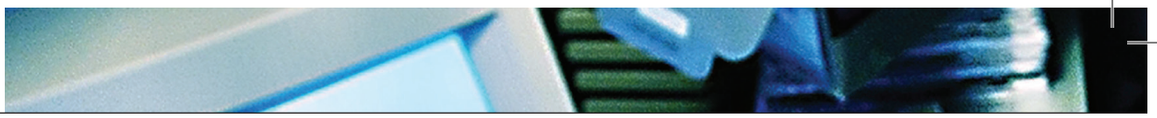
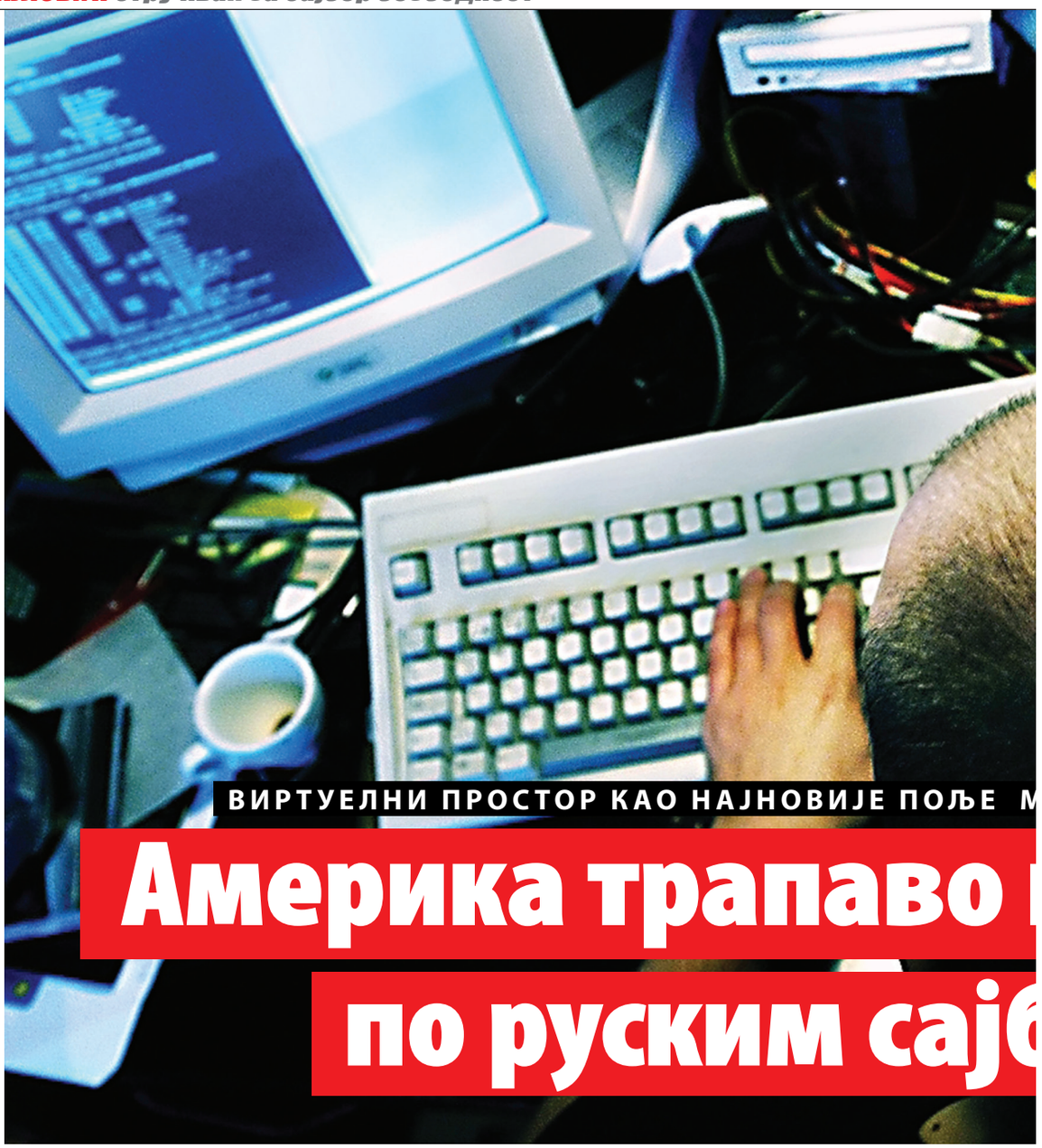




ВИРТУЕЛНИ ПРОСТОР КАО НАЈНОВИЈЕ ПОЉЕ М

Америка трапаво
по руским сајб

Да се којим случајем бира председник Новог светског поретка, мултимедијске сајбер кампање! Русија је у 2014. години Едвард Сноуден је у Москви, Џулијан Асанж неуморно у украјинску кризу, Оливер Стоун оштро критикује Обамину оријентисану позицију, уз гласно неодобравање понашања

Разговарала
ДИЈАНА ИВАНОВИЋ

С професором Радомиром Михајловићем, једним од оснивача постдипломских студија за смер сајбер безбедност на Њујоршком институту за технологију (NYIT) и на Метрополитан универзитету у Београду, као првих академских студијских програма такве врсте у САД и Европи, разговарамо о сајбер ратовању и том простору као новом домену војних сукоба, спрези медијског и сајбер ратовања, (не) безбедности врхунски чуваних система за аутоматско управљање нуклеарним постројењима, нападу на сервере „Сонија“ у Холивуду, о нашим дигиталним телефонима и дигиталним телевизорима као потенцијалном оружју у рукама сајбер ратника, специјалним сајбер јединицама модерних војски света...

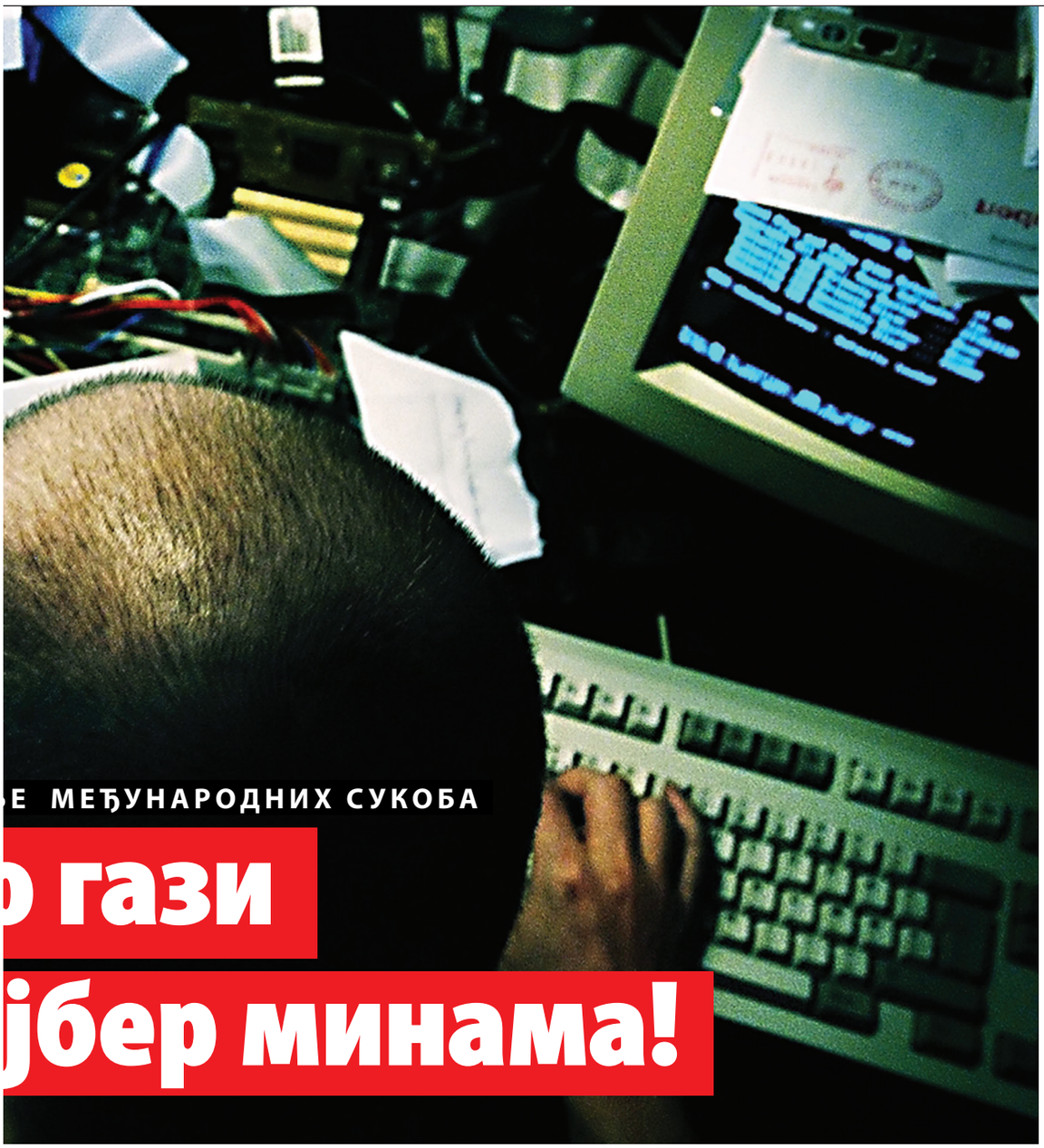
Сведоци смо недавних вести о масовним хакерским нападима на велике америчке корпорације, које, по неким експертима, указују на Северну Кореју као земљу са чије се територије лансирају сајбер напади на Сједињене Државе. Постоје многе дефиниције сајбер рата – о чему се ту, према вашем схватању, заправо ради, шта је сајбер рат?

Сајбер рат би најбоље био дефинисан као рат у виртуелном простору или сајбер домену, који је у свим модерним војним доктринама, а пре свега америчким, прихваћен као нови легитимни простор са могућим војним конфликтима. Познати су домени војних сукоба – копно, море, ваздух и васиона. Овим доменима је недавно придодат и сајбер простор као виртуелни простор.

Дефиниција сајбер рата као војног конфликта преко интернета није ваљана, јер се не уклапа у прецизно одређење сајбер простора. Наиме, сајбер простор је простор са свим рачунарским машинама и програмима, умреженим и неумреженим. У случају умрежења, интернет би био само једна од технологија умрежавања, базирана на познатом систему протокола TCP/IP, а сајбер простор би био целокупни дигитални простор са свим постојећим дигиталним уређајима и придруженим програмима, наравно уз све дигитализоване податке. Илустрације ради, ваш дигитални телефон или дигитални телевизор су елементи сајбер простора и потенцијално оружје у рукама сајбер ратника. Према сликовитом приказу сајбер простора, сајбер оружје би могло да буде чак и веб страница или пак податак на веб страници.

Како се концепт сајбер рата примењује на нове структуре војних снага великих сила? И ко је отишао најдаље у реорганизацији својих војних и полицијских снага?

Све војске развијеног дела света, укључујући ту и Војску Србије, имају данас специјалне јединице такозваних сајбер ратника. Сајбер ратници се деле



Е МЕЂУНАРОДНИХ СУКОБА

о гази

јбер минама!

Путин би убедљиво добио Обаму због своје много успешније добила интелектуални виртуелни рат. Сајбер суперратник објављује компромитујуће материјале о америчкој уплетености администрацију, док Ноам Чомски уредно заузима лево великих корпорација и званичне политике САД

на сајбер ратнике у униформи и у цивилу, где ових других има много више. Сличан је случај и са полицијским снагама развијенијих држава. На моје велико задовољство, све је више униформисаних посетилаца Београдске годишње BISEC конференције о сајбер безбедности, чији сам иницијатор и један од суоснивача, а која се одржава једном годишње већ шести пут заредом.

Најдаље у реорганизацији војних и полицијских снага свакако је отишла и најугроженија држава у сајбер простору, САД. Она је највише отворена у сајбер простору, са несразмерно већим ризиком од катастрофалних губитака у случају успешних сајбер напада од стране било које земље света. На пример, војне снаге ове најмоћније силе имају сајбер команду при свим родовима војске, при армији, морнарици, авијацији и морнаричкој пешадији. Рецимо, САД имају армијску сајбер команду, где армија означава пешадију и јединице опремљене самоходним возилима, тенковима, борним колима итд. Ту су, такође, и

> **Врховни командант НАТО снага за Европу Филип Бридлав: Русија води запањујући информациони „блицкриг“, досад невиђен у историји информационог ратовања**

сајбер команде америчке флоте, USFLTFORCOM, авијације AFCYBER итд. Сајбер команда – USCYBERCOM јесте централна команда, која је под контролом USSTRATCOM-а (Централне стратешке команде Америчких снага).

Вратићемо се касније великој рањивости држава које су најотвореније у сајбер простору и (не)безбедности њихових стратешких дигитализованих система. Али да бисмо то правилно разумели, објасните нам природу везе између медијског или информационог рата и сајбер ратовања?

Класични рат, па и сајбер рат, представљају неку врсту мултидимензионалне и мултиполарне социјалне појаве. Сајбер рат је, такође, социјална појава због неизбежног присуства интеракције човека са човеком, мултиполарна појава јер је могуће сучељавање више јасно издвојивих центара сајбер моћи, а вишедимензионална, јер може да ангажује различите имплементације електронске инфраструктуре. Како је основни облик модерних информационих технологија заснован на електронској инфраструктури, то је информациони рат један од видова или праваца сајбер напада.

Обрада података и њихова електронска размена су у тесној вези са обрадом и преносом информација. Појам података и информације треба јасно раздвојити. То су две повезане, али различите ствари. Податак је носилац информације, где ин-

„Тотална интернет блокада једне земље, па макар то била и озлоглашена земља попут Северне Кореје, по многима би била апсолутно неприхватљив вид сајбер агресије. Случај недавног искључења ове државе је опомена свим земљама света да се припреме за такву могућност“

Професор Радомир Михајловић

формација означава семантичку вредност податка. Семантика је наука о значењу, или наука о томе како људи разумеју, односно интерпретирају податке. Манипулација подацима и њиховим преносом, како би група људи на мети сајбер напада разумела одређене податке на начин пожељан од стране нападача, по дефиницији је истовремено информациони, а и сајбер напад.

Термини „медијски рат“ и „информациони рат“ се тако суптилно разликују, изгледа као да нису намењени истим конзументима?

Атрибут медијски се више односи на платформу имплементације рата, док се атрибут информациони односи на семантички карактер извођених операција. У вези са тим, интересантно је поменути изјаву генерала Филипа Бридлава, врховног команданта НАТО снага Европе (SACEUR) на НАТО самиту у Велсу септембра 2014. године. Генерал Бридлав је изјавио да Русија води „запањујући информациони ‚блицкриг‘, досад невиђен у историји информационог ратовања“. По мом мишљењу на тему конфликта између Русије и англоамеричког блока у Украјини, руске информационе снаге су установиле у сајбер простору до сада заиста невиђену форму бојног поља – назовимо га „интелектуалним ратиштем“. Традиционална употреба пропаганде је ефектно применљива на интелектуално просечну популацију, која конзумира садржаје класичних медија као што су радио, телевизија и штампа. У самој Русији су класични медији ефикасно ангажовани на стишавању уобичајене политичке гужве, као и на промоцији јединства постојећег естаблишмента. На спољнополитичком плану прилаз је био другачији. Природа саме технологије и начин коришћења интерактивних мултимедијалних садржаја преко интернета имају за резултат одређену сегрегацију публике, са фокусом на компјутерски писменој, образованијој и рационалнијој публици. То су руске информационе снаге одлично сагледале и интензивно се обратиле доминантно рационалним становницима у сајбер простору. Чини се да је Русија у 2014. години добила интелектуални сајбер рат. Сајбер суперратник Едвард Сноуден је у Москви, Џулијан Асанж неуморно објављује компромитујуће материјале о америчкој уплетености у украјинску кризу, Оливер Стоун оштро критикује Обамину администрацију, док Ноам Чомски уредно заузима лево оријентисану позицију, уз гласно неодобравање понашања великих корпорација и званичне политике САД.

Да ли то значи да Путин придобија интелектуалну елиту Запада у сајбер простору?

Да! Да се којим случајем бира председник глобализованог света, после много успешније мултимедијске сајбер кампање, Путин би убедљиво победио Обаму. Како западни, тако су и руски интелектуалци листом уз Путина.

Ипак, у реалном свету позиције моћи су обрнуте. Како се такав утицај из виртуелног света преноси у физичку реалност, од чега може да зависи брзина транспоновања сајбер доминације у сферу материјалног света?

Захваљујући улагањима астрономских размера, позиције моћи у реалном свету су заиста обрнуте. Међутим, многи доводе у питање оправданост таквих улагања када је обрт ситуације лако могућ по много нижој цени. Прецизније, у односу на широко прихваћену ситуацију, интелектуална елита углавном игра улогу ђавољег адвоката и својим растом до одређене критичне величине лако покреће такозване „револуције“. У случају текућег информационог рата, виртуелни сајбер простор служи као нека врста замајца, акцелератора интелектуалне синхронизације умова у сајбер простору, умова опречно постављених у односу на тренутне правце деловања англоамеричког естаблишмента.

Да ли је Украјина добар и најактуелнији пример медијског сајбер ратовања?

Испада да је позитиван одговор на ово питање прави одговор. Ја бих као конкретну илустрацију релевантног медијског сајбер рата издвојио рат тролова (енг. Troll war) који је достигао највећи интензитет управо у току украјинског грађанског рата.

Евидентно је да се у Украјини води брутални грађански рат, иза којега индиректно ратују САД и Русија. Европска унија је присилни учесник. Паралелно са, да кажем, „врућим“ ратовањем, у којем гине хиљаде људи и уништавају се милијарде долара приватне и јавне имовине, одиграва се класични медијски рат тенденциозног или непотпуног информисања, као и конкретни медијски сајбер рат.

По дефиницији, „тролинг“ би био термин који, са једне стране, означава семантички интернет вандализам, где тролови својим грубим коментарима нападају садржај одређених мултимедијалних веб страница или садржај претходно постављених порука других тролова, док са друге стране, означава један вид колаборационе продукције динамичког садржаја активних веб страница. Тролови започињу провокативне расправе на интерактивним сајтовима. Трол који је иницирао лавину повратних порука јесте успешан трол.

Трол ратници се сукобљавају и на бенигним сајтовима као што су Фејсбук или Јутјуб, али се најжустрије ратује на сајтовима са вестима и на популарним геополитичким блоговима. Политика различитих интерактивних сајтова у односу на трол ратнике варира. Рецимо, модератор Би-Би-Сијевих страница не дозвољава радикалне и неизбалансиране коментаре, тако да је ту трол ратовање нешто мање динамично, да не кажем мање узбудљиво. Са друге стране, модератори Информационе агенције РТ не филтрирају трол коментаре, па се на њиховим страницама подиже огромна сајбер прашина од силног троловања. На РТ сајтовима се јуначки боре и српски трол ратници, од којих бих издвојио Дарка Дакића и Драгана Радуловића. Њихови коментари су чести а углавном добијају значајан одзив. Поред трол бојишта, интензивни сајбер конфликти се понекад одвијају преко Твитер система. Новија вест је да ирански ајатолах Али Хамнеј преко свог твит-налога води кампању против председника Обаме. Ту, значи, имамо сукоб два врхунска политичара у дубоком конфликту, у реалном, а и у сајбер простору. А најновија је вест да су снаге сајбер калифата Исламске Државе успешно

извеле напад на Твитер налоге Централне команде САД (CENTCOM).

Википедија је, такође, често мета трол конфликта и тенденциозног искривљавања чињеничног стања.

Да ли трол ратовање, као и сваки други облик рата, има своје циљеве и стратегије?

И те како! Трол ратиште има врло озбиљне ратне циљеве, са озбиљним стратегијама и тактикама организованих трол ратника. Трол ратници могу да буду индивидуални сајбер герилци, као што су поменути Дарко и Драган, а могу да буду и припадници организованих трол јединица. Поред жустрог семантичког надметања, на трол ратишту можемо често да приметимо неке интересантне појаве. На пример, гушење оригиналног тролера је манифестација тактике организованих трол јединица (групе или тима трол ратника) коришћене у оквиру стратегије спречавања нежељеног утицаја на публику датог сајта. Када би, рецимо, један трол ратник уверљиво подржавао или нападао постављену страницу оригиналним аргументима, против таквог ратника би се покренуо тим непријатељских тролова, који би или брутално омаловажавали оригиналног трол ратника или би масом невезаних порука утопили вредну поруку у безвредне коментаре. Нека истраживања указују да се у нападима на оригиналну страницу или трол поруку, типа трол димне завесе, трол ометања или трол спеминга, користе трол дронови, програми за аутоматско генерисање трол порука.

Такође, треба напоменути да се сва трол бојна поља пажљиво осматрају од стране сајбер снага заинтересованих држава. Трол бојна поља су извор драгоцених информација које могу да утичу на одговарајуће промене курса у ратним операцијама у реалном простору. Учешће у трол конфликтима у виду аналитичког посматрача могло би се сматрати тактиком пасивног ратовања.

Шта мислите о недавном севернокорејском нападу на мултинационалну корпорацију „Сони“?

Према изјавама ФБИ, по експертима „Сони“ корпорације, као и по стручњацима неколико специјализованих компанија за анализу сајбер напада на радне станице и сервере „Сонија“ у Холивуду, тај досада невиђени напад изванредно је планиран и изведен са злоћудним програмима, који су, недетектовани, дуго активно радили на уништењу великог броја рачунара, као и на изношењу масивне количине података веће од 100 терабајта. Без много образлагања, кривица за напад је приписана једној од најслабије технолошки опремљених војних сила, Северној Кореји. Чињеница је да кинеске сајбер снаге периодично испробавају различита сајбер оружја лансирана са севернокорејске интранет мреже. По дефиницији, интранет је јасно дефинисана подмрежа интернета у власништву и под контролом једне одговорне организације.

Појачане америчке санкције према Северној Кореји следиле су објаву да је напад потекао из ове земље. Изјаве, које примамо са дозом природне резерве у оваквим случајевима, указују да је напад започео брисањем података на „Сонијевим“ серверима. Брисање података је већ виђено у случајевима напада на сервере у Јужној Кореји у марту 2013. године, као и на сервере у Саудијској Арабији у октобру 2012. године.

„Ирански ајатолах Али Хамнеј преко свог твит-налога води кампању против председника Обаме. Ту имамо сукоб два врхунска политичара у дубоком конфликту, у реалном, а и у сајбер простору“

Захваљујући интелектуалцима, Путин би потукао Обаму у виртуелном избору за глобалног председника

Да ли је уопште јасно како је откривено да је напад лансиран управо из Северне Кореје и како је напад извршен, готово савршено, из земље која се не може похвалити нарочитим технолошким стандардом? Доводи ли то у сумњу оптужбе против Северне Кореје?

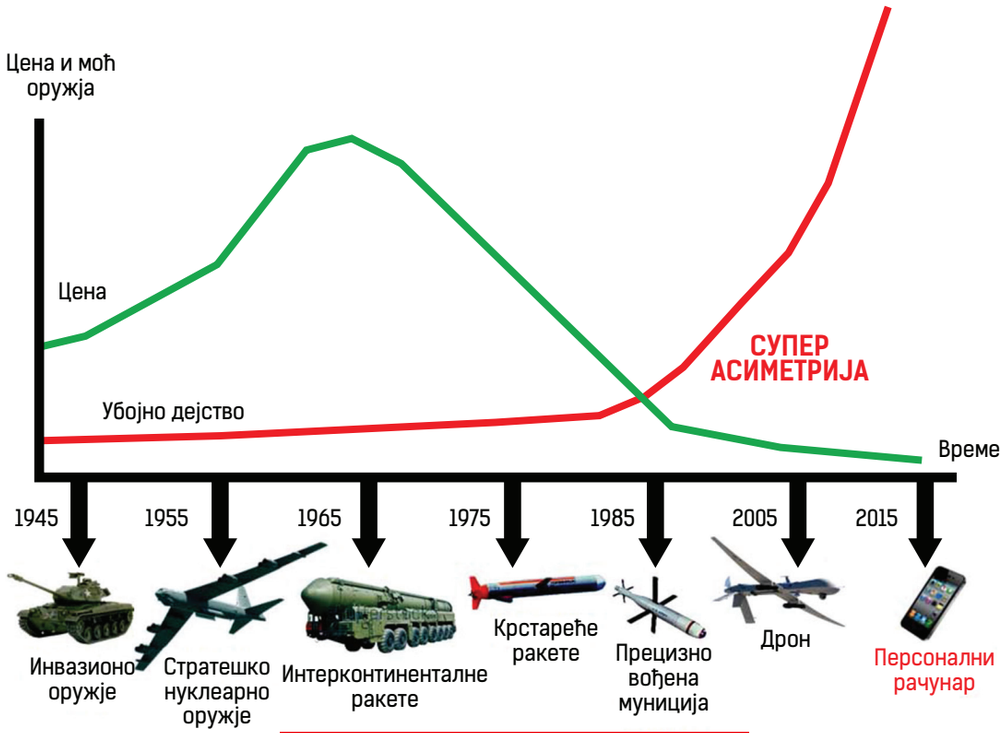
Северна Кореја је повезана на интернет преко само једног провајдера из Кине и због тога је врло отежано да се у сервере у Северној Кореји упада или да се неоткривено преноси велика количина података у било којем смеру. Међутим, напад и затварање излаза на интернет преко само једног провајдера врло је лако, што се видело у сајбер контранападу који је из Америке лансиран на националну мрежу ове земље 22. децембра 2014, највероватније масивним нападом укидања мрежног сервиса. У периоду од око 10 сати све комуникације Северне Кореје преко интернета су биле укинуте.

Многи теоретичари завера тврде да је маса украдених података из „Сонија“ завршила не у Северној Кореји, већ у лабораторијама Националне агенције за безбедност НСА.

Да ли је сајбер контранапад на Северну Кореју био изведен само као одговор на напад на „Сони“ или су ту могући и неки други мотиви?

Поред неког вида одмазде, интернет помрачење Северне Кореје је највероватније било могући пробни маневар сајбер снага САД како би се тестирало извесно сајбер оружје. Изостанак било каквог коментара или категоричног порицања званичника САД ствара оправдане околности за овакве претпоставке.

Искључење једне земље са интернета је први пут помињано недавно као претња и додатна ужасна могућност блокаде Русије због наводне инвазије на Украјину. Тотална интернет блокада једне земље, па макар то била и озлоглашена земља попут Северне Кореје, по многима би била апсолутно неприхватљив вид сајбер агресије. Случај недавног искључења ове



Модерна историја цене и ефективности оружја од Другог светског рата па до данас

државе је опомена свим земљама света да се припреме за такву могућност. Мишљења сам да се овакав вид сајбер агресије мора забранити посебном конвенцијом Уједињених нација.

Које је, по вама, најопасније сајбер оружје до сада виђено?

Већина напада на сајбер мете су базирани на малициозним програмима познатим као сајбер црви (енг. Worms). Сајбер црви се користе директно или индиректно у току извршења сајбер напада. Примера ради, при нападу на корејску националну мрежу коришћено је комбиновано, директно и индиректно дејство сајбер црва. Вероватно најдеструктивнија врста сајбер црва је такозвани стакснет црв (енг. Stuxnet worm) који се користи за напад на индустријска постројења, односно на специјализоване рачунаре за контролу машина.

Прва верзија стакснета је употребљена 2009. године при нападу на нуклеарне центрифуге у Ирану. Већина безбедносних аналитичара сматра да је напад лансиран из Израела уз помоћ немачког „Сименса“, чији су PLK рачунари контролисали центрифуге, и подршку америчких сајбер снага. Развој стакснет софтвера је започео по директиви председника Буша Млађег, а тајним програмом познатим под именом „Олимпијске игре“ настављен је са доласком председника Обаме у Белу кућу. Сам напад на иранска нуклеарна постројења је као акт сајбер рата био темпиран у погрешно време а имао је и мало деструктивних ефеката. Уништење нуклеарних постројења није било сврха првог стакснет напада. Напад је за сврху имао да демонстрира изводљивост и потенцијалне могућности таквог сајбер оружја.

Да ли то значи да се стакснетом може напасти баш све!? Путнички авиони у лету, контроле летења, железничке скретнице, електродистрибуционе мреже или рафинерије? Шта је с банкарским системима?

Као што сам малопре напоменуо, стакснет се користи за напад на индустријска постројења аутоматизована малим рачунарима. За нападе на добро брањене велике рачунаре банкарских система користи се сајбер оружје које се драстично разликује од стакснета. Иначе, све у сајбер простору је мета потенцијалног напада широким спектром сајбер оружја.

Као одмазду за напад стакснетом, Иран је у лето 2010. објавио опис стакснет програма, тако да су сви хакери света могли да се са таквим злоћудним софтвером боље упознају. Логика Ирана је била да су САД, као најумреженија и најаутоматизованија земља на свету, највећа мета и највећи изазов за сајбер герилце, хактивисте и сајбер анархисте. Интересантно је напоменути да је у децембру 2014. објављен извештај по којем су иранске сајбер снаге у 2014. години напале више од 50 мрежа распоређених у 16 земаља. По свему судећи, стакснет напад из 2009. послужио је као велика инспирација иранским сајбер ратницима да се опробају широм света.

Да ли је могуће прићи рачунарима у врхунски чуваним системима, као што су системи за аутоматско управљање нуклеарним постројењима, без сарадње с оригиналним произвођачима опреме?

Како су критичне рачунарске мреже индустријских постројења углавном добро изоловане од јавне инфраструктуре интернета, типични продор стакснет сајбер црва се обавља физичком употребом меморијских USB „флешкица“. За такве сајбер нападе су потребни храбри сајбер диверзанти и њихово физичко присуство на простору нападнуте мреже, или сарадња са оригиналним произвођачима опреме.

Рачунари и секундарне меморије са заједничким приступом (енг. Net-shares) најчешће су добра подршка продуктивности тимова корисника, али су, при томе, и најопаснији системски елементи са којих се могу лако лансирати различити напади, као што је стакснет напад. У случају иранског стакснета, коришћени су комбиновано „флешкице“ и заједнички приступ ресурсима.

Поменули сте на почетку разговора Београдску BISEC конференцију, као један од њених кључних иницијатора. О каквом форуму је реч?

Као нека врста евангелисте сајбер безбедности, са неколико колега сам, пре десет година, покренуо програм постдипломских студија на NYIT-у у САД, а пре шест година смо тај исти програм транспоновали на Метрополитан универзитет у Београду како бисмо у Србији одржали корак са еквивалентним трендовима у свету. Паралелно са програмом безбедности на Метрополитан универзитету, уз велику помоћ Народне банке Србије и колега са Метрополитана, покренуо сам годишњу конференцију за сајбер безбедност BISEC. Сам назив конференције је идеја колегинице Оливере Лазаревић. Учешће наших униформисаних сајбер јединица на BISEC форумима кренуло је врло стидљиво, са неколико војних лица у цивилу, да би њихова посета постајала, из године у годину, све масовнија.

Како је критична важност сајбер безбедности драстично нарасла, прошле 2014. године, као суоснивач покренуо сам фокусирани постдипломски програм у области међународне и сајбер безбедности на Унион универзитету „Никола Тесла“ у Београду.