуално послуже. Нема веродостојних потврда да су напад „стакснет“ црвом (сајбер црв је вирус који се сам умножава и шири), извели Израелци, или све околности на то указују.



Сајбер свет

## **6. Амерички обавештајни пребег Едвард Сноуден тврди да Национална агенција за безбедност злоупотребљава поједине компаније за своје прљаве работе. Да ли је то тачно?**

Едвард Сноуден највероватније није амерички обавештајац, мада такву могућност не бисмо смели да искључимо. Он је технички специјалиста који је радио за приватну фирму „Буз Ален Хамилтон”, подизвођача радова Националне агенције за безбедност. Пракса да се државни војно-обавештајни радови обављају преко приватних подизвођача кренула је с „хладним ратом”. Данас је нарасла до великих размера, с изгледима да кроз корупцију и недовољну транспарентност начини више штете него користи. Едвард Сноуден је на то указао на један начин који није у потпуном складу са законима САД. По мени је прљава работа не прислушкивање америчких грађана, већ плата од неколико стотина хиљада долара годишње коју је један младић, ка што је Едвард Сноуден, примао без дипломе са, рецимо, МИТ-ја или Станфорда. Најпрљавије је ту расипање позајмљеног новца, с тим се мора прекинути, не само у САД, већ и у свету. А то, свакако, важи и за Србију.

## **7. Ко је у Србији главнокомандујући? Колико је наша земља угрожена?**

Не бих могао да одговорим. Међутим, приметио бих да после катастрофалних губитака у Првом и Другом светском рату и недавног трагичног југословенског грађанског рата, Србија има врло мало тога да изгуби, па је на неки начин мало угрожена.

„Чесће аларманћине вести указују да се раћна Јојришта и сукоби међу војним силама Јомерају из физичкој у лојички Јросћор, уоквирен у сајбер суперјросћор”



Едвард Сноуден

„Сајбер Јросћор је нови Јравац надмешања у коме су се, њој свему судећи, Руси и Кинези за сада боље снашли. Руси су Јобедили у интелекуалном одмеравању, а Кинези у индустиријској шијунажи и којирању резулташа врло скучих развојно-испраживачких Јројеката, углавном финансираних ог америчких комјанија и америчке државе. Мноћи указују на њој да Америка усјешно води Трећи свећски раћ на свим Јољима, али не и у сајбер Јросћору”

„Засјтрашујуће и истинићо јесће ћо да су у џоку расјраве да се војним машинама омогући да аутономно бирају која ће убићи. Могуће је да нас као себи непотребне једног дана претворе у своје гориво или нас, пак, одстране као своје смеће. Страхујем да је у току прерастање латинске „Deus ex machina“ (Бог из машине) у „Deus est machina“ (Машина је бог).”

Смањена величина и сиромаштво су, на неки начин, у овом часу најбоља одбрана. Из података са конференција имам утисак да скромне сајбер одбрамбене снаге постоје. Мој мали допринос томе је подизање свести да је сајбер безбедност важна и у настојању да се уведу последипломске студије сајбер безбедности на Метрополитан универзитету и на универзитету „Никола Тесла“ у Београду. Ту бих додада годишњу конференцију која се, под покровитељством Метрополитан универзитета, одржава седми пут 17. јуна у Београду.

## **8. Испоставља се да је првидни или виртуелни свет постао савршено окружење за крају новца, података, идентитета и државних тајни?**

Сајбер простор омогућује дела и недела која се тешко могу пратити, јер се у овој свеукупној сложености успешно сакривају трагови после криминалних радњи и то инспирише многе да се опробају. Али се не бих сложио да је то окружење савршено. Нови софтверски алати и уређаји све више ограничавају маневарски простор сајбер нападачима.

## **9. У којој мери су поткрепљене оптужбе да из Кине долази највише настрадаја, а да је одмах из Америка која је и најчешћа мета?**

Оптужбе да су кинески хакери веома активни у настрадајима на америчку сајбер територију су, углавном, поткрепљене многобрojним доказним подацима. Мало их занимају политичка и војна питања, првенствено су заинтересовани за индустријске тајне и, као што сам поменуо, за резултате скупих истраживања. Крајом индустријских тајни драстично се обара цена одговарајућег производа, чиме се повећава кинеска компетитивност на светском тржишту. Од овакве врсте настрадаја неопходна је одбрана, како сајбер технологијама, тако и законодавним међународним прописима са којима се, нажалост, врло споро напредује.

## **10. Очекујете ли да ће машине наставити тамо где су људи стали?**

То већ машине увек чине. Помоћу машина видимо што даље и што ситније, можемо да летимо као птице и више од птица, да се крећемо као рибе под водом и преко воде, да рачунамо брже од људи без машина, да једним ударцем убијемо милион људи. Најстрашније, можда, тек наилази. Могуће је да машине постану самосталне и да без нас крену у походе. Застрашујуће и истинито јесте то да су у току расправе да се војним машинама омогући да аутономно бирају кога ће убити. Могуће је да нас као себи непотребне једног дана претворе у своје гориво или нас, пак, одстране као своје смеће. Страхујем да је у току прерастање латинске „Deus ex machina“ (Бог из машине) у „Deus est machina“ (Машина је бог).