ОДБРАНА

Специјални прилог 93

Сајбер ратовање

НЕСЛУЋЕНЕ МОГУЋНОСТИ НОВИХ ТЕХНОЛОГИЈА

„Не могу да се вратим у јуче, јер сам био друга особа тада”

Луис Керол,
Алиса у земљи чуда

Пише Драган МЛАДЕНОВИЋ

НЕСЛУЋЕНЕ МОГУЋНОСТИ НОВИХ ТЕХНОЛОГИЈА

Током историје људи су примењивали различите технике и средства за вођење рата. Они су зависили од развоја и организације људског друштва и односа у њему, али првенствено од степена технологије. Штавише, нове технологије су одувек прву примену имале баш у сукобима и ратовима. Оне нације које су прве овладавале новим технологијама остваривале су стратегијску предност у глобалним размерама. Технологија често драстично мења однос снага. У новијој историји она држава која је поседовала атомску бомбу бивала је заштићена, чак и од великих сила. На исти начин на који је развој технологије и организације у друштвима утицао на вођење рата, тај процес је ишао и у обрнутом смеру, јер су рат и потреба да се осигура безбедност државе утицали на убрзавање развоја технологије. Такав случај је и данас у савременом информационом друштву.

Шта је сајбер ратовање?

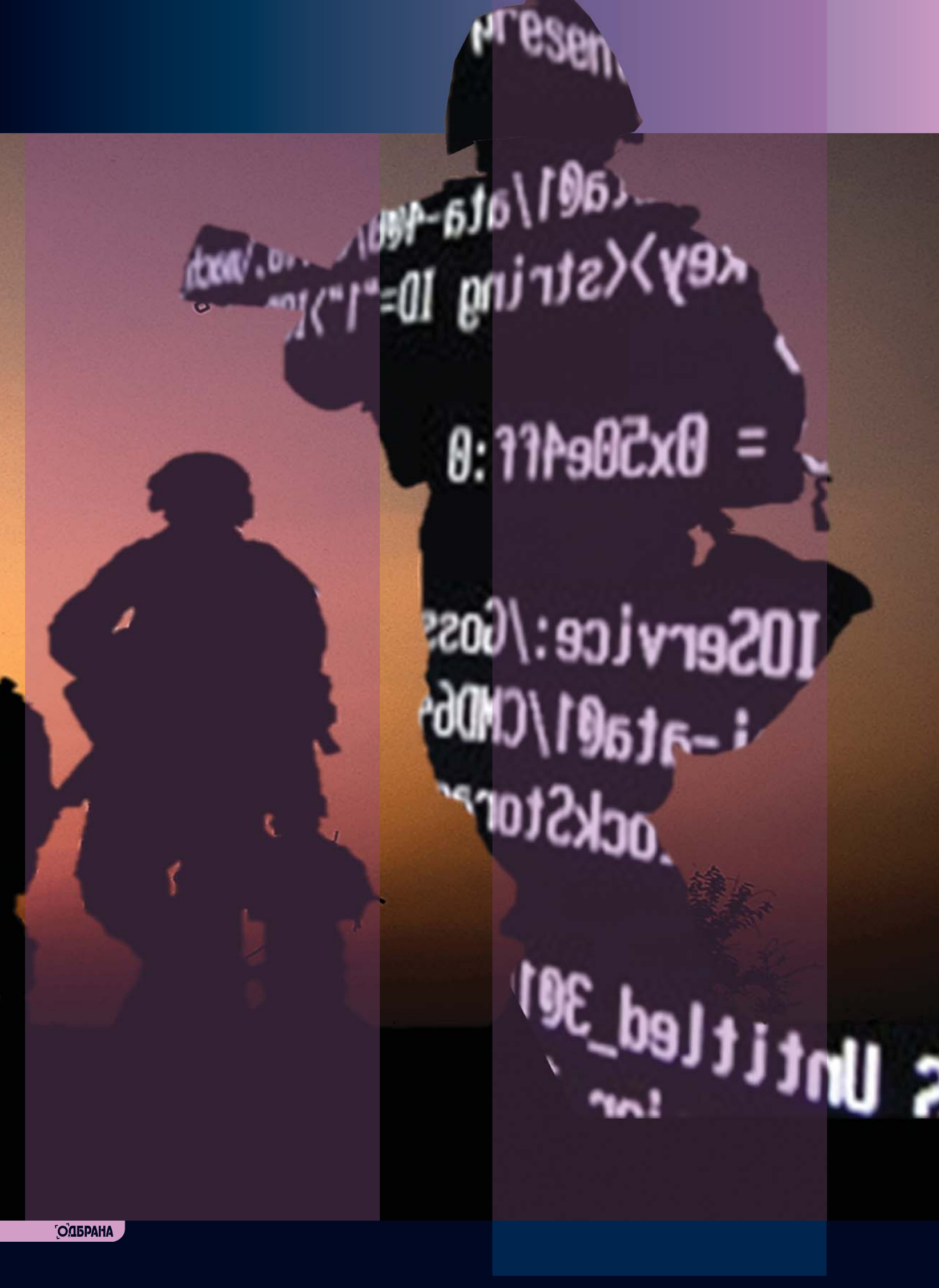
У рату конвенционалним оружјем, мање-више, све је јасно. Употреба тих средстава је националним и међународним прописима ограничена на оружане снаге, које их користе у сврху припреме и вођења сукоба. Прописи међународног ратног права могу се применити на ситуације сукоба између држава или других субјеката међународног права, јер је употреба традиционалне ратне технике углавном отворена и уочљива. Ипак, и у том случају има доста проблема, јер ситуације у којима се дешавају сукоби нису увек јавне и не дешавају се без разлике у ставовима страна у сукобу.

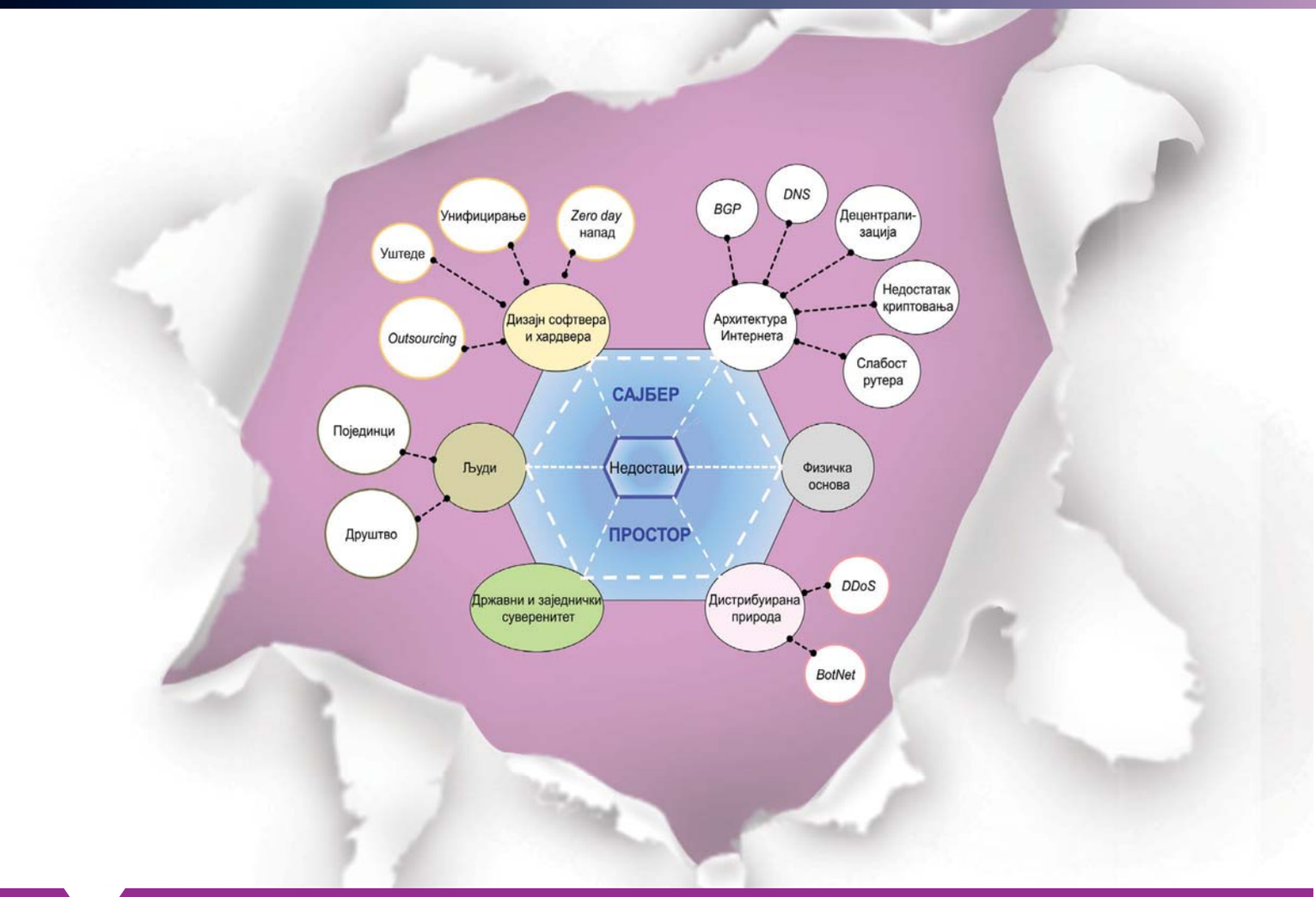
У сајбер рату проблем је знатно компликованији. У њему се за покретање напада, као и за одвраћање и за одбрану од напада, не користи специфична група средстава, која се јасно може разликовати по својим техничким карактеристикама и својствима, већ цело једно технолошко подручје. Међутим, примена тих технологија није карактеристична само за вођење сукоба, већ се иста технологија користи и за мирнодопске потребе. Додатни проблем јесте што предмети тих рачунарских и информационих технологија немају материјални облик, већ се налазе у вештачком подручју – „сајбер простору". Манипулација и рад са тим технологијама се много теже откривају него у случају традиционалних борбених средстава, која постоје у физичком свету и чије дејство је углавном видљиво.

Имајући све то у виду, може се рећи да сајбер ратовање представља вођење сукоба између међународноправних субјеката (што му и даје карактер ратовања) применом рачунарских и информационих технологија, при чему су те технологије примарна средства за напад, одвраћање или одбрану. Све би било јасније када бисмо појам информационих и рачунарских технологија сузили на дигиталне технологије и када бисмо рекли да је сајбер ратовање примена дигиталних технологија за вођење сукоба између држава. Међутим, у апсолутном смислу, то није тако, јер се у оквиру информационих и рачунарских технологија примењују и аналогне технологије, а у будућности је очекивана примена и квантних технологија.

Други начин да се дефинише сајбер ратовање јесте да кажемо да је то вођење сукоба у сајбер простору. И у овом случају постоје нејасноће. Иако неке државе, попут САД, сматрају сајбер простор петим подручјем ратовања, поред копна, мора, ваздуха и свемира, не постоји заједничка, међународно прихваћена дефиниција сајбер простора. Уколико се сајбер простор свеобухватно посматра као електронски медиј у оквиру којег се информације у електронском облику стварају, шаљу и примају, чувају, обрађују, мењају и бришу, онда једноставно можемо рећи да је сајбер ратовање, у ствари, ратовање у сајбер простору. У овом случају потребно је разумети природу сајбер простора и чињеницу да он, иако није материјалан, не може постојати без своје физичке основе, било да је она физички опипљива у случају хардвера, или енергетски уочљива у случају простирања зрачења и електромагнетних таласа у етру.

Може се рећи да је, у технолошком погледу, сајбер простор глобално подручје које постоји у информационом окружењу и које се састоји од технолошки међузависних мрежа информационе инфраструктуре, укључујући телекомуникационе мреже, интернет, рачунарске системе и многобројне уграђене процесоре и контролере. Такође, важно је разумети и појам информационе инфраструктуре, који се односи на целину свих људи, процеса и система који сачињавају сајбер простор, односно остварују утицај на њега. У ширем смислу, сачињавају је просторно окружење (географско или вештачко), енергија, хардвер (полупроводници, процесори, оптички и метални каблови и други уређаји),





Недостаци који омогућавају сајбер ратовање нису садржани само у софтверу, већ у свим елементима сајбер инфраструктуре

софтвер (изворни и компајлерски програми, разне корисничке апликације и драјвери, базе података и друго), мреже (са својим чворовима, везама и топологијама), електронски садржај (саме информације које се крећу и складиште унутар инфраструктуре), људи (програмери, оператери, особље за одржавање и други), као и правила, регулативе и стандарди. То је значајно јер сви ови елементи остварују неки вид интеракције и дејства на процесе и системе у сајбер простору. Такође, ниједан од ових елемената није савршен, односно њихове активности и суштина имају скривене недостатке. Ти недостаци су оно што омогућује сајбер ратовање. Када противник открије недостатак неког актера или објекта у сајбер простору, он га може намерно искористити и остварити циљ сајбер напада.Постоји још једна важна ствар у вези сајбер ратовања, а то је да се рачунарске и информационе технологије, та основна средства и циљеви сајбер ратовања, развијају и мењају изузетно брзо. Пре више од једне деценије сајбер операције су се у доктринама појединих армија сматрале искључивим делом и потподручјем информационих операција. Сајбер деј-

Нептуново копље

Операција „Нептуново копље" – хватање Осаме Бин Ладена у Пакистану 2011. године преношена је у реалном времену од ситуације на терену до *Беле куће* захваљујући рачунарској вези од камера на шлемовима морнаричких фока, који су упали у Бин Ладенову кућу, до мрежних уређаја хеликоптерима и беспилотним летелицама, преко земаљске станице и сателита. Филипидес, грчки антички маратонац – гласник је два дана непрекидно трчао од Атине до Спарте да тражи војну помоћ пред битку Атињана са Персијанцима, а затим од Маратонског поља до Атине, да Атињанима јави велику победу њихове војске над Персијанцима. Учинивши то, пао је мртав. Данас дигиталне информације и мреже омогућавају руководству једне државе да у директном преносу прати акције својих специјалних јединица на другом крају света.

Извор: commons.wikimedia.org

Свет око нас

Најновија студија Уједињених нација из 2013. године је показала да ће до краја ове године, за око 7 милијарди људи на свету, постојати око 6,8 милијарди корисника мобилне телефоније. У време објављивања овог чланка, 91 држава на свету има више мобилних телефона него људи. С друге стране, у овом тренутку, преко 2,4 милијарде људи широм света има приступ интернету. Раст употребе мобилних технологија и интернета је изузетно брз. Сви поменути мобилни уређаји, укључујући мобилне телефоне, добијају приступ интернету и у скорој будућности ће се ова два броја изједначити. Са информационом технологијом наступили су нови односи међу људима. Ми данас живимо у свету у којем више људи има мобилни телефон, него приступ чистом тоалету (само 4,5 милијарди људи га има).

ства су била ограничена на употребу интернета и одређеног софтвера. Како се развија технологија, а свет постаје све зависнији од рачунарских и информационих технологија, природа сајбер ратовања се развија и значајно мења. Такође, мења се и његов утицај на вештачки и природни свет и, самим тим, значај у активностима одбране и безбедности. Људи мењају технологију, која повратно утиче на њихов живот и свет. Мења се и природа сукоба и њихове последице. Уколико нације желе да остваре ефикасну одбрану у таквом, веома променљивом свету, морају и саме да мењају своје стратегије и доктрине безбедности и одбране и прилагоде их новим технологијама, ризицима и претњама.

У поређењу са конвенционалним ратовањем сајбер ратовању је заједничко само то да их планирају и организују државни органи да би остварили властиту политичку вољу. Сајбер ратовање се налази у подручју које не лежи у истој равни са традиционалним ратовањем. Њихове додирне тачке се не налазе тамо где смо навикли да их очекујемо. Њега могу, али не морају, да воде војне снаге; оно може, али не мора, да се води током рата; може, али не мора, да се води против војних снага противника, чак ни против непријатељски настројене државе; на крају, као врхунац изненађења, сајбер ратовање чак не мора да се води против циљева ван властите нације.

Велики број новинара, професионалаца и стручњака у медијима често износи опречне ставове о природи сајбер ратовања. За једне је оно оружје будућности које само што није изазвало катастрофу националних размера, док за друге оно у стварности и не постоји. Уз све то, вероватно ће додатно збунити чињеница да велики број држава у свету интензивно усваја стратегије сајбер одбране и безбедности и развија капацитете за дејства у сајбер простору, а за то одваја своте новца које су веће него годишњи национални буџети већине држава света.

Никада до сада техника и технологија нису били толико блиски људима и човечанству, као у данашње време. Ту револуцију данас остварују рачунарске и информационе технологије, производ рада огромног броја инжењера и научника, којима морамо да одамо захвалност због битног доприноса нашем животу. Ипак, не заборавимо, све главне рачунарске и информационе технологије настале су директно или посредно за потребе одбране и ратовања.

Зашто је то тако? Познати француски теоретичар безбедности и филозоф Пол Вирилио је, пре скоро три деценије, рекао да савремена култура ствара перманентно стање кризе и да је стално усредсређена на безбедност и брзину. Основно питање које она нуди је: ко себе може заштитити брже и боље? Одговор је сукоб који се води у времену уместо у простору. Како он каже: „Физички рат престаје да буде бојно поље, које постаје подручје идеологија, економије и брзине". Практичан пример се види при поређењу времена откривања, идентификације и уништења циља на ратишту од стране америчке Војске, тренутно најумреженије оружане силе на свету. У операцији „Пустињска олуја", 1991. године у Ираку, за овај процес била су потребна четири дана. У „Операцији ирачка слобода", 2003. године, то време је смањено на око 45 минута. Данас време од идентификације до уништења појединачног циља износи свега 10 минута, захваљујући умреженим борбеним системима које чине беспилотне летелице стално задејствоване у ваздушном простору, авиони, сателити и земаљске станице, борци на терену и многобројне информационе мреже. Сутрашњи борбени системи су потпуно аутоматизовани роботи, које не воде људи–оператери, већ их погони софтвер и самостално доноси одлуке о дејствима. Сајбер експлоит (програмски код, скуп података, секвенца команди или било шта друго, што омогућава да се искористи постојање недостатка за нежељено или неочекивано понашање у неком софтверу или хардверу), може се поставити годинама унапред у неки систем, где ће чекати да покрене своје дејство у програмираној ситуацији или на даљинску команду нападача. Константним праћењем активности целокупног човечанства на мрежама може се предвидети понашање појединаца и народа и утицати на њега превентивно. Данашње дејство постаје толико брзо да предвиђа понашање потенцијалног противника и покреће његово онеспособљавање пре него ли он и нападне. Ове операције засноване су на ефекту и последици јединственог дејства, а не искључиво на традиционалном начину планирања, припреме наоружања и војних снага и извођења војних операција.

Преглед усвојених националних стратегија сајбер безбедности		
Аустралија	Стратегија сајбер безбедности	2009
Аустрија	Национална ИКТ стратегија безбедности Аустрије	2013
Велика Британија	Стратегија сајбер безбедности Велике Британије. Заштита и промовисање Велике Британије у дигиталном свету	2011
Европска Унија	Стратегија сајбер безбедности Европске уније: отворени, безбедан и сигуран сајбер простор – JOIN Предлог за директиву Европског парламента и Већа који се односи на мере за обезбеђивање заједничког високог нивоа информационе и безбедности мрежа унутар Уније – COM Извршни преглед процене утицаја	2013
Естонија	Стратегија сајбер безбедности	2008
Индија	Дискусиони предлог о националној политици сајбер безбедности	2011
Јапан	Стратегија информационе безбедности за заштиту нације Ка стабилној и ефективној употреби сајбер простора	2010 2012
Јужноафричка Република	Предлог политике сајбер безбедности Јужноафричке Републике Одлука Кабинета о прихватању	2011 2012
Канада	Канадска стратегија сајбер безбедности. За снажнију и просперитетнију Канаду	2010
Литванија	Програм развоја електронске информационе безбедности за период 2011–2019.	2011
Луксембург	Национална стратегија сајбер безбедности	2011
Малезија	Национална политика сајбер безбедности	
Немачка	Стратегија сајбер безбедности Немачке	2011
Нови Зеланд	Стратегија сајбер безбедности Новог Зеланда	2011
Норвешка	Национална стратегија сајбер безбедности Акциони план	2012
Пољска	Стратегија развоја информационог друштва у Пољској до 2013. Владин акциони план за сајбер безбедност 2011–2016.	2008
Румунија	Стратегија сајбер безбедности Румуније (радни документ)	2011
Руска Федерација	Концептуални ставови о активностима оружаних снага Руске Федерације у информационом простору Доктрина информационе безбедности Руске Федерације	2011 2000
Сједињене Америчке Државе	Међународна стратегија за сајбер простор. Просперитет, безбедности у отвореност у умреженом свету Стратегија Министарства одбране за деловање у сајбер простору	2011
Словачка	Словачка национална стратегија информационе безбедности	2008
Уганда	Национална стратегија информационе безбедности	2011
Финска	Финска стратегија сајбер безбедности Резолуција Владе о Стратегији националне информационе безбедности	2013
Француска	Одбрана и безбедност информационих система – Стратегија Француске	2011
Холандија	Стратегија сајбер одбране Чињенично стање о Стратегији обране Холандије за деловање у сајбер простору Национална стратегија сајбер безбедности. снага кроз сарадњу	2012 2012 2011
Чешка	Стратегија сајбер безбедности Чешке Републике за период 2011–2015. године Акциони план Стратегије сајбер безбедности Чешке Републике за период 2011–2015. Информација о Националној безбедносној агенцији која је основана 19. октобра 2011. као национално тело за сајбер безбедност	2011
Швајцарска	Национална стратегија за заштиту Швајцарске од сајбер ризика	2012

Садашњост и будућност ратовања не зависе само од примене најмоћнијих оружја, већ и од унутрашње и спољне организације. Нуклеарно наоружање није довело до краја ратовања, већ до промене начина на који његови власници ратују. Да је то реалност, показује случај примене рачунарских малвера (злонамерних програма) Стакснет и Флејм, као стратегијске војне операције онеспособљавања нуклеарног програма Ирана као алтернативе авио-бомбардовању и ескалацији регионалног сукоба. Можда изгледа необично што су ово веома асиметрично дејство (највероватније) предузеле постојеће нуклеарне силе, много јаче у конвенционалном и нуклеарном капацитету од Ирана, а не Иран, који је, ипак, од њих војно слабији, али све то иде у прилог чудној и неочекиваној природи сајбер ратовања.

Уколико сајбер операције посматрамо из угла конвенционалног ратовања, јасно је да група хакера која нетремице гледа у екран свог рачунара нема никакве шансе у директном сукобу са тенковском четом. Међутим, такво поређење је смешно и не даје никакав увид у сврху и значај сајбер ратовања. Сајбер ратовање се не посматра насупрот конвенционалног и нуклеарног ратовања, већ као његово надопуњавање, катализатор, део или алтернатива. Као што се од соли не може направити јело, тако и јело без соли није укусно. Значај сајбер ратовања је важан и може бити чак и пресудан. Да би се примењивало, неопходно је упо-

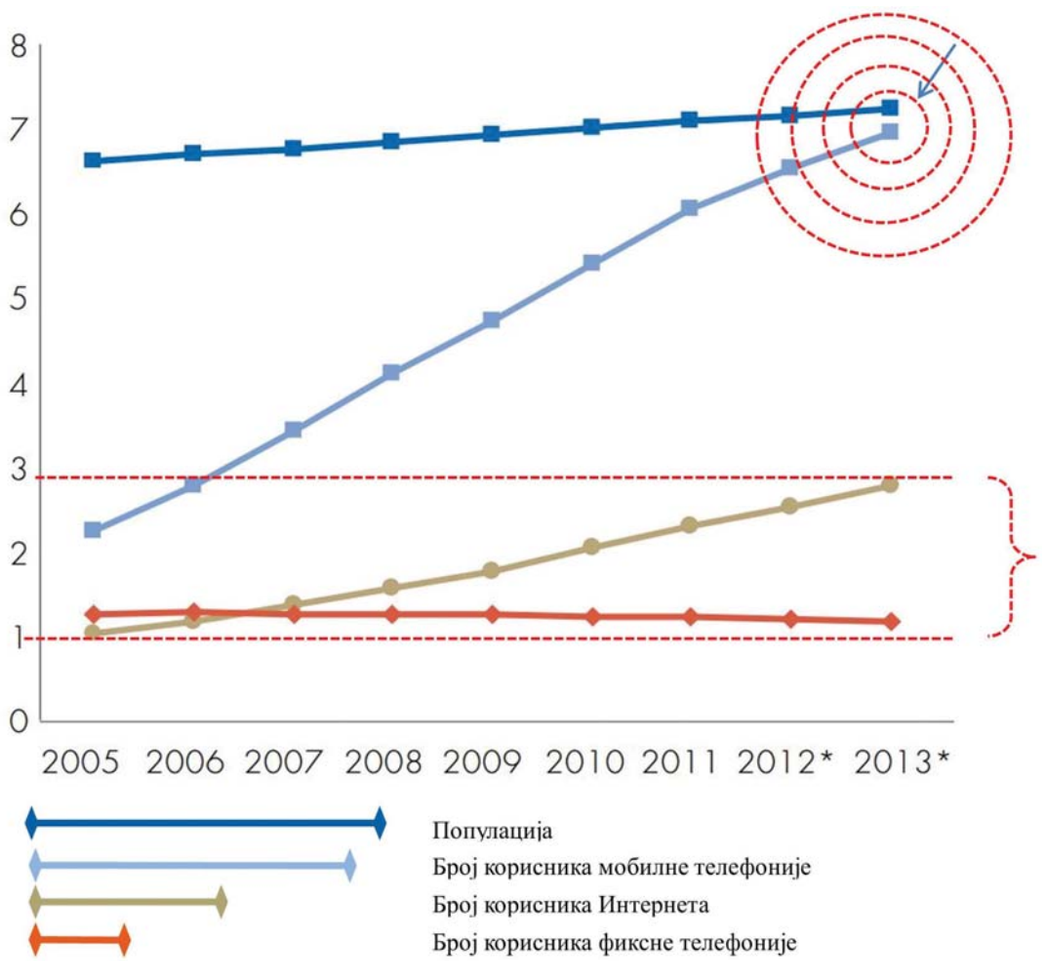
знати његову праву природу, могућности, извор и највероватније исходиште у будућности. Одрицањем од оваквих технологија, само због тога што оне немају опипљиву природу, схватљиву по конвенционалним стандардима, онемогућавамо властитим снагама да створе оперативну и стратегијску предност над противником, и истовремено омогућавамо противнику који више цени сајбер ратовање да ту предност оствари над нама.

Како је све почело?

Све рачунарске и информационе технологије некада су настале за потребе војске и одбране. И идеја о стварању интернета настала је у Сједињеним Државама као одговор на претње хладног рата са Совјетским Савезом. Након што је совјетска влада успешно лансирала први вештачки сателит у орбиту Земље (*Спутњик,* 1957. године), у САД је основана специјализована државна агенција Advanced Research projects Agency (ARPA) чији је задатак био покретање и развој пројеката напредних технологија у име Министарства одбране САД. Велики број технологија које су настале из њених програма остварile су каснији значајан утицај на свет и технолошки развој човечанства. Једна од кључних технологија биле су рачунарске мреже, NLS систем у којем су први пут на практичан начин примењени хипертекст везе, графички кориснички интерфејс, рачунарски екрани и друге периферије, који су и данас незаобилазни део сваког рачунарског система.

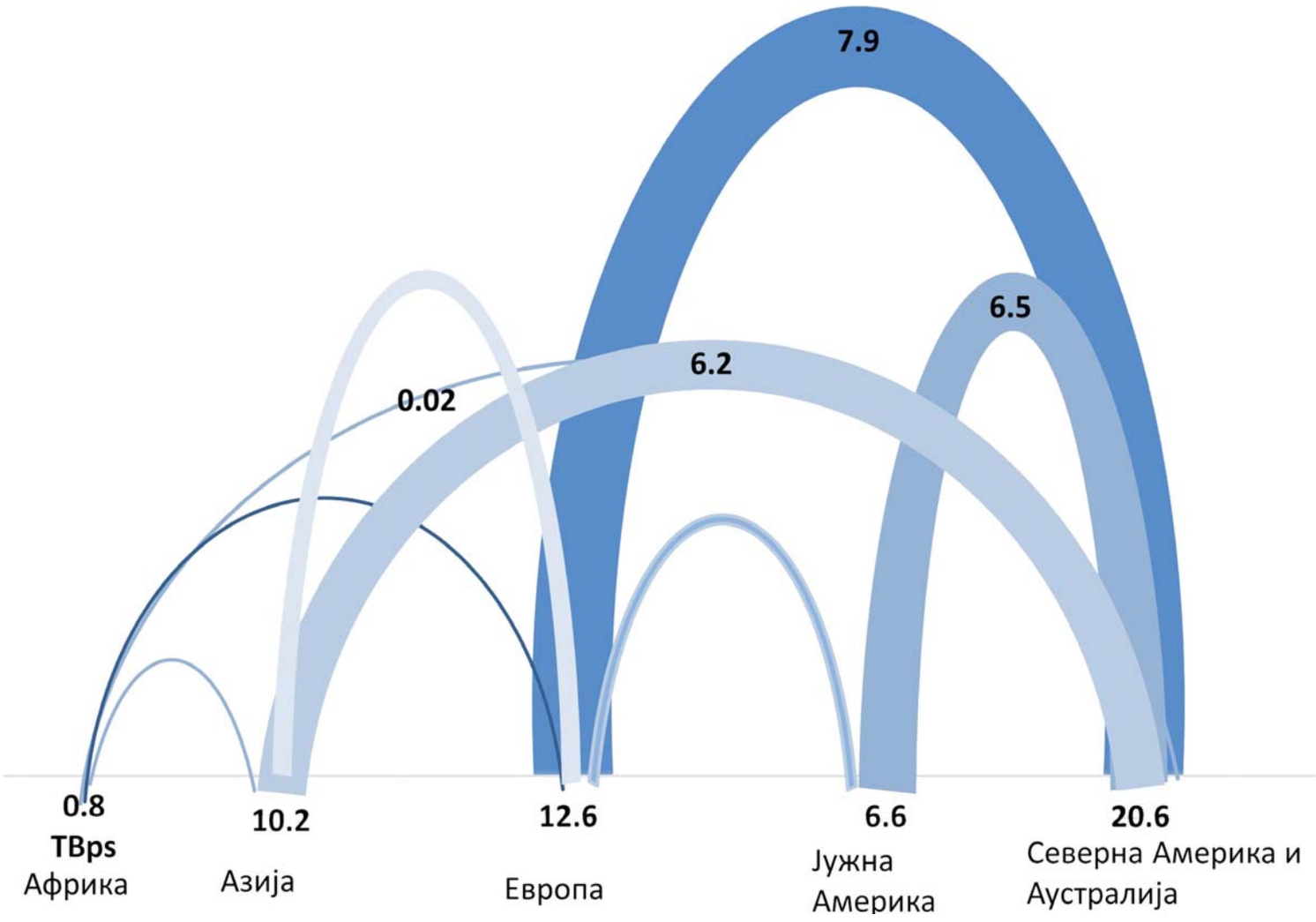
Након што је влада Јапана покренула амбициозан пројекат развоја рачунарске технологије пете генерације и вештачке интелигенције, са тада огромним фондом од неколико милијарди долара, америчка влада је то доживела као јапанску научно-технолошку претњу по америчку технолошку доминација у свету. Због тога је, у периоду од 1983. до 1993. године, покренула и водила Стратегијску рачунарску

Статистички подаци о броју корисника телекомуникационих технологија у свету



Подаци за 2012. и2013. годину су прелимиране процене

Извор: УН, Извештај – Миленијумски развојни циљеви, 2013.



Капацитет укупне пропусне моћи Интернета између континената у терабитима у секунди

иницијативу, програм стварања напредних рачунарских технологија и вештачке интелигенције. У оквиру њега развијани су пројекти попут дизајнирања и масовне производње рачунарског чипа, унапређења хардверске архитектуре рачунара, стварања софтвера за напредну вештачку интелигенцију и други. Дугогодишњи директор овог програма био је истакнути пионир интернета Роберт Кан, који је са другим америчким научником Вином Церфом поставио основне принципе за функционисање интернета. Истовремено, постепено је напуштен преамбициозан и превремен концепт ратовања у космосу, под називом Рат звезда. Тако је, још у време Реганове администрације, док нисмо ни знали шта је виртуелни свет, сајбер ратовање остварило превагу над Ратом звезда.

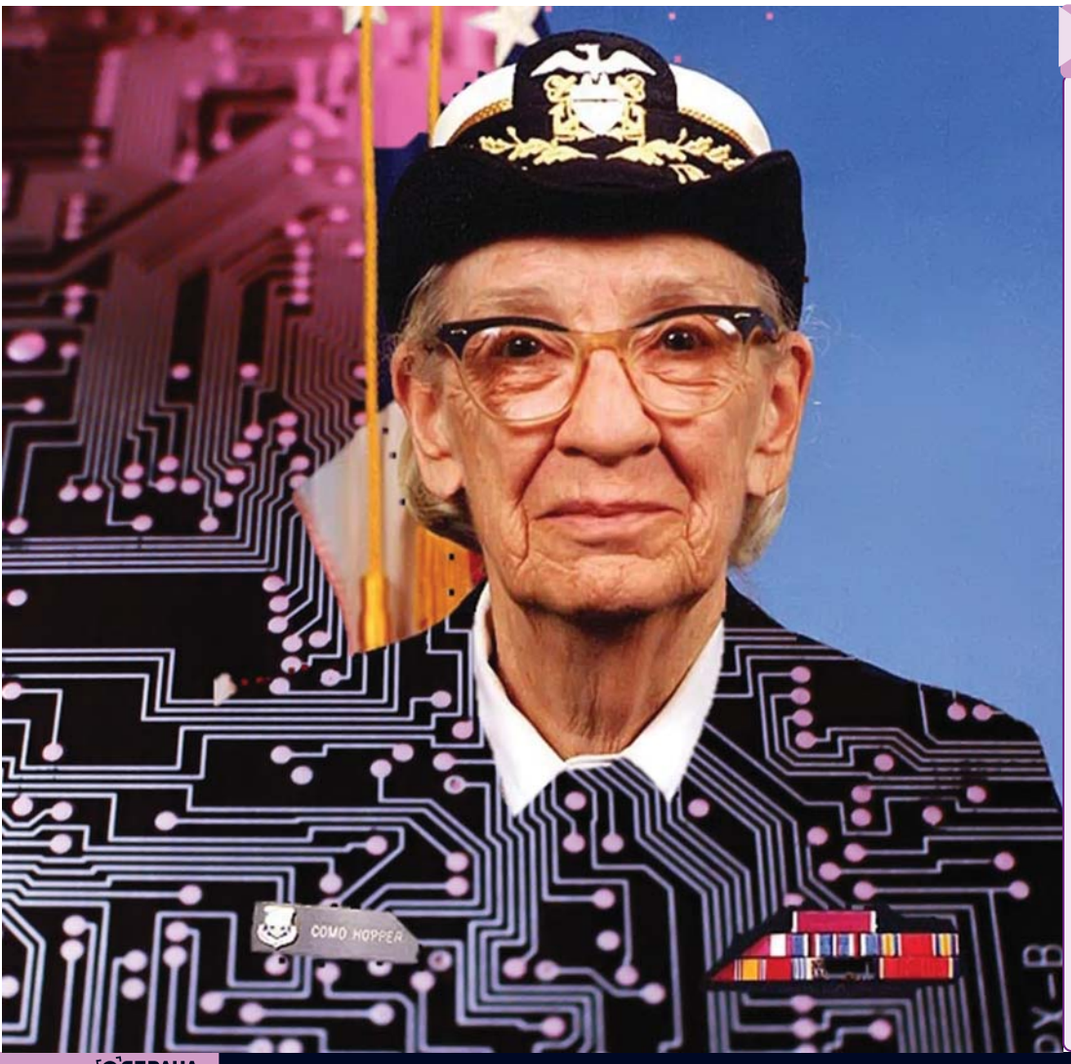
Инжењери и научници који су радили на настанку интернета имали су задатак да створе мрежу која је у потпуности аутономна, децентрализована и еластична. Разлог за ове захтеве био је захтев да се обезбеди поуздана комуникација у случају нуклеарног сукоба. Зато је и данас, у основи, интернет огромна мрежа са децентрализованом архитектуром. Почетни циљеви за настанак мреже над мрежама су се временом веома изменили. Основни савремени захтеви су безбедност и државна контрола (на националном, али и глобалном нивоу). Од мреже свих мрежа, интернет се креће у правцу да постане мрежа свих државних мрежа са примењеним унутрашњим суверенитетима, али и културним обрасцима. То се ради унапређењем безбедно-

сти сервиса на постојећој мрежи, али и изградњом нових мрежа са уграђеним системима безбедности.

А онда су дошле бубе

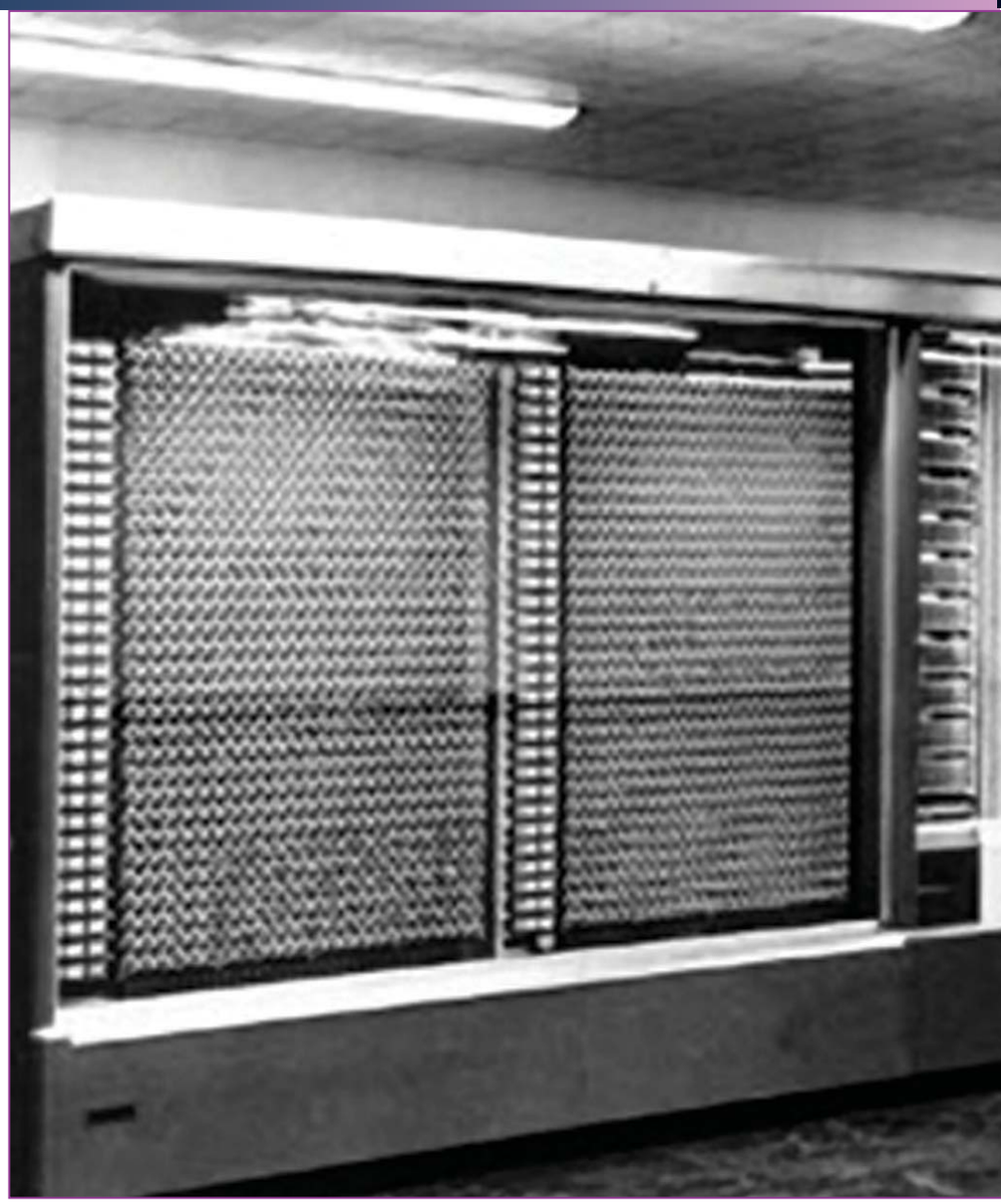
Иако је интензиван раст рачунарских и информационих технологија и глобална зависност човечанства од њих релативно нов феномен, карактеристичан за пар последњих деценија, може изгледати необично да је основа за сајбер ратовање настала истог момента када су се појавиле и дигиталне технологије. Она је била садржана у самим тим технологијама, у форми њихових недостатака којима је могуће манипулисати и тако изазвати уништење система који зависе од тих технологија. Други део услова стекао се у периоду када су информационе и рачунарске технологије постале незаобилазан део света око нас, важан за практично све. Помало је зачуђујуће да сви противници давања значаја сајбер ратовању заборављају на чињеницу да су рачунарска технологија и рачунарске мреже настали у пројектима војске и за потребе војске. За време Другог светског рата вероватно је највећих носилац војних операција америчких оружаних снага била америчка ратна морнарица, с обзиром на географски положај Америке и чињеницу да је ратовала против две велике прекоморске силе – Јапана и Немачке. У време док је рат увелико беснео, америчка морнарица наручила је огромни електромеханички рачунар, сада чувени *Mark I*, који је био намењен за израчунавање сложених балистичких прорачуна за њене потребе.

У комплексном свету савременог програмирања и рачунарства, све врви од грешака. Компајлери претражују грешке у програму и листају их одједном, у скупу. Уколико програм нема грешака, они га конвертују изворно у објектни код, који може извршити машина одвојеним наредбама. Интерпретери проверавају једну по једну наредбу, траже грешке и сукцесивно их преводе у машински код и извршавају. Данас постоји велики број програмских језика. Поједини језици се чак пишу за извршавање појединачних, специфичних задатака. Процес превођења је изузетно сложен и постоји много могућности за појаву грешака, које је, уколико настану, тешко открити. Отежана читљивост оваквих програма посебно је изражена у великим и комплексним пројектима, па се због тога и немогућности практичног конвертовања једног асемблерског кода на другу процесорску



Рачунарска буба

Контра-адмирал Грејс Мари Хупер (1906-1992) је истакнути амерички рачунарски научник, један од првих програмера на чувеном електромеханичком рачунару *Марк I*. Као високи официр америчке војске са најдужим активним стажом у служби, попут војводе Мишића, два пута је пензионисана и враћана у активну службу по посебном председничком указу. Сматрају је „баком програмског језика COBOL“ и творцем првог програмског компајлера. Као изванредан програмер и по духу весела особа, у масовну употребу је увела израз „рачунарска буба“ да означи необјашњиву грешку у програмирању. Једног дана, са сарадницом је пронашла праву бубу, мољца, унутар рачунара и нашалила се да је то разлог што програм погрешно функционише. Контра-адмирал Хупер је позната и по својој изреци: *Најштетнија фраза у језику је да се то одувек радило на овај начин.*



Рачунар Mark I (IBM Automatic Seqence Controlled Calculator – ASCC), претеча модерних рачунара. Био је дугачак 16 метара и тежак 4.500 килограма. Био је први рачунар на свету који је могао да израчунава дугачке низове прорачуна. За то му је трабало 765.000 појединачних компоненти, укључујући осам стотина километара каблова, 3 милиона конектора, на хиљаде релеја, вишеполних прекидача, калема и других компоненти. Имао је 60 сетова по 24 прекидача за мануелни унос података и могао је да запамти свега 72 броја дужине 23 децимална места, док су му за дељење два броја требале 15.3 секунде, а за израчунавање логаритамске или тригонометријске функције више од једне минуте. Налазио се на Универзитету Харвард, где је вршио сложене балистичке прорачуне за потребе америчке ратне морнарице током и непосредно након Другог светског рата.

Фотографија: Encyclopedia Brittanica

архитектуру ови програми користе само за временски критичне програме, као што су машински адаптери (драјвери), у интегрисаним системима (Embedded Systems), као што су микроконтролери и слично. Колико је оваква архитектура рачунарских елемената битна и колико дуго постоји, говори и чињеница да су и савремени малициозни програми, намењени за уништавање важног система противничке државе, *Стакснет* (Stuxnet) и *Флејм* (Flame), користили недостатке у оваквом типу програмирања.

Буба уништава ракету

Рано ујутро, 4. јуна 1996. године, на небу Француске Гвајане, у 40. секунди по лансирању у космос, експлодирала је ракета Европске свемирске агенције – *Аријана 5*. Њен задатак био је да у Земљину орбиту понесе товар вредан 500 милиона долара, али је у томе спречена чудном грешком у софтверу која је изазвала експлозију (обратите пажњу на део који следи, јер он илуструје необичну природу сајбер ратовања). Исти софтвер је претходно годинама успешно коришћен у претходној верзији *Аријане*. Међутим, са инжењерима који су развијали пету генерацију ракете поиграла се чудна злокобна игра захтева и услова. Захтеви времена тражили су да се повећа носивост ракете, како би она била способна да у космичка пространства понесе већи број тежих сателита, па је изграђена већа и снажнија ракета. Док су искусни техничари и научници одбројавали последње тренутке много пута поновљене и проверене процедуре лансирања, нису могли ни слутити да ће им кодне линије, написане у програмском језику ADA, који служи за програмирање софтвера највеће поузданости и безбедности, тог јутра донети непријатно изненађење. Грешка, сакривена у лошој комбинацији састављених околности, чекала је да изазове тренутак разарања.

Ракета је имала инерцијални референтни систем, који је служио да одреди правац и брзину кретања мерењем положаја ракете у односу на лансирну рампу и да измерене податке проследи централном рачунару који одређује параметре лета. Ради поузданости, постојала су два идентична инерцијална система са истим хардвером и софтвером, као и два независна централна рачунара, један у функцији, а други у „врућој приправности”, спремни да се укључе у

рад у случају да примете грешку у раду примарних система. Иако је сваки појединачни елемент информационог система био у реду, до грешке је дошло услед погрешне архитектуре система.

У конкретном случају, софтвер је вршио конверзију бројних података који представљају вредност хоризонталне брзине лета, записаних у формату 64-битног записа са покретним зарезом у 16-битну целобројну вредност. Код претходне верзије *Аријане* није било могуће да параметри лета у првих 40 секунди лета достигну вредност коју је немогуће приказати у програмираном бројном запису. Веће носивости и снаге, у складу са захтевима времена, Аријана 5 је имала и јачи мотор и, самим тим, и већи потисак и брзину, услед чега су њени параметри лета брзо достигли вредности које за рачунар нису биле схватљиве. Та вредност бројног записа параметра лета је у једном моменту постала већа од 32.766, што је највећа вредност која се може записати у другом формату, па конверзија тог броја није успела. Систем сигурности рада био је прилагођен хардверској, а не софтверској представи (ако се један део поквари, одмах се укључује резервни у рад). Пошто је први инерцијални систем понудио немогућу вредност параметра, централни рачунар је аутоматски пребацио рад на други инерцијални систем, који је отказао с обзиром на исту „немогућу" вредност (у суштини, правилно израчунату). Пошто рачунар није могао да се врати на први инерцијални уређај, јер му није веровао због грешке, по својој бинарној рачунарској логици прихвата последње податке које је добио од другог уређаја. Међутим, то нису били параметри лета, већ су представљали део друге дијагностичке поруке, којом се осигурава процедура лансирања. Тај мали део изворног кода осигуравао је процедуру лансирања у случају непредвиђених застоја и функција му је имала смисла само док је ракета у лансеру. Ипак, за сваки случај, као мера додатне пре-


У ХАВА
САЈБЕ


РИЈИ ЗБОГ
Р НАПАДА

дострожности, он се извршавао и даље, све до 50. секунде од одбројавања.

Пошто није поверовао у немогућу вредност оригиналних параметара лета, а све друге виталне компоненте су му показале неприхватљиве вредности, рачунар је по својој роботској рачуници те нове податке прихватио као параметре лета и употребио их да контролише летелицу. Ракета је потпуно пореметила лет, а систем за самоуништење, као последњи фактор сигурности лета, правилно је реаговао у случају појаве нестабилности у лету. Тако је ракета, са теретом вредним пола милијарде долара, самоуништена у експлозији на небу, како не би пала на неко насеље на Земљи. Дакле, све је било појединачно добро функционисало и осмишљено да буде сигурно, али принцип који је употребљен за дизајн рачунарског система летелице у целини није ваљао.

Аријана није једина ракета која је експлодирала због софтверске грешке. Давне 1962. године, свемирска сонда *Маринер I* лансирана је на свој далеки пут према Венери. Експлодирала је у Северном Атлантику. По незваничним теоријама, грешка у софтверу десила се када је приликом укуцавања програмског кода изостављена једна цртица, услед чега је при полетању дошло до скретања с путање и летелица је уништена обарањем из контролне собе. Неколико година касније Артур Кларк је изјавио да је *Маринер I* срушен због најскупље цртице у историји.

Ако уместо *Аријане* и *Маринера* имамо балистичку ракету са бојевом нуклераном главом, као што је, на пример, руски *Тополь М*, као и космичка ракета, она има властити инерцијални систем и систем за глобално позиционирање (ГЛОНАСС), рачунарски систем и софтвер. Помоћу ње се чак лансирају сателити у орбиту Земље. Разлика је само у нуклеарној бојевој глави *МИРВ* од 550 килотона. Уколико њен софтвер има недостатак (а многи програмери тврде да га сваки софтвер има), замислите последице случајне грешке у евентуалном раду или намерне у сајбер нападу. А, да ли је могуће сајбер нападом напасти изоловани, неумрежени информациони систем?

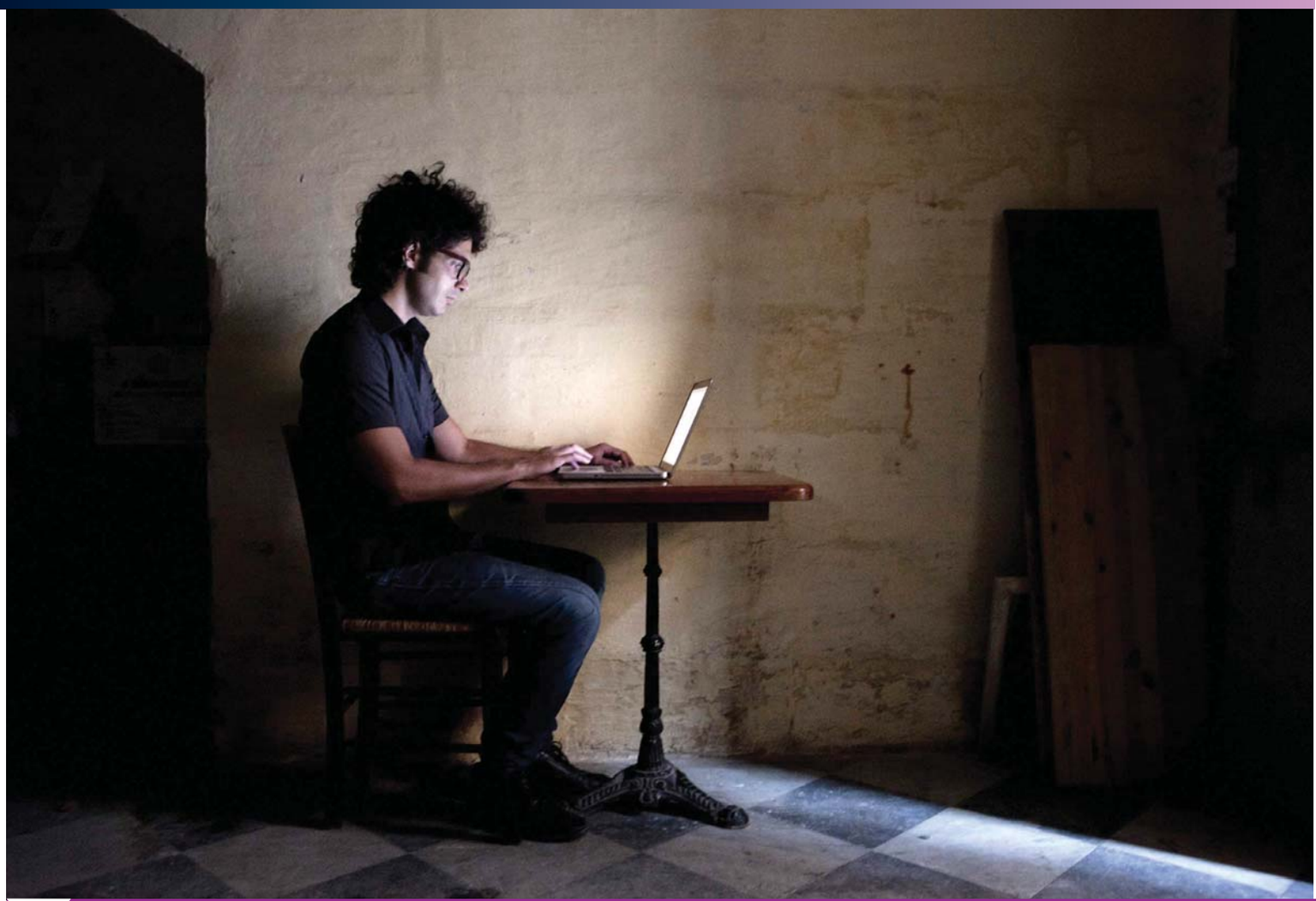
Уништавање гасовода

Експлозија *Аријане* на небу Гвајане деведесетих година била је мала у поређењу са великом експлозијом руског гасовода 1982. године, коју у својој књизи наводи бивши саветник за сајбер безбедност више америчких председника Ричард Кларк. По његовој причи, америчка агенција CIA је почетком осамдесетих година прошлог века подметнула Совјетском Савезу модификовани софтвер за контролу рада гасовода, знајући намеру Совјета да индустријском шпијунажом дођу до готовог пројекта у Канади. То им је омогућио француски шпијун у редовима КГБ, совјетски обавештајни потпуковник Ветров (шпијунски надимак који му је доделила CIA био је Ferewell, у преводу због, опроштајни поздрав), чији је посао у Првом директорату КГБ била баш индустријска шпијунажа технологија са Запада. Након бизарног инцидента у коме је под дејством алкохола уништио службени аутомобил, затражио је од свог француског колеге помоћ и мрежа око њега је почела да се заплиће. Касније је француској обавештајној служби дао велики досије од преко 4.000 куцаних страна о свим совјетским операцијама индустријске шпијунаже на Западу, ангажованим шпијунима и списку жељених технологија, који су Французи (полу)грешком проследили агенцији CIA. Уместо да одмах ухапсе 250 совјетских шпијуна, Американци су прво совјетским шпијунима подметнули више измењених технологија у области борбене авијације, космичких система, стелт технологије и критичне инфраструктуре. Ти програми су претходно били намерно измењени, тако да су били нефункционални, а неки су чак били подешени да нанесу опасну штету. Један од њих је био канадски софтвер за рад нафтовода и гасовода. Совјети су били посебно заинтересовани за рачунарске софтверске и хардверске технологије и веома задовољни што су дошли у посед индустријских тајни. Применили су набављени софтвер на властитом систему за пренос енергената. Он је у почетку функционисао веома добро, али је, наводно, након одређеног времена, изазвао поремећај у раду гасовода, тако што је затворио вентиле на једној страни, а на другој изазвао максималан притисак прекомерним радом пумпи које су погониле гас. Последица ове намерно пројектоване грешке била је најјача експлозија ненуклеарног порекла икада измерена на планети, укупне јачине три килотона, која се догодила у јесен 1982. године.

Експлозијом је, наводно, уништен систем који је доносио приход од 8 милијарди долара годишње. У руској штампи су једну експлозију на наведеном систему окарактерисали као последицу лоше конструкције, а не рачунарске саботаже. Иако овај случај није никада званично потврђен ни од једне стране, више о случају се може прочитати у електронској онлајн библиотеци агенције CIA, а посебно је занимљив есеј учесника тих догађаја, Гаса Вајса, под називом *The Farewell Dossier*. Било како било, скоро десет година касније, саветник за науку совјетског председника Горбачова, чије су одлуке допринеле окончању постојања СССР-а, написао је да су технологија и наука СССР-а касниле за западним стандардима 15 година у подручју микроелектронике и рачунара и да је најочитији пример била неспособност да се произведе домаћи суперрачунар. Овај пример показује да су рачунари и софтвер укључени у савремено ратовање дуже него што то већина претпоставља.

Шта је *zero-day* недостатак?

Сви програми имају грешке (бубе) које могу бити злоупотребљене за креирање сајбер напада. Након откривеног напада жртва анализира како је до њега дошло, које методе је нападач предузео и које недостатке је искористио. С обзиром на постојање интернета, вести о нападима и новим



Луиђи Ауриема живи на Малти и зарађује тражећи пропусте у софтверу које његови клијенти могу да злоупотребе за нападе на државе.
Извор. The New York Times, 2013.

откривеним безбедносним пропустима шире се готово тренутно. Зато је мала вероватноћа да нападачи вишекратно у дужем периоду користе исте недостатке за напад. Нападачима су највреднији софтверски пропусти који су до тренутка напада били непознати свима, осим њима самима. Такви напади, који су остварени експлоатацијом *zero-day* недостатака, зову се *zero-day* напади (напади нултог дана).

Израз нулти дан односи се на чињеницу да су недостаци били непознати ауторима софтвера, односно да су били познати 0 дана пре него што су их нападачи злоупотребили за напад. Софтвер или метод, скуп података, секвенца или команда напада који користи недостатак нултог дана назива се експлоит нултог дана. Нападач га креира да искористи постојање софтверске „бубе" (недостатка) како би изазвао неочекивано или непредвиђено понашање софтвера, хардвера, протокола везе, односно било ког техничког система који почива на раду електронике и дигиталне технологије. Нови, неиспробани напади су најефикаснији, али нове пропусте у противничким системима није лако утврдити. Та чињеница у великој мери повећава трошкове офанзивних дејстава сајбер ратовања. У таквим околностима већина војних система ће вероватно мање пажње полагати на примену принципа етичности, а више на ефикасност напада. Сигурносни пропусти налазе се у сваком софтверу. Најраширенији оперативни или апликативни софтвер, попут оперативних система компаније Мајкрософт, производа компаније Адоб, сви савремени интернет прегледачи или Јава апликација, пуни су сигурносних пропуста, које у честим временским интервалима откривају програмери софтверских компанија, добронамерни или злонамерни појединци и групе.

Овакви недостаци омогућавају сајбер нападе у миру, било да се ради о актима криминала, шпијунаже или ратовања У суштини, сајбер ратовање, као и сајбер шпијунажа и тероризам, заснивају се на примени оваквих напада нултог дана. Основни принцип јесте да се открије недостатак пре другог. Нападачи журе да открију недостатке пре аутора софтвера и жртава, бранитељи журе да открију недо-

статке пре нападача, аутори софтвера журе да открију недостатке пре свих, да не би изгубили пословни реноме и клијенте. Због њих данас у свету сајбер безбедности влада права помама ко ће те недостатке први наћи. Софтверске компаније организују такмичења на која позивају хакере и додељују им високе награде у жељи да их подстакну да нађу што више недостатака у њиховом софтверу, које ће након тога њихови инжењери поправити и објавити ажурирање основног софтвера (производа) и тако га безбедносно унапредити.

Тренутни шампион у подстицању програмера широм света да учествују у проналажењу недостатака је компанија Мајкрософт, која за документоване информације о недостацима појединачно плаћа и до 150.000 долара. Са друге стране, и криминалци траже ове недостатке да би их злоупотребили и остварили криминалне намере. Данас у свету постоји развијено тржиште на којем се тргује недостацима и експлоитима у подземљу.

Ипак, државне агенције, као и увек, имају апсолутну предност и највећа средства. Оне такве недостатке купују на другом специјализованом светском тржишту или користе властите законе и споразуме са приватним компанијама у својој надлежности (регистрованим на територији државе) да остваре ексклузивно право њихове употребе, пре свих, чак и пре самих компанија чији је софтвер у питању (како тврди Сноуден, то чине агенције NSA, CIA и FBI у САД). Круг узајамних услуга између обавештајних агенција и великих приватних компанија или између самих агенција изузетно је добро развијен. Недостаци служе да се креирају напади, а пошто владе држава света не користе сајбер нападе да би хаковали мрежне игрице или предузимали искључиво криминалне радње, јасно је да их користе за оно што им је у опису дужности: за ратовање, шпијунажу и фамозни „државни тероризам". Сама чињеница да државне агенције редовно прибављају овакве недостатке довољан је доказ постојања сајбер ратовања.

Откривање софтверских недостатака

Погрешно је сматрати, на основу скорашњих медијских вести о случају одбеглог узбуњивача, бившег систем-администратора у NSA, Едварда Сноудена, да само Влада САД има овакве намере. У ту активност укључене су готово све владе које развијају капацитет за операције у сајбер простору. По истраживачком извештају који је недавно објављен у Њујорк Тајмсу, а по изјавама представника компанија које истражују недостатке ради продаје државним агенцијама, у куповини јавно неоткривених софтверских недостатака предњаче владине агенције из САД, Велике Британије, Израела, Русије, Индије и Бразила. То значи да они ове недостатке користе за одбрану од нападача који их могу применити, али и за напад на било кога ко користи технологије у којима су откривени недостаци. У свету постоје многе мале, специјализоване приватне компаније, као што су *Вупен* и *Ревулн*, састављене од неколицине искусних програмера, који по цео дан траже *zero-day* недостатке и експлоите и затим, за приличне своте новца, продају информације о њима и „ауторско право" на њихову примену искључиво државним обавештајним агенцијама. У зависности од могућности недостатка, те своте се крећу од стотину хиљада долара до милионских износа. Уместо препродаје оружја, у сајбер ратовању се препродају информације о недостацима.

На Малти се налази мала компанија *Ревулн*, коју сачињавају само два програмера. Она је пре извесног времена продала информације о недостатку у оперативном систему компаније Epl (iOS) за пола милиона долара. Ова компанија се специјализовала за недостатке у софтверу за индустријске контролне системе *(Supervisory Control and Data Acquisition – SCADA)*, а продају их искључиво државним агенцијама, укључујући и NSA. Овај концепт стартап предузећа у области откривања и продаје *zero-day* недостатака је толико популаран да

Вупен, француска компанија. Посао ових младих момака је да открију податке о софтверским недостацима за које не знају ни произвођачи софтвера и продају их разним владама света.
Извор: Vupen Security Hacking, 2012.

њихов број брзо расте у целом свету. Пре неколико година било је уобичајено да програмери своје резултате продају познатим компанијама или им уступе информације у залог за запослење, а онда су схватили да је много уноснije да информације и полупроизводе продају државним обавештајним агенцијама.

Француска компанија *Вупен* се јавно рекламира као „водећи провајдер дефанзивне и офанзивне обавештајне сајбер безбедности" у свету. Само годишња претплата на каталог недостатака те мале фирме из Монпељеа, у Француској, да би се стекло право на могућност куповине њихових хакерских производа, кошта разне светске владине агенције 100.000 америчких долара. Иако су највећи светски произвођачи софтвера, попут компанија Мајкрософт, Епл, Адоб и Оракл солидне платише, обавештајне службе највећих држава света ипак имају већу платежну моћ.

Компанија *Вупен* је специфична, јер се рекламира на оригиналан начин. На пример, прошле године је одржано хакерско такмичење у проналажења *zero-day* недостатака у најпознатијим веб прегледачима (браузерима) попут Интернет експлорера, Гугл хрома, Мозиле фајерфокс и других, које користи сваки корисник интернета да приступи садржајима на интернету. Такмичење се зове *Pwn2Own* и део је годишње *CanSecWes* конференције о безбедности. Група *Вупен* појавила се на такмичењу и креирала експлоит којим је превазиђена заштита у сендбокс модулу *хром* прегледача компаније Гугл. На њему је радила шест недеља пре такмичења, а на такмичењу је само јавно представила метод напада.

Уместо да објави и документује недостатак и прими заслужену награду од приређивача такмичења у висини од 60.000 долара, вођа тима, Чауки Бекрак, објавио је на конференцији да ће задржати информацију за себе и своје клијенте. То је најпре изазвало изненађење представника компаније Гугл, који је тиму одмах јавно понудио додатних 60.000 долара од компаније уколико обелодане информацију о недостатку, на шта се Бекрак насмејао и изјавио да ће можда размислити уколико Гугл понуди милион долара. Ако се питате ко су клијенти, можда ће вам помоћи Бекракова изјава: „Ми продајемо (*zero-day* недостатке) једино демократским државама. Ми поштујемо међународне регулативе, наравно, и продајемо једино државама од поверења и демократијама од поверења. Не продајемо тиранским државама".

Да ли је Бекрак под „демократијом од поверења" мислио на античку Атину или неку модерну северноатлантску државу – знају он и његови клијенти. Такође, само он зна да ли је под „међународним регулативама" мислио на Допунски протокол I уз Женевске конвенције из 1949. године. Јер, иако то није изричито забрањено неким посебним ставом у праву оружаних сукоба, по члану 43. наведеног протокола, цивили немају статус бораца, па самим тим немају ни право да директно учествују у борбама. Учешће цивила у борбама је по законима већине држава света противзаконита активност, а пошто цивилима међународно право не даје статус бораца, њихово учешће у борбама је кривично дело. Такво објашњење важи за свако учешће у борби, укључујући и сајбер ратовање.

С друге стране, напад на цивиле, за време док учествују у борбеним операцијама, јесте легалан. Уколико се сајбер ратовање схвати као акт агресије, онај ко „активно учествује у борбама", односно ствара и припрема нападе („сајбер оружје"), по неким мишљењима може се сматрати сајбер борцем. Наравно, услов за то је да „Бекракова демократија" предузме напад на другу државу, чије последице изазивају ефекте оружане агресије, уништење материјалних добара и погибије лица. Уколико, пак, уместо напада са кинетичким ефектима држава купац експлоита предузме шпијунску операцију, Бекрак би се могао сматрати шпијуном, а у оба случаја вероватно и ратним плаћеником, с обзиром на висину новчане накнаде за коју обезбеђује сајбер нападе. Наведени ставови су у складу и са схватањем НАТО војног савеза, ако имамо у виду мишљења његових највећих правних стручњака, сажетим у скоро објављеном међународноправном приручнику о сајбер ратовању Центра изузетности НАТО у Талину.

У сваком случају, уколико последице међународног сајбер напада који су креирали припадници неке компаније и учествовали у његовом предузимању у замену за новчану надокнаду буду погибије или материјална уништења у другој држави, еквивалентна последицама напада физичком силом, по многим стручним мишљењима и ставу самог НАТО-а, „тиранска" држава има правне основе да чланове тима *Вупен* сматра борцима, плаћеницима или шпијунима и поступа са њима онако како се са њима иначе поступа у сукобу. Исто се догађа и уколико „демократска" држава нападне САД њиховим експлоитом и изазове наведене последице, јер, по влади САД, учешће цивила у борбама на некој од зараћених страна представља индивидуални ратни злочин по међународном праву, али и колективни, уколико те цивиле ангажује друга држава. Овај принцип влада САД је применила када је по одредби Акта о војним судовима из 2006. године оптужила Канађанина ухваћеног у Авганистану који је учествовао у борбама на страни Ал Каиде, на противзаконит начин, како је наведено у пресуди војног суда у САД.

Како армије примењују сајбер ратовање?

Ипак, правни проблеми су државама мање важни од безбедносних. Уколико имате у виду да је чувени малвер *Стакснет* имао, не један, већ најмање пет *zero-day* недостатака, можете претпоставити колико може да кошта сајбер ратовање. Такође, уколико сте службеник државе, вероватно вам већ пада на памет идеја да можда и не морате

Командант ISAF-а извештава команданта Сајбер команде и директора Националне геопросторне обавештајне агенције о стању на терену, током њихове посете, 28. јула 2010. године, на Међународном аеродрому у Кабулу, једном од ретких потпуно безбедних места од талибанских побуњеника у Авганистану. Маја у позадини и радни папири на столу накнадно је замаглио званични фотограф.
Извор: ISAFMedia, Flickr, 2010.

имати много новца за куповину недостатака, већ да би било ефикасније да имате једну овакву групу у оквиру своје организације. Или можда две, три, четири…

Британска армија позната је у свету по строгим критеријумима за физичку кондицију својих припадника. Начин селекције кандидата за пријем у њихове специјалне ваздушнодесантне јединице, као што је SAS, чувен је у свету по физичком исцрпљивању кандидата. Група од 200 кандидата под пуном ратном опремом прелази велике раздаљине дању и ноћу по дивљим пределима широм света у укупном трајању од пет недеља. Најбољи од оних који издрже биће примљени у SAS. Нису ретки ни случајеви да кандидати умру од исцрпљености током селекције. Овај метод је толико познат да је постао узор многим армијама у свету за селекцију кандидата за специјалне јединице. Ипак, британска армија је толико сензибилна за питања сајбер ратовања да је прва армија у свету која је званично одлучила да не примењује пријемне и периодичне тестове физичких способности за припаднике армије (активне резерве) који се баве сајбер ратовањем. Оволика сензибилност за хакере вероватно потиче од чињенице да је британска влада пре две године одлучила да издвоји 650 милиона фунти на сајбер ратовање у периоду од четири године, и то првенствено на офанзивне сајбер капацитете, за шта сваког дана неко од британских званичника тврди да је недовољно.

По изјави Џона Арквиле, специјалног саветника америчког председника Обаме за сајбер безбедност, америчка администрација озбиљно размишља о ангажовању десетине хиљада хакера, међу којима на стотине из Русије и азијских земаља, као и ангажовање хакера прекршилаца закона, како би радили за државне агенције. На сличан начин је америчка војска, пре краја Другог светског рата, ангажовала све немачке ракетне научнике до којих је могла да дође пре Совјета и одведе их у САД. Стога не чуди што ниједна важна хакерска конференција у САД није протекла без присуства високих представника Министарстава одбране и отаџбинске безбедности, NSA или NASA.

Пре две године најпознатијој хакерској конференцији на свету *DefCOn*, коју је уз пуну анонимност посетило 16.000 хакера, присуствовао је и Ричард Џорџ, технички директор одељења NSA задуженог за сајбер одбрану. Он је том приликом изјавио: „Данас су сајбер ратници ти које ми тражимо, не ракетни научници". Следеће године, у име NSA, на *DefCOn* конференцији је држао предавање директор NSA и командант америчке Сајбер команде, генерал Кит Александер, како свима изгледа, човек на тренутно најмоћнијем положају по питању сајбер ратовања у свету. Генерал са највећим мирнодопским чином у америчкој војсци изашао је на бину у фармеркама са окаченим свежњем привесака и у црној мајици са кратким рукавима са апликацијом знака агенције NSA. На почетку презентације позвао је на бину 11-годишњу девојчицу – хакера са надимком CyFi, која је са својим другарима пре извесног времена пронашла један *zero-day* недостатак и онда је скинуо горњу мајицу са знаком NSA, испод које је била *DefCOn* црна мајица са кратким рукавима са знаком два разграната дрвета чије се крошње преплићу. Затим је окупљеним тинејџерима и адолесцентима хакерима, који су се гурали стојећи у сали, како би боље видели генерала, упутио позив и директан изазов у лице: „Дођите код нас и пробајте да установите да ли сте способни да се носите са неким од најтежих проблема сајбер безбедности у свету".

Пошто је жеља за доказивањем и бављење информационих технологијама углавном и натерала младиће и девојке са *DefCOn*-а да постану то што јесу, слободно замислите колико њих је пожелело да оде у NSA и да се опроба са „најтежим проблемима у свету"? Ове године организатори *DefCOn* конференције нису желели присуство владиних званичника у знак протеста због објављених информација о масовном праћењу свих комуникација на интернету од стране агенције NSA, али је позив дошао од друге најпознатије кон-

ференције *BlackHat* и био је прихваћен, поново од генерала Александера.

Командант Сајбер команде не креће се само по хакерским конференцијама. На званичној фотографији команде америчке војске у оквиру војне операције ISAF, која се одвија у Авганистану под покровитељством УН, војни фотограф је приказао детаљ са брифинга команданта операције званичној делегацији из Вашингтона, коју су сачињавали Александер и вицеадмирал Марет, тадашњи директор Националне геопросторне обавештајне агенције, у лето 2010. године. Недуго након тога, генерал-потпуковник Милс, заменик команданта рода маринаца је на једној војној церемонији у Луизијани јасно нагласио колико команданти на терену у реалним борбеним ситуацијама сматрају сајбер операције важним делом њиховог војног арсенала: „Могу вам рећи да сам као командант у Авганистану 2010. године, био у могућности да употребим сајбер операције против мог непријатеља са великим успехом. Био сам у могућности да уђем унутар њихових комуникационих мрежа, инфицирам њихове командне центре, и у ствари, да на тај начин одбраним себе од њихових константних настојања да уђу у наше комуникације и тако утичу на моје операције".

Ко изводи те сајбер операције на терену и како му изгледа радни дан у реалним борбеним условима може се прочитати на веб сајту *24th Air Force* (јединица пропорционална рангу ваздухопловне армије) , највеће јединице Војске САД за сајбер дејства. У најкраћем, дневно ангажовање у оквиру деветочлане Сајбер команде у оквиру мисије ISAF је од 6 до 12 часова, седам дана у недељи, непрекидно шест месеци на планирању рачунарских мрежних операција, нарушавању и праћењу рада непријатељских комуникација и реализацији офанзивних задатака ради подршке властитим снагама. За шест месеци тим је извео девет већих сајбер операција против талибана којима је озбиљно нарушио систем противничке онлајн пропаганде, бројне специјалне сајбер операције у којима је нарушио противнички систем командовања и комуникација и створио нове процедуре којима је повећао ефикасност сајбер операција на терену за 60 посто. Један од најзначајнијих задатака био му је упознавање претпостављених старешина о практичним могућностима овог малог тима да допринесе борби и о томе како сајбер операције са кинетичким и некинетичким дејством на циљ треба да се укључе у оперативно планирање и извођење војних операција. Истовремено, као једну од највећих опасности у току мисије, наводи непоуздану храну у Авганистану и самоубилачке нападе на мисије. Официр наводи да је претходно био упућиван у Ирак 2007. године и Босну 2002. године. Укупно је руководио током више од 5.000 војних сајбер операција и за то је добио високо одликовање – Бронзану звезду.

Тим Елемента за сајбер подршку војне експедиције из 24. Ваздухопловне армије у саставу команде ISAF у Кабулу.

Ко унајмљује хакере?

Свима је позната одлука америчког председника да се војна мисија у Авганистану повуче из те земље до краја 2014. године. Међутим, у плану је да око 10.000 припадника америчке војске остане и после тог рока у Авганистану. Они ће тамо водити сајбер и специјалне операције, као и ратовање беспилотним летелицама. Једна приватна компанија из Калифорније, Леони, са канцеларијом преко пута Пентагона, која за потребе владе САД ради послове у области сајбер, информационих и специјалних операција, у априлу ове године објавила је оглас за радно место под називом планер сајбер операција у Кабулу. Лице које буде примљено мораће да се бави покретањем офанзивних сајбер операција, интегрисањем сајбер операција у стратегијске операције, обавештајним сајбер активностима и сличним радњама. Поред CEH, CISSP и CCNA сертификата, кандидат обавезно мора да поседује војно искуство у извођењу специјалних мрежних операција и то оно које је стечено у Авганистану или Ираку, као и важећи амерички туристички пасош.

САД имају за циљ да остваре глобалну доминацију у сајбер простору, на исти начин како су остварили војну доминацију у ваздушном и космичком простору. Очекивана доминација у сајбер простору је потуна и односи се на офанзивна сајбер дејства на рачунарским системима и мрежама, као подршку конвенционалним снагама, доминацију у електромагнетном спектру и у информационом подручју. Ти циљеви могу се закључити из америчких стратегијских докумената који се односе на сајбер безбедност.

Овако захтевну стратегију реализује најгломазнија војна сила у области сајбер безбедности на свету. У њој је централна војна институција Сајбер команда, док је то у оквиру Министарства одбране агенција NSA. Сајбер команда тренутно има 917 запослених, али је у току повећање њене формације за 4.000 лица, и она је надлежна команда за све припаднике америчке војске који се баве сајбер операцијама. У овом моменту, у ваздухопловству на местима која се баве сајбер ратовањем постављено је око 17.000 лица, у Морнаричкој сајбер команди/Десета флота више од 14.000 лица, у маринцима око 800, у копненој војсци више од 21.000, што укупно, без NSA и других обавештајних агенција, чини око 58.000 лица. По једном извештају кинеске владе, у САД на активностима сајбер ратовања ради јединица од 100.000 сајбер ратника. Званични подаци су много мањи и износе око 11.000 лица. У овогодишњем саслушању испред Комитета Сената за оружане снаге, генерал Александер је навео успостављање 13 офанзивних јединица за сајбер ратовање којима је основни циљ дејство против потенцијалних нападача, 27 тимова за подршку у планирању офанзивних сајбер операција и већи број тимова са сајбер одбрану националних капацитета. Сви они ће сукцесивно у три фазе бити задејствовани и оперативно спремни до 2015. године.

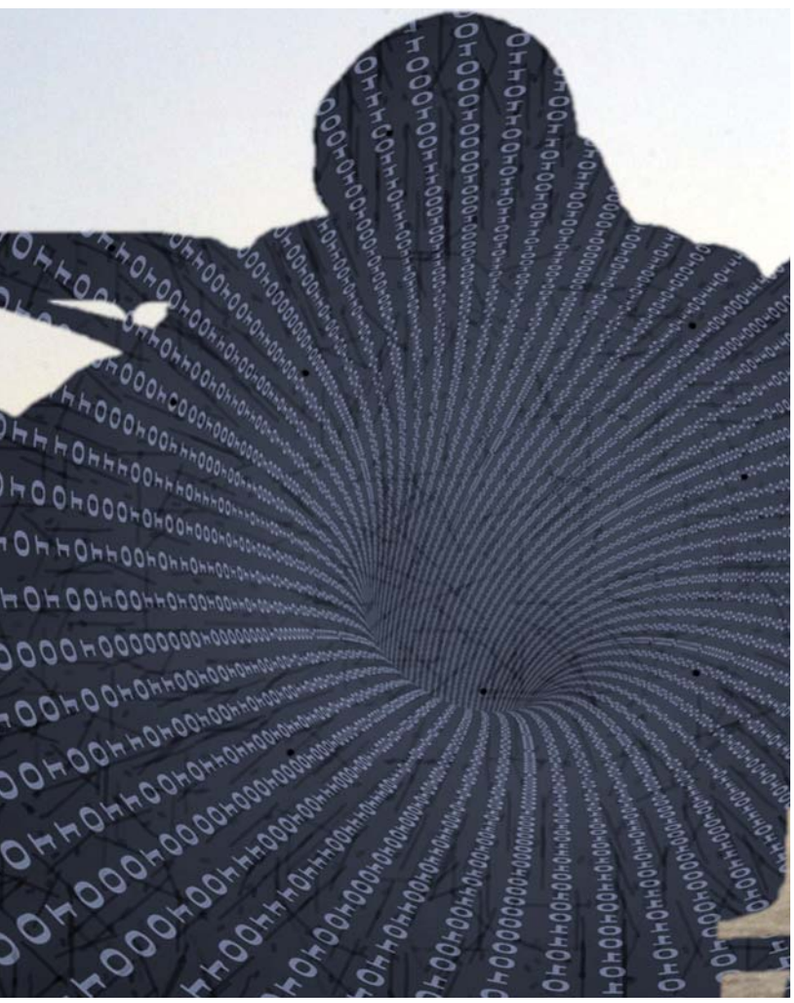
Смештена у касарни Форт Мид у Мериленду (у истој оној у којој је агенција NSA), комплекс Сајбер команде је и физички импозантан, јер се простире у подручју већем од 920.000 квадратних метара, у којем се налази 14 административних зграда са укупном површином од 167.000 квадратних метара и са електричном трафостаницом укупног капацитета од 150 мегавата (што је скоро 20 посто од максималне потрошње струје града Београда). Оволико велика потрошња струје је, поред осталог, потребна и због рада суперрачунара. Колико њих има није познато, али зграда у којој се они налазе има припремљену површину од 90.000 квадратних метара и 50 људи. У наредних 16 година, по урбанистичком плану предвиђена је површина од 540.000 квадрата, што практично одговара површини од 60 зграда и 40 великих паркинга. Предвиђени трошкови за тај период

су 5,2 милијарде долара, а запошљаваће 11.000 лица. Команда је већа него многе армије света и троши много више струје.

Раст улагања САД у сајбер одбрану је изузетно велики. У односу на прошлу годину, САД су усвојиле за милијарду долара већи буџет за операције у сајбер простору. Сматра се да годишње потроше преко 30 милијарди долара на добра и услуге за потребе сајбер одбране и безбедности. То

је основни разлог што се војноиндустријски комплекс у САД, који је доживео велики бум након терористичког напада 11. септембра 2001. године и каснијих ратова у региону Блиског и Средњег истока врло брзо преоријентисао са ратова у Ираку и Авганистану на подручје сајбер одбране и безбедности, које је постало подручје са највећим растом у одбрамбеној индустрији. Многе велике компаније које раде за америчку владу, као што су Genaral Dynamics, SAIC, CSC, Booz Alen Hamilton, Boeing и Raytheon у последњих годину-две изградиле су велика постројења, развојне и истраживачке центре у подручју сајбер одбране и безбедности. Већина тих новоотворених центара налази се у држави Мериленд, тик поред седишта NSA и Сајбер команде.

Иначе, у Мериленду функционише Сајбер Мериленд, најпознатији пословни инкубатор на свету, који обједињава



интересе, потребе и ресурсе владе, војске, бизниса и академских институција. Свако ко нешто значи у бизнису сајбер безбедности тамо има своју улогу. Ту су обједињене све компаније у области војне индустрије у САД и све водеће научноистраживачке установе и лабораторије у области информационих технологија и одбране. Већина иновација у области сајбер безбедности потиче одавде. Сајбер безбедност у САД доживљава невероватан бум. Уколико на интернету прегледате објављене позиве за посао у овим компанијама, или сте пријављени на форуме друштвених мрежа оријентисаним ка бизнису, као што је популарни LinkedIn, видећете да у овом региону (и уопште у САД) постоји права помама у тражњи стручњака за нове егзотичне послове као што су специјалиста за рачунарске мрежне нападе, специјалисте за обавештајне операције у сајбер простору, аналитичар великих података (Big Data Analyst), консултант за напад и насилни продор у рачунарске мреже и друге у сличном тренду.

Све веће ангажовање цивила у подручју сајбер одбране доводи до важне карактеристике сајбер ратовања, а то је да разлика између бораца (и војног персонала) и цивила (запослених у компанијама под уговором са министарствима одбране) постаје занемарљива. Та чињеница директно се коси са међународним хуманитарним правом, које забрањује цивилима да учествује у борбама, односно не даје им правну заштиту од непријатељских дејстава, ако се ангажују у борбама. Колике размере има ангажовање приватних компанија у пословима сајбер одбране и безбедности показује и случај Сноуден, а још јасније пројекат Вашингтон поста из 2010. године, под називом „Тајна Америка", у којем је документовано ангажовање 165 великих приватних компанија у САД, потребе за 22 команде, агенције и владине организације у САД у области офанзивних или дефанзивних сајбер операција.

Неке од тих приватних компанија преузимају чак део или целокупну функцију државних обавештајних агенција. Најочитији пример је компанија Ендгејм Системс (Endgame Sistems). У питању је стартап компанија основана 2008. године у Атланти од неколико већих пословних компанија. Ова компанија, по новинским написима часописа Wired, Defense News и Bloomberg Businessweek, развија поступак за упаде у све умрежене уређаје на интернет, тражећи скривене *zero-day* недостатке у програмима које ти уређаји користе, укључујући и сам антивирусни софтвер. Међутим, иде и корак изнад тога. Она је створила мапу свих светских уређаја умрежених на интернет, са прегледом утврђених недостатака који могу бити искоришћени за напад споља. Улога ове компаније у пословима одбране није била позната све док извршни директор једне друге компаније која обавља послове у подручју сајбер безбедности за америчку владу, HB Garry, у зиму 2011. године није објавио да се његова фирма успешно инфилтрирала у организацију тајне хакерске групе Анонимуси. Уместо одговора Анонимуси су извели више напада на компанијин веб сајт, имејл и телефонске сервисе. Том приликом доши су у посед електронских порука које доста говоре о улози компаније Енггејм. У једној од њих нуди се приступ њиховој колекцији од 25 важних zero-day недостатака за претплату од тричавих 2,5 милиона долара. Годинама Ендгејм настоји да се држи стриктно по страни од јавне сцене. Њени главни „производи" су платформе *Bonesaw* и *Velocity*. По речима неименованог пред-

ставника компаније *Bonesaw* платформа обезбеђује комплетно решење за обавештајне аналитичаре и планере операција да остваре свеобухватан приступ на откривању циља, смањивању времена потребног за стварање оперативних планова мереног у данима на минуте.

Bonesaw има способност да темељно мапира сваки уређај повезан на интернет и ствара евиденције о његовом хардверу и софтверу. Сви сервери и рутери на свету тако постају приступне тачке помоћу којих агенције попут NSA и војне јединице унутар Сајбер команде САД могу да изврше сајбер нападе на техничке и организационе системе било које државе. Ендгејм не врши нападе, само нуди потпуне и довољне информације владиним агенцијама о њима. И наплаћује их скупо. Када плати, купац може да изврши напад по жељи. Мапа коју нуди Ендгејм је импозантна, јер обједињава податке из разних извора, на пример, геолокацијске податке, IP и MAC адресе уређаја, организационе називе система, софтвер, недостатке софтвера и нуди могуће нападе. На пример, клијент може да лоцира државу, регион, град, организацију (по називу или адреси). Софтвер показује списак свог софтвера који се користи на рачунарима унутар те организације, врсте недостатака које садржи, могући малвер којег домаћин није свестан, да ли се налази у некој ботнет мрежи (што је врло чест случај; приликом истраживања функције програма *Wiresha*rk, пакетног анализера мрежног саобраћаја, пре неколико година, аутор овог текста је утврдио да је један од његових рачунара, који је умрежен на Интернет, био повезан не у једну, већ у две ботнет мреже), као и списак потенцијалних експлоита погодних за напад.

Унапређена платформа под називом *Velocity* (брзина) обезбеђује тренутни приступ сваком мапираном уређају на интернету и праћење измена хардвера и софтвера на њему. То значи да омогућава тренутне сајбер нападе. У суштини, то значи да компанија Ендгејм поседује огромну базу података о сваком јавно неоткривеном недостатку на сваком познатом хардверу и софтверу који се користи у свету, односно да зна више недостатака о производима него што знају њихови произвођачи. Велика је шанса да се и ваш кућни рачунар налази у њиховој бази података. Какав је правни статус овакве пословне понуде још није јасно, али бивши директор за информациону безбедност агенције NSA, наводи: „По мом мишљењу, овакве активности представљају акт рата или у најмању руку, увод у будуће акте рата".

Критична инфраструктура

Осим пегли, старијих модела шпорета и појединих грејних тела, скоро сви индустријски, комуникациони и кућни технички уређаји имају у себи уграђене дигиталне технологије. Многи од њих су и умрежени на интернет ради остваривања квалитетнијих сервисних процеса. Дигиталне технологије користе се не само у електронским, већ и у скоро свим механичким уређајима. Аутоматизација дигиталних система подразумева употребу података и информација у дигиталном облику, софтвера који обрађује те податке и могућност повезивања са другим уређајима, системима и мрежама. Применом дигиталне технологије врши се манипулација дигиталним подацима које је могуће копирати у идентичном облику као што је оригинал, преузимати, истраживати, модификовати, генерисати и уништавати. Ова

чињеница омогућава дејство на техничке системе и системе чији је рад заснован на дигиталним технологијама, а последице таквог дејства у крајњем исходу могу бити идентичне физичком дејству на њих.

Сајбер напади на критичну инфраструктуру представљају један од најважнијих циљева нападача у миру и рату и једну од најозбиљнијих опасности по сваку нацију данашњице. То је нагласио сада већ бивши државни секретар САД за одбрану Леон Панета, на конференцији у Њујорку, у октобру прошле године. Том приликом он је дословце рекао: „Агресорска нација или екстремистичка група може употребити сајбер средства да преузме контролу над критичним тачкама…они могу избацити из шина путничке возове, или возове са смртоносним хемикалијама. Они могу контаминирати систем водоснабдевања у главним градовима или срушити електроенергетски систем у огромним деловима земље". Представници Министарства одбране у пратњи државног секретара су том приликом инсистирали на ставу да секретарове речи не треба схватити као хиперболу, већ као одмерену реакцију на сајбер нападе на САД који су се већ десили.

Да ова тврдња није преувеличана, илуструје податак да је, раније ове године, америчка војска утврдила да је страни нападач (појединац, терориста, државна агенција) провалио у електронску базу података свих америчких брана, а коју је чувао Инжењеријски корпус Копнене војске САД. База садржи податке о преко 76.000 брана на америчком тлу, од којих је 13.991 класификована као високоризична мета напада (то је она мета чији отказ може да изазове људске жртве).

Термин „критична инфраструктура" је након терористичког напада домаћег десничарског екстремисте на федералну зграду америчке владе у Оклахоми 1995. године, из америчке унутрашње политичке сцене брзо ушао у глобалну употребу. Наредне године је извршном одлуком америчког председника формирана такозвана Председничка комисија за заштиту критичне инфраструктуре, чије је једно од тежишта била и заштита од претњи са интернета. Под овим термином подразумева се скуп индустријских и државних система који су од нарочитог значаја за функционисање друштва и привреде, попут електроенергетских система, система за производњу, чување и дистрибуцију нафтних деривата и других енергената, система за јавно информисање и телекомуникације, за производњу и снабдевање водом и храном, пољопривреду, системе за грејање, здравство, финансијски сектор, систем националне безбедности и одбране, органе државне управе, поштански саобраћај, хемијску индустрију, војну наменску индустрију и друге. Иако је дугачак, списак ове инфраструктуре овде није коначан, јер свака држава има сопствени списак институција и система од посебног значаја за одбрану и функционисање друштва. Важно је напоменути да ни једна држава није заинтересована само за одбрану од сајбер напада на критичну инфраструктуру, већ и за активно предузимање напада на противничке системе. Разлог за то је да се познавање слабости технологија система који се користе у подручју критичне инфраструктуре може применити у обе сврхе.

Најзначајнију улогу у контроли рада критичне инфраструктуре у индустрији имају SCADA системи. То је вр-

Plan X

Планове и платформе за аутоматизовано сајбер дејство не израђују само приватне компаније које их нуде као готов производ америчкој влади, већ и истраживачке агенције у оквиру Министарства одбране. Међутим, и те агенције врло често ангажују приватне компаније за развој, истраживање и услуге у подручју сајбер безбедности. Изгледа да се идеја компаније Ендгејм допала водећим људима америчке Војске. У САД, главна научноистраживачка агенција је DARPA, која у сарадњи са више војних команди и безбедносних агенција, ради на стварању нарочитог програма за вођење сајбер операција. Тај програм, под радним називом, Plan X, намењен је да сваком појединачном војнику учини сајбер ратовање релативно једноставним, а америчкој војсци, да омогући „доминацију на сајбер бојишту". Ова платформа је намењена за офанзивна и дефанзивна сајбер дејства. Буџет програма за период од 2013. до 2017. године износи 1,54 милијарде долара. Овај огроман износ је намењен за ангажовање неких од најпознатијих програмера и менаџера који производе познате комерцијалне софтверске апликације данашњице, који ће се потрудити да произведу платформу способну да сајбер ратовање спусти на ниво оператера и да његова дејства учини предвидивим, попут дејства пешадијског или артиљеријског наоружања, у форми активности која се много не разликује од играња неке игрице. То значи да сваки сајбер нападач не мора да познаје програмски језик у коме је апликација направљена, нити мора да познаје логичку топологију нападнуте мреже. Он не мора да зна да ли је боље да изврши убацивање руткита у језгро система или у фирмвер неког уређаја. Потребно је само да притисне тастер на тастатури или мишу.

На презентацији за медије у Министарству одбране САД, одржаној у априлу ове године, директорка научноистраживачке агенције DARPA, Арати Прабхакар је о програму изјавила:

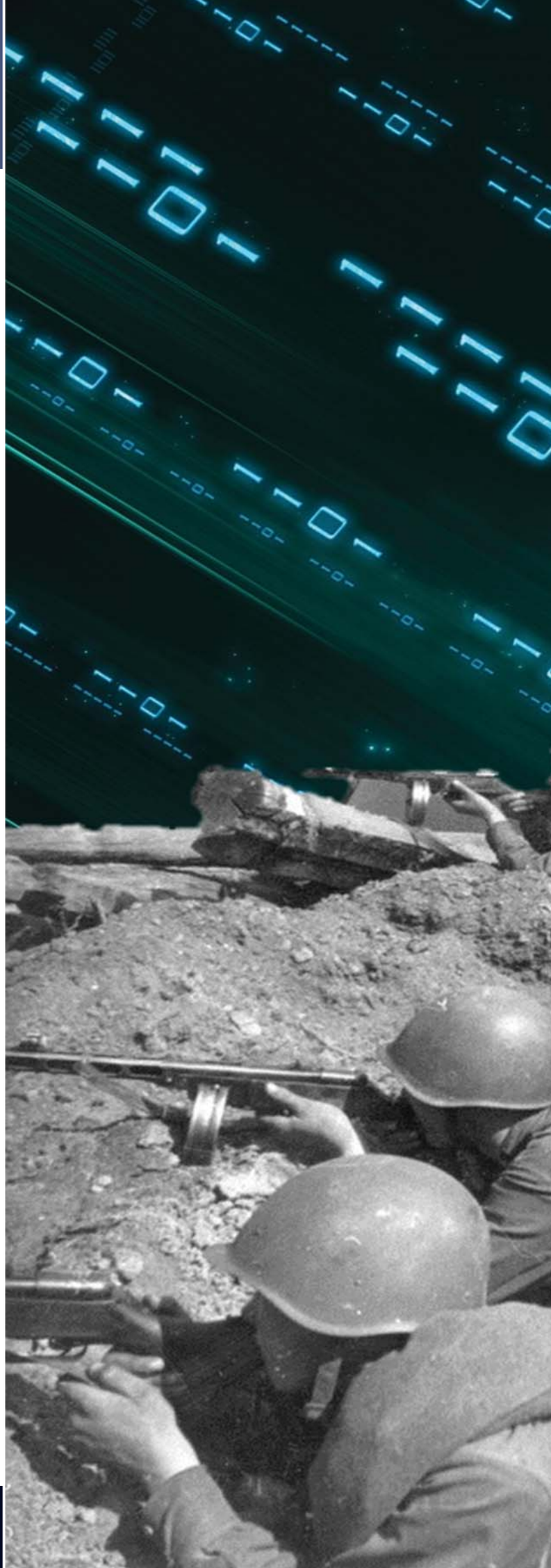
„Ми данас стварамо будућност у којој борбени авиони имају способност да користе сајбер средства као тактично наоружање које је потпуно интегрисано у кинетичка дејства и градимо нову генерацију електронског ратовања која ће доминирати над оним шта друге државе предузимају у развоју технологије ратовања... Ми видимо сајбер претње као критичне претње по војску и шире, целокупну националну безбедност".

ста индустријских контролних система који надзиру процесе у индустријским системима и аутоматски управљају њима. Пошто директно комуницирају са машинама, њихов софтвер се прилично разликује од корисничког софтвера PC рачунара с којим свакодневно долазимо у контакт. Да би њихова функција била представљана људима, они морају имати специфични интерфејс који људима представља процесе и податке. Морају бити високо поуздани, јер се често користе за системе заштите у аутоматизованим процесима, као рачунари за надзор процеса и података у техничким системима, за повезивање сензора, пријем и конверзију њихових сигнала у дигитални облик, као програмабилни логички контролери и у разним другим ситуацијама.

У прошлости, стандард за њихову имплементацију било је одсуство икакве везе са спољним јавним мрежама, чак ни са локалном мрежом на којој крајњи корисници могу умрежити рачунар. Данас више није тако, јер се савремени SCADA системи се све више крећу ка клијент–сервер моделу са централизованим управљањем уз истовремено задржавање карактеристике рада у реалном времену. То значи да се контролни систем, сензори и уређаји међусобно повезују како би остварили оптималан рад. Баш тај захтев им умањује ниво заштите, јер употреба безбедносног софтвера, попут антивирусне заштите, успорава време одзива целокупног система. Такође, ажурирање инсталираног SCADA софтвера може донети више проблема него користи уколико изазове нарушавање поузданости аутоматике, која по основним захтевима увек мора бити апсолутно поуздана са тренутним одзивом и то уз непрекидан рад. Због

Ноћ судбине

Сауди Арамко је званична државна нафтна компанија у Саудијској Арабији. По вредности је највећа компанија на свету (укупна процењена вредност је преко 10.000 милијарди долара, или 20 пута већа од вредности компаније Ексон Мобајл). У свом саставу има 15 великих рафинерија са преко 56.000 радника. У августу 2012. године, дан уочи муслиманског верског празника „Ноћ судбине", нападнута је сајбер нападом злонамерним програмом *Shamoon the Wipper*, који је заразио више од 2.000 сервера и преко 30.000 рачунарских радних станица, са чијих хард дискова је обрисао целокупан садржај. Компанији је требала недељу дана да обнови процес рада. Колика је штета нанета компанији, с обзиром на то да је годишњи профит у 2011. години био 311 милијарди долара, вероватно знају само њени директори. Не зна се ко су нападачи, а више хакерских група пријавило је ауторско право на напад. Напад се догодио свега неколико месеци након сајбер напада на иранска нафтна постројења. Пар дана касније сличан напад је погодио Расгас, највећу компанију за производњу природног гаса у Катару.



тога се ажурирања инсталирају ретко и тек после детаљних провера. То отвара врата за интервенције друге врсте, оне злонамерне.

Стакснет, гласник нових претњи

Неколико армија света већ има могућност да предузме готово сигурно ефикасне сајбер нападе на противнике који могу да физички униште опрему и постројења, односно да изазову погибије људи. Такви напади су предузимани у недавној прошлости. Најпознатији од њих је почињен у, до сада, најсофистицираније, вишегодишњој операцији примене злонамерних програма *Стакснет* (Stuxnet), *Флејм* (Flame) и *Дјукју* (Duqu), а можда и других, неоткривених малвера, и уз извођење пратећих тајних операција. Већина светске стручне јавности сматра да су у операцији учествовале америчке агенције NSA и CIA у сарадњи са израелском обавештајном службом у периоду дугом неколико година, током средином прошле деценије, али за то нема званичне потврде.

Познати израелски новинар Јоси Елман, који годинама пише о обавештајној заједници у дневном листу *Харец*, помињао је да је бивши директор Мосада, Меир Даган био укључен у велики обавештајни пројекат у сајбер простору у време функционисања *Стакснета*. Те исте новине објавиле су извештај са опроштајне забаве начелника генералштаба израелских оружаних снага Габи Ашкеназија, приликом одласка у пензију, на којој је приказан видео-запис у којем се међу успесима израелске војске у периоду његовог рада помиње и успех *Стакснета*.

С друге стране, пре неколико месеци у америчкој јавности је објављена вест да је бивши заменик начелника генералштаба Војске САД, генерал Џејмс Картрајт, под истрагом због објављивања поверљивих информација штампи о сајбер нападима на ирански нуклеарни програм. У питању је његов тајни интервју новинама Њујорк тајмса прошле године, где је детаљно описао операцију „Олимпијске игре", која у ствари представља покретање серије сајбер напада на нуклеарна постројења у Ирану, укључујући и оподметање малвера Стакснет, Флејм и других.

Било како било, са доказом или без њега, *Стакснет* је био први познати софтвер који је употребљен у смислу правог сајбер ратовања. Променио је историју. Био је веома сложен, јер се кретао кроз разне средине. Морао је стићи до нуклеарног постројења Натанц, које је смештено дубоко под земљом, у бункеру који може да издржи удар најснажније бомбе. Прошао је мере обезбеђења кроз које човек не може да прође. Прелазио је са графичких оперативних система на машинске оперативне SCADA системе. То није лак процес. Да би се то постигло, потребно је изузетно много рада, труда, ресурса и времена. Ипак, тај мали програм од свега 500 килобајта је био довољно снажан да

физички онеспособи скоро хиљаду центрифуга у постројењу које су обогаћивале уранијумске шипке. Званичне процене израелских обавештајних служби данас сматрају да је тренутак када ће Иран имати оперативно нуклеарно оружје као последица дејства ове сајбер операције померен за три године, на период између 2014. и 2015. године. Алтернатива овом парчету софтвера била је војна акција борбеног ваздухопловства уз примену најскупљих и најразорнијих бомби огромне снаге намењених за уништавање подземних бункера. Уз такву акцију обично иде и регионални рат великих размера са огромним бројем погинулих и расељених. Сајбер операција је остварила исти ефекат без директне употребе физичке силе, на прикривен начин.

Операцију *Стакснет* (или како је многи називају, операцију „Олимпијске игре") највероватније су покренуле одређене владе света да остваре стратегијске циљеве против владе треће државе. Операција је била пажљиво планирана, организована и спроведена у време мира, без објаве рата или било какве активности која се може са сигурношћу окарактерисати актом агресије на начин како то дефинишу Повеља УН и Женевска конвенција. Операција је спроведена као претходна акција физичком нападу, али и као његова алтернатива. Акцију су највероватније припремиле специјалне војне јединице, обавештајци, али и цивили, истраживачи и програмери који су нашли безбедносне пропусте на машинском софтверу програмабилних логичких контролера који се користе на SCADA опреми. Операција је била потпуно тајна, јер се не може доказати њен починилац. Прикривена је, јер иако целом свету изгледа очигледно ко ју је покренуо, не постоје никакви докази за ту тврдњу. Претпоставке без доказа, колико год очигледно изгледале, се не могу употребити као правни разлог примене адекватних акција од стране Савета безбедности, у циљу спречавања агресије, нити од стране Ирана, као разлог за војни акт самоодбране, у складу са Повељом УН. У потпуности је асиметрична, јер је програмски код употребљен ради уништења нуклеарног постројења.

Иако се ни на један начин не може окарактерисати ратом, она представља облик ратовања, јер је овај сајбер напад спровео један међународноправни субјект против другог, ради наметања властите политичке воље, у активности која представља акт агресије без примене очигледног агресивног понашања. У најкраћем, ова операција је, војнички гледано, идеална. Резултати овакве операције оправдавају сваки динар уложен у њену припрему. Она је карактеристичан пример новог облика ратовања, који постоји паралелно са традиционалним, физичким ратовањем и појачава му ефекте. Сајбер ратовање не може се посматрати из угла и у истој равни са традиционалним ратовањем, већ као његов катализатор и супституит у многим ситуацијама. Сајбер рат можда се и неће водити још дуго, али се сајбер операције и ратовање воде већ неко време и то веома успешно.

Иако се може рећи да је *Стакснет* имао ограничено дејство, јер је само одложио реализацију иранског нуклеарног програма, да ли је заиста тако? Прошле године познати аналитичар вашингтонског Центра за међународне стратешке студије (CSIS), Ентони Кордесман, који важи за једног од најозбиљнијих војних аналитичара у САД са блиском везама са званичним војним естаблишментом, са сарадницима је извео у јавности најкомплетнију и најобимнију хипотетичку студију о војним могућностима војске САД и Израела да предузму превентивну војну акцију за уништење нуклеараних потенцијала Ирана. У њој је набројао и анализирао све војне потенцијале ове три државе, од броја бомбардера

Фото: Сателитска фотографија тајног, најјаче утврђеног нуклеарног постројења „Фордов" у Ирану, поред светог града Ком, укопаног дубоко у планину.
Извор: АР

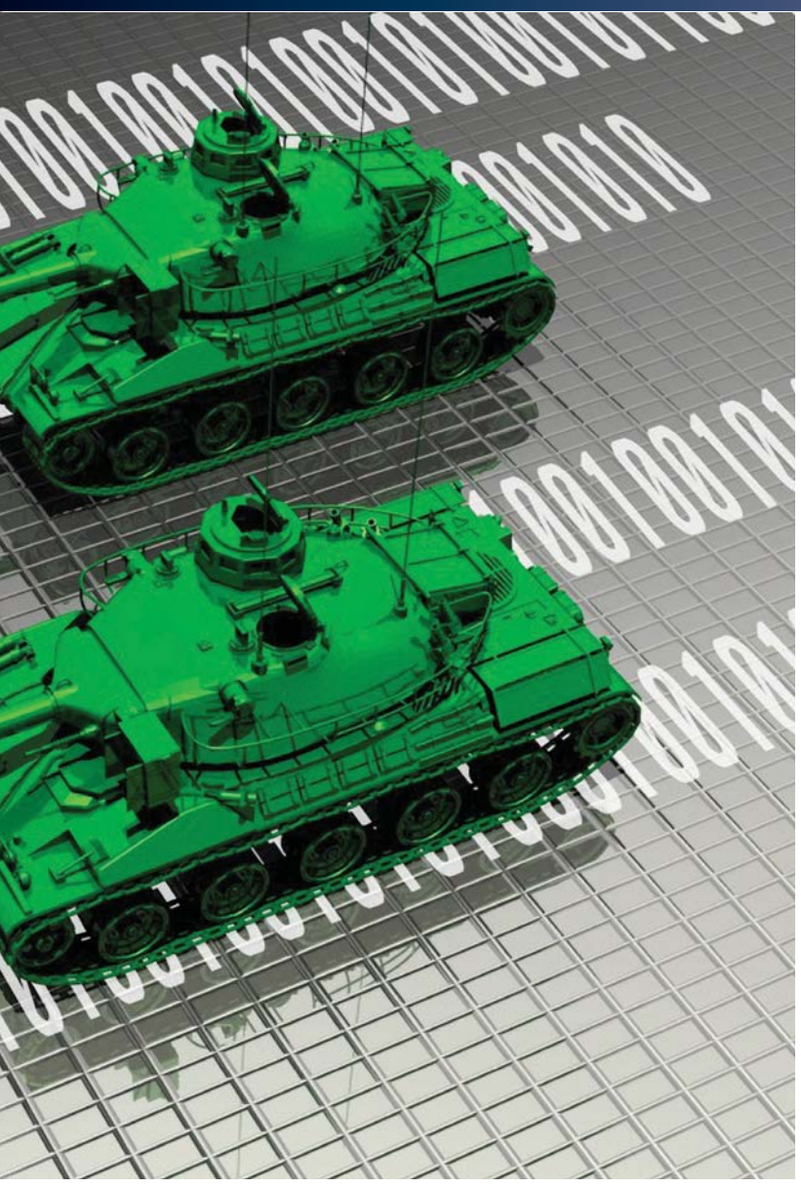
до врсте бомби које могу бити употребљене за напад, укључујући нуклеарне и конвенционалне, па чак и нови модел масивне бомбе за пробијање утврђених нуклеарних бункера, тешке 15 тона (Massive Ordnane Penetrator), коју за специјалне потребе, попут ове, производи Боинг (и која се наводи системом GPS, дакле дигиталном технологијом). Сва ова војна технологија у његовом закључку не би била у стању да трајно заустави развој иранског нуклеарног програма, већ би га само успорила за краћи број година (самосталним нападом Израела до две, а масовним нападом САД до десет година). Да не говоримо о чињеници да би производња и промет сировом нафтом у свету био потпуно поремећен. Поред тога, крајем прошле године, амерички званичници су јавно изразили сумњу да икакве конвенционалне бомбе, па чак и претходно поменута, могу да униште појединa утврђена подземна нуклеарна постројења у Ирану. Они стога предлажу употребу тактичког нуклеарног наоружања.

Рачунарски програми *Стакснет*, *Флејм* и *Дјукју* успели су оно што можда не би могла да учини ни конвенционална супербомба МОР. Није извесно да ће у неком будућем рату бити употребљене балистичке ракете са нуклеарним бојевим главама, али је сасвим извесно да ће у већини будућих сукоба уз конвенционално наоружање бити употребљени сви могући облици сајбер и електронског ратовања.

Принцип напада је исти као у већини случајева. Познајући недостатак, нападач га искоришћава и остварује физички приступ систему или мрежи. Након тога покреће напад или, што је чешће, подмеће софтвер који извршава циљ напада. Међутим, операција пометања малвера Стаскнет никако се не може сматрати искључиво сајбер операцијом, јер су програмери морали имати детаљне и потпуно тачне информације о нападнутом систему, начину његовог рада, уграђеним компонентама, процесима у систему, распореду итд. Поред тога, нуклеарно постројење је закопано дубоко под земљом у једној од најтајнијих места у Ирану, који годинама живи под претњом војног напада из САД и Израела и нико не очекује да нуклеарни уређаји буду повезани на интернет. Зато је било неопходно да се дође до самог система и мануелно подметне малвер у систем. *Стакснет* је стога првенствено специјална војнообавештајна операција са ефикасним сајбер завршетком. Међутим, не зна се где јој је почетак. Годину дана након откривања овог малвера у дневном листу *Њујорк тајмс* објављена је презентација немачке компаније Сименс о заједничком напору стручњака ове компаније са стручњацима Ајдахо националне лабораторије у САД на откривању недостатака на SCADA уређајима, који аутоматски управљају и надзиру индустријске системе у многим областима, међу којима су били и програмабилни логички контролери Simatic-300 и S7-400. У сваком

случају, до ових широко распрострањених индустријских управљачких уређаја било је лако доћи.

По писању штампе, подаци до којих су удружени истраживачи дошли предати су службама америчке и израелске владе, којима су послужиле као полазна основа за стварање малициозног програма. Ову тврдњу касније су одбиле обе истраживачке куће. Иако се творац тог малог, али моћног програма може само претпоставити, поуздано се знају ефекти његовог дејства. Он је заразио системе најмање 14 постројења која су довођена у везу са обогаћивањем уранијума или другим сегментима иранског нуклеарног програма. *Стакснет* је био пример драгуља међу рачунарским црвима (црви су малициозни програми који имају способност да се самостално шире зараженим мрежама) и историја ће га сигурно запамтити. Своју функцију остварио је кроз три етапе, показујући да су његови програмери тачно знали све појединости око функционисања циља. *Стакснет* је функционисао на основу искоришћавања најмање пет zero-day недостата-



ка и два украдена дигитална сертификата. Користио их је да би дошао до софтвера рачунарске опреме у индустријским постројењима компаније Сименс.

Стакснет је развијан дуго и озбиљно и писан је у неколико програмских језика, укључујући и C и C++. Тако обиман и озбиљан рад на сајбер нападу не би се исплатио ниједној криминалној организацији, па се само на основу обима пројекта поуздано може тврдити да је реч о сајбер ратовању. До сада је откривен већи број различитих верзија овог софтвера, чијим упоређивањем се јасно види временска хронологија развоја пројекта. Најстарија верзија датира из новембра 2005. године, а била је у оперативној употреби између 2007. и 2009. године.

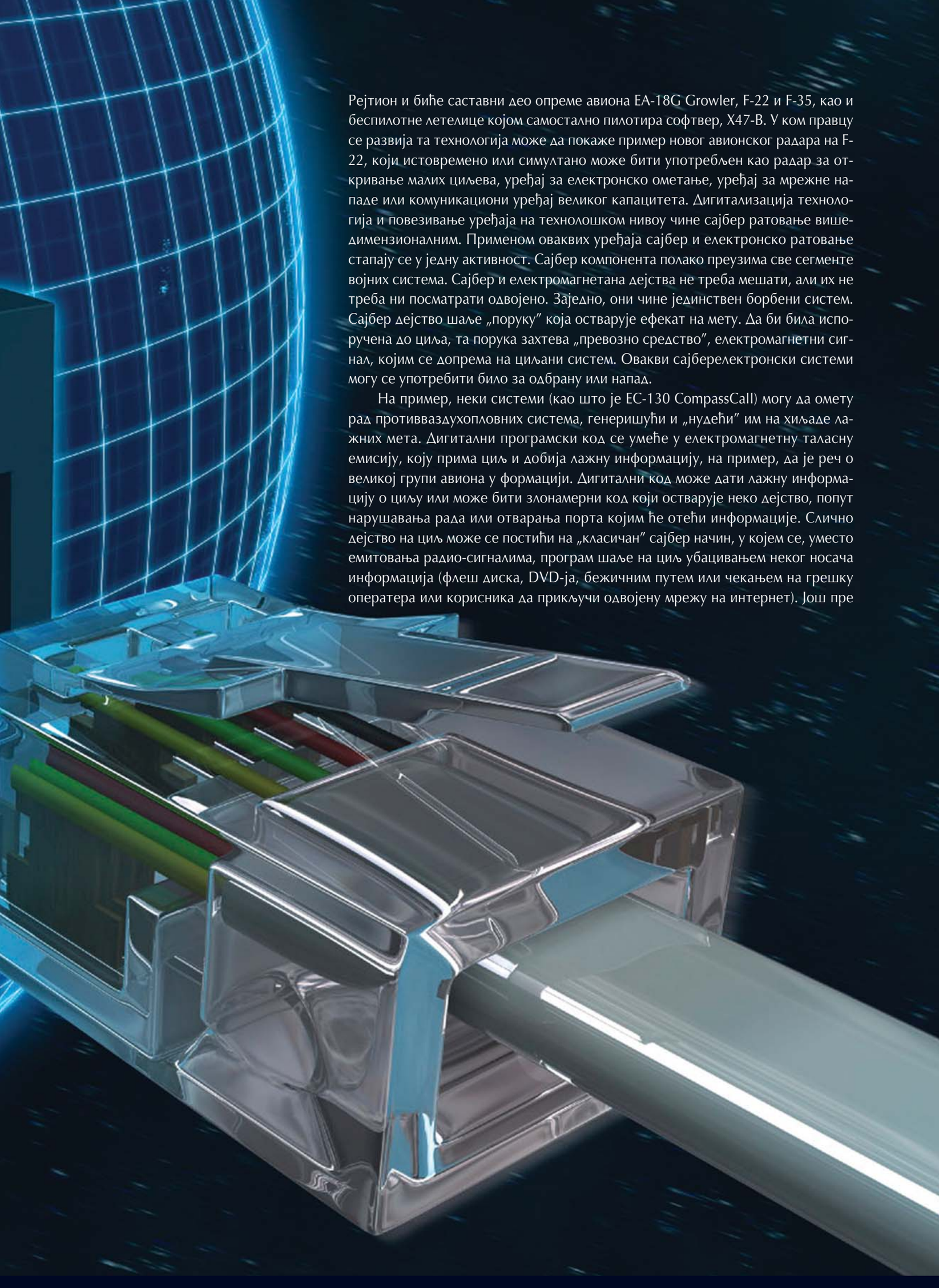
Недуго након објављивања открића малвера *Стакснет*, на интернет форумима појавио се велики број неформалних извора на којима је било ко могао преузети декомпајлиране делове изворног кода. Први који је то учинио био је један египатски студент, који је почетком 2011. године превео и објавио један важан драјвер, део *Стакснета*, који је служио да се превари оперативни систем рачунара употребом лажног дигиталног сертификата. У међувремену се на интернету појавио велики број извора са којих је могуће преузети различите верзије програмских кодова написане у вишим програмских језицима, по угледу на *Стакснет*. Сви они могу бити употребљени у прилагођеној форми у функцији нових злонамерних програма за нове нападе. Поред *Стакснета*, постоје и други програми, попут *Дјукју* (Duqu) и *Гаус* (Gauss) малвера, за које аналитичари сматрају да деле део изворног кода оригиналног *Стакснета*. Нико не зна да ли су аутори ових програма исти, па су употребили делове претходног рада, или се ради о новим играчима, који су одлучили да копирају делове разрађеног софтвера. Поседовање изворног кода није довољно за предузимање нових напада на исте системе, већ их је потребно укомпоновати са деловима који специфично одговарају новим метама. Такође, потребно је обезбедити и нове дигиталне сертификате, како би се несметано извршавао унутар оперативног система рачунара циљаног система. Иако није лако доћи до украденог дигиталног сертификата, који је лична карта сваког програма, крађе оваквог типа су релативно честе широм света. Иначе, крађе дигиталних сертификата не служе ничему другом, сем за креирање нових сајбер напада.

Нико не зна колико је недостатака *Стакснет* користио за напад и да ли су сви откривени. Сименсових програмабилних индустријских контролера има по целом свету и остаје нам да се надамо да су пронашли и отклонили све недостатке у софтверу који је компромитовао *Стакснет*. Simatic уређаја има и код нас, а контролишу велики спектар разних индустријских постројења, као што је, на пример, рад енергетског блока у Фијатовој фабрици аутомобила у Крагујевцу.

Спој електронског и сајбер ратовања

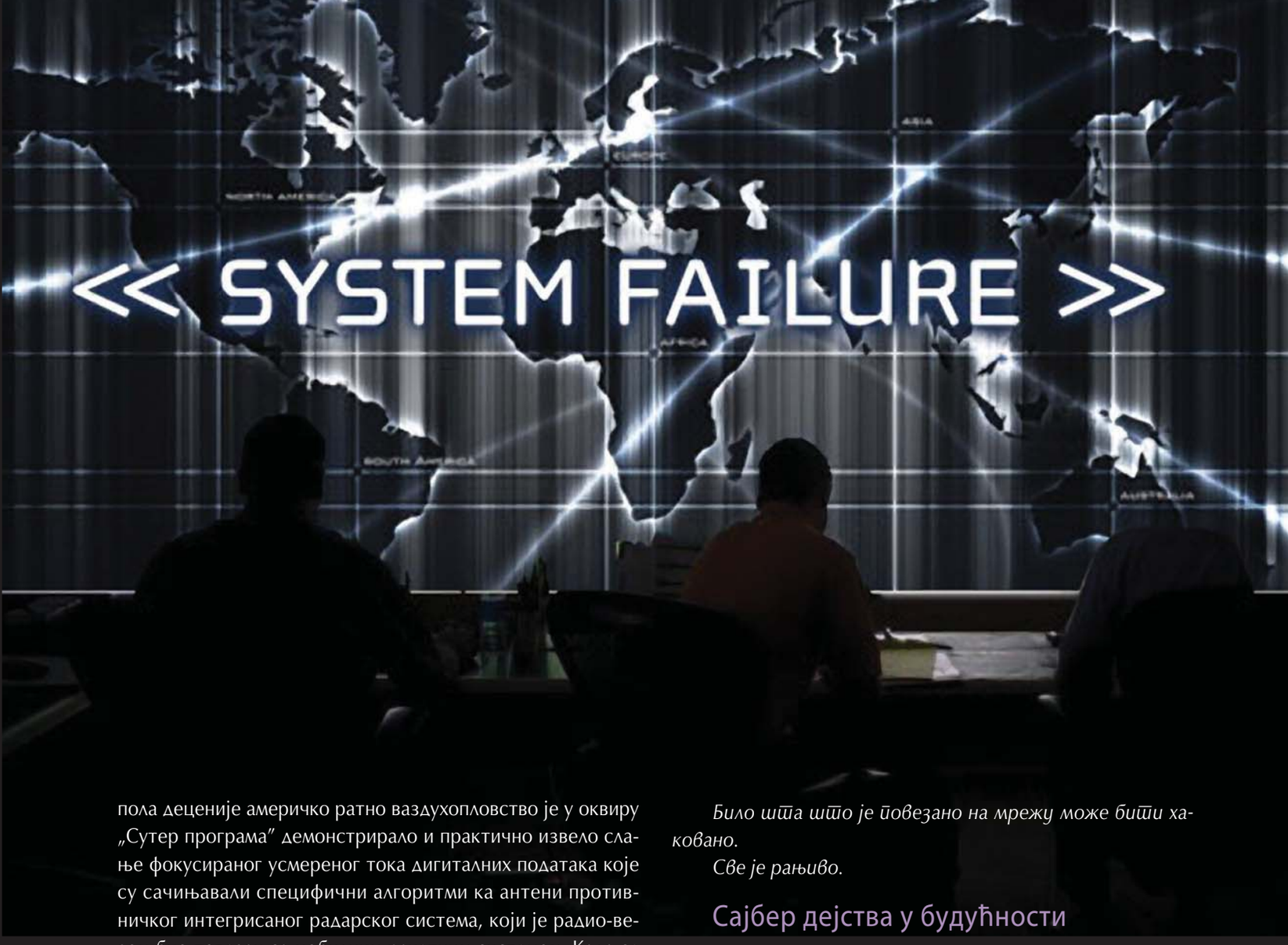
Одобравање огромних износа за истраживање и развој технологија које комбинују електронска дејства и сајбер ратовање у многим армијама света данас је често и логично. Све борбена средства и опрема постали су зависни од електронике, рачунарских технологија и мрежа, софтвера и дигиталних података. А како се види у претходним примерима, на њих се итекако може активно утицати. Високотехнолошке армије стога ужурбано доносе одлуке да развијају овакве системе да би их нападали у подручју у којем су најосетљивији: електромагнетном спектру.

Један од највећих добитника у предлогу новог војног буџета САД је морнарички електромагнетни ометач нове генерације, авионски уређај, намењен за ометање противничке електронике, даљинско детонирање бомби, слање малициозног софтвера бежичним путем у противничке рачунарске мреже и за сличне, до сада незамисливе активности. За потребе његовог истраживања и развоја предвиђено је више од четвртине милијарди долара. Развија га компанија



Рејтион и биће саставни део опреме авиона EA-18G Growler, F-22 и F-35, као и беспилотне летелице којом самостално пилотира софтвер, X47-B. У ком правцу се развија та технологија може да покаже пример новог авионског радара на F-22, који истовремено или симултано може бити употребљен као радар за откривање малих циљева, уређај за електронско ометање, уређај за мрежне нападе или комуникациони уређај великог капацитета. Дигитализација технологија и повезивање уређаја на технолошком нивоу чине сајбер ратовање вишедимензионалним. Применом оваквих уређаја сајбер и електронско ратовање стапају се у једну активност. Сајбер компонента полако преузима све сегменте војних система. Сајбер и електромагнетана дејства не треба мешати, али их не треба ни посматрати одвојено. Заједно, они чине јединствен борбени систем. Сајбер дејство шаље „поруку" која остварује ефекат на мету. Да би била испоручена до циља, та порука захтева „превозно средство", електромагнетни сигнал, којим се допрема на циљани систем. Овакви сајберелектронски системи могу се употребити било за одбрану или напад.

На пример, неки системи (као што је EC-130 CompassCall) могу да омету рад противваздухопловних система, генеришући и „нудећи" им на хиљаде лажних мета. Дигитални програмски код се умеће у електромагнетну таласну емисију, коју прима циљ и добија лажну информацију, на пример, да је реч о великој групи авиона у формацији. Дигитални код може дати лажну информацију о циљу или може бити злонамерни код који остварује неко дејство, попут нарушавања рада или отварања порта којим ће отећи информације. Слично дејство на циљ може се постићи на „класичан" сајбер начин, у којем се, уместо емитовања радио-сигналима, програм шаље на циљ убацивањем неког носача информација (флеш диска, DVD-ја, бежичним путем или чекањем на грешку оператера или корисника да прикључи одвојену мрежу на интернет). Још пре



пола деценије америчко ратно ваздухопловство је у оквиру „Сутер програма" демонстрирало и практично извело слање фокусираног усмереног тока дигиталних података које су сачињавали специфични алгоритми ка антени противничког интегрисаног радарског система, који је радио-везом био повезан са мобилним ракетним системом. Када се дигитални алгоритми нађу унутар рачунарског система радара, могу утицати на његов рад тако да радар, уместо откривања циља, врши откривање самог себе, шаљући податке у форми радарског зрачења ка летелици или на други начин омете или онеспособи рад рачунарског система. Циљ експеримента било је онеспособљавање рада противавионског система усмереним слањем података.

Сваки савремени циљ електронског напада постао је нека врста рачунарске мреже (у било ком дистрибуираном облику) који користи неки вид бежичне комуникације са другим мрежама, системима или сензорима. Такви уређаји користе се са авионима са стелт технологијом, велике брзине и висине лета, који могу продрети дубље у непријатељски простор који штите све бољи радари и ракете већег домета. Свети грал ваздухопловних електронских дејстава је систем који је способан да активно претражује подручје у пуном кругу од 360 степени, извршава електронски напад на противваздухопловне системе и мрежни упад у рачунарске системе и мреже, док је сам истовремено потпуно неприступачан за свако електронско и сајбер дејство противника. Уколико је радарски систем повезан на неку иформациону или рачунарску мрежу могуће је остварити сајбер дејство на њега. Такав концепт дејства потврђује теорију Рода Бекстрома, бившег председника ICANN-а и Националног центра САД за сајбер безбедност:

Било шта што је повезано на мрежу може бити хаковано.

Све је рањиво.

Сајбер дејства у будућности

Иако изгледа страно и необично, сајбер ратовање није толико сложено. Потребно је само да се уместо специфичне врсте наоружања у њему користи цело једно подручје информационих и рачунарских технологија, да се уместо оружја користе недостаци у тим технологијама, а да се уместо муниције користе експлоити и други малициозни програми. Замислимо још и да га не морају примењивати само оружане снаге, већ да могу бити укључени сви они који иначе вешто користе те технологије, укључујући и тинејџере. Оно што су материјални ресурси и жива сила у традиционалном ратовању, то су знање и вештина у сајбер ратовању. Замислимо да све то можемо применити потпуно прикривено и против непријатеља и против савезника. Уместо праска експлозије пројектила или бомбе замислимо отказ било ког система чији рад зависи од информационих и рачунарских технологија и све ће нам у вези сајбер ратовања бити јасно.

Можда нације и државе никада неће једне против друге ратовати искључиво сајбер оружјем, али је сигурно да ће сви примењивати сајбер дејства у будућности. Без обзира на то да ли је реч о државама Запада или Истока, о богатим и војно моћним државама или не, за успех у подручју сајбер ратовања неопходно је пронаћи магични однос између интереса одбране, политике, безбедности, бизниса, науке и појединаца. ■