Кибертероризам

УДК: 327.88:007:621.391

Др *Слободан Р. Петровић*

У раду су обрађени неки аспекти кибертероризма, нове форме тероризма која настаје као последица, с једне стране, технолошке зависности и слабости савременог друштва узрокованих наглим ширењем и коришћењем информационе технологије, и настајањем, с друге стране, специфичног амбијента који, с аспекта терориста, нуди нова средства, методе и технике деловања и нове, веома атрактивне циљеве. У вези с тим, посебно су означене потенцијалне последице, као и специфичне карактеристике по којима се кибертероризам разликује од традиционалног тероризма. С обзиром на озбиљност и сложеност тог феномена, који има и међународни карактер, аутор је сугерисао основне правце за успешно супротстављање тој, новој, друштвеној опасности.

Увод

Садашњи свет је препун разних контроверзи проузрокованих политичким, социјалним, економским, расним, религиозним и разним другим односима, у чијем се разрешавању користе најразличитије методе: од мирољубивих и дипломатских до насилних и крајње бруталних метода. У екстремном разрешавању проблема издваја се тероризам – радикална стратегија под којом се подразумевају убиства, киднаповања, отмице, подметање бомби и слично ради постизања одређених терористичких циљева. Због тога је тероризам на најнепосреднији начин претња стабилности држава и безбедности њихових грађана која не би смела да се игнорише. Та форма психолошког ратовања,[1] у којем се убијање релативно малог броја невиних цивила користи као брутална порука мржње и страха стотинама милиона људи с намером да се изазове паника која ће се проширити кроз популацију и изазвати у одређеном периоду социопсихолошко стање нелагодности и несигурности, један је од највећих проблема савременог света. Међутим, тероризам није феномен савременог доба, јер су примери терористичког понашања веома бројни и досежу у далеку прошлост. Још је 500 година пре наше ере кинески генерал Сун Цу Ву био заступник специјалних јединица за нападе на владаре. Он је желео јаке и вичне људе, „навикнуте на све врсте радних дужности, способне да поднесу глад и зиму и да одбаце стид и срамоту".[2] Јеврејски фанатици водили су кампању терора против

[1] *The mythology of terrorism on the net,* Summer, 1995, http://www.t0.or.at/cae/mnterror.htm

[2] R. Thomson, *Terrorism,* Reuterlink:extra, The online newsletter of the Reuter Foundation Winter 1996/7, http://www.foundation. reuters.com/!terrori.htm

Римљана у 1. веку наше ере, док је секта *Shi ia Muslim,* позната као *Hashshashin,* која је дала литерарно значење речи атентатор у Енглеској, у 11. веку систематски убијала лидере и утицајне људе.[3]

Период након Другог светског рата може да се означи као доба модерног тероризма, а крај шездесетих и почетак седамдесетих година као почетак међународних терористичких инцидената. Захваљујући дугој и богатој традицији, као и искуствима које су бројне земље стекле у тој области у вези с мотивима, циљевима, стратегијама и тактикама терористичких организација, тероризам је идентификован, веома добро простудиран и детаљно документован. Међутим, и поред тога још увек нема општеприхваћене дефиниције тероризма, већ се користе бројне, мање или више сличне дефиниције, од којих су многе прагматичне.[4] Према једној од тих општих дефиниција тероризам је *политички мотивисано физичко насиље организованих група са намером да се изазове страх и лична несигурност грађана и да се угрози државни ауторитет.*

У тој традиционалној дефиницији, као и у већини других, постоји подела на следеће елементе: *политичка мотивација, организована група и физичко насиље.* Међутим, ти елементи, иако су потребни, нису довољни за обухватање нових и све бројнијих мотивационих чинилаца, форми организовања и начина терористичког деловања у савременим условима. На пример, само *политичка мотивација* искључује могућност терористичких активности због финансијских или религиозних циљева, а управо резултат наглог пораста и ширења транснационалних криминалних организација, увећања области њиховог дејства и размера њихових операција могло би да буде прибегавање терористичким акцијама ради остваривања финансијског профита као водеће мотивације. Ширење радикалног исламског фундаментализма указује на његову религиозну мотивацију, али она може да буде у тесној вези с политичком мотивацијом. Елемент *организоване групе* искључује терористичку активност појединца (који није укључен у групу) која је у последње време све чешћа и очигледнија, и која ће бити у сталном порасту првенствено због ширења оружја за информационо ратовање. Најзад, елемент *физичко насиље,* у традиционалном значењу, искључује примену софистицираних информационих форми ремећења и деструкције. Дакле, тероризам се стално мења и да би се могао целовито сагледавати, разумети и разрешавати неопходно је да се прате и анализирају стања и промене компонената које пресудно утичу на те промене. Међу тим компонентама најзначајније су *међународни амбијент и технологија.*

---

[3] *Counter-terrorism,* Canadian Security Intelligence Service, July, 1999, http://www.csis-scrs.gc.ca/eng/backgrnd/back8e.html

[4] C. B. Collin, *The future of cyberterrorism: where the physical and virtual worlds converge,* Institute for Security and Intelligence, http://www.acsp.uic.edu/OICJ/CONFS/terror02.htm; *Counter-terrorism,* исто; M. Milosevic, Lj. Stajic, V. M. Petkovic, *Some aspects of contemporary terrorism,* Belgrade, „Meaning", Theoretical Review of the Socialist Party of Serbia Jun, 1998, 4–5, http://209.207.236.112/irp/world/serbia/docs/aspekti_e.html; F. R. Perl, *Terrorism, the Future, and U.S. foreign policy,* Foreign Affairs and National Defense Division, Updated December 9, 1996, http://209.207.236.112/irp/crs/95–112.htm

Међународни амбијент

Окончањем „хладног рата“ нарушена је привидна равнотежа у свету, што је изазвало драстичне промене у многим областима, па и у тероризму. Свет је – при преласку из релативно стабилног биполарног стања на „нови светски поредак“, који још није потпуно дефинисан – захваћен великим променама високог степена нестабилности. Дезинтеграција Совјетског Савеза и претходне Југославије омогућила је реафирмацију националистичких, етничких и религиозних снага, што је довело до насиља у периоду после „хладног рата“. Унутар република бившег СССР-а многи етнички и национални покрети су добили прилику да изразе своје сепаратистичке захтеве, који су често праћени политичким насиљем, укључујући и тероризам, различитим формама конфликата ниског интензитета и наглим повећањем организованог криминала, уз мањи или већи утицај и спољних чинилаца. Ситуација је слична и на просторима претходне Југославије, посебно на Косову и Метохији. Осим тога, нестабилности доприносе локални и регионални конфликти у другим деловима света, економска разноликост, хегемонистичке тежње појединих земаља, немаштина, масовно кретање избеглица, брутални и корумпирани режими и повећање порозности националних граница. Све то изазива фрустрације и очајање, који се, у крајњем, исказују актима тероризма. Стога се, поред политичких, јављају и друге мотивације за предузимање терористичких акција, па је тероризам комплексан феномен, изазван мешавином *изменљивих* чинилаца и мотива.

Технологија

Промене у међународном амбијенту праћене су и технолошким променама, које ће и даље значајно утицати на међународне и локалне терористичке операције. Разне врсте технологија су одувек, мање или више, утицале на поједине аспекте друштвеног живота, али, чини се, информациона технологија је надмашила све што је човечанство до сада познавало. Наиме, скоро да нема области у којој није нашла примену, па рачунари, између осталог, све више постају нервни центри индустријских процеса, научноистраживачког рада, медицине, образовања и друмског, железничког и ваздушног саобраћаја, али и средство за остваривање личних права грађана, националне одбране и безбедности земље. Спрегнуте компјутерске и телекомуникационе технологије, на основу све минијатурнијих, али снажнијих и бржих саставних делова, прогресивно увећавају моћ информационих система, а мреже се шире и међусобно повезују формирајући националне, регионалне и глобалне рачунарске мреже, с бројним физичким и логичким везама, неограниченим бројем приступних тачака и мноштвом познатих и непознатих корисника.

Информациона технологија, иако смо још увек на самом почетку нове (информационе) ере, већ је унела суштинске промене у све поре

друштвеног живота, претварајући дигитални универзум у витални ресурс који омогућава корисницима нове начине комуницирања, информисања, образовања, рада и забаве. Међутим, истовремено, нагли пораст и глобализација рачунарских мрежа, с мноштвом различитих људи, компјутера, веза, садржаја и могућности, омогућили су бројне нежељене појаве, посебно у технолошки најразвијенијим земљама. Једна од њих је и нова форма тероризма, позната под називом *кибертероризам,* што у слободном преводу значи *тероризам будућности,* али будућности која је већ почела. Префикс *кибер* требало би да укаже на технолошку зависност и слабости који настају у новом неуређеном информационом свету, у којем тероризам добија нове могућности за организовање и деловање, нове атрактивне циљеве и ново оружје. Пандорина кутија је поново отворена, али овог пута у једном сасвим другом – виртуелном свету.

Дефинисање и карактеристике кибертероризма

Акт кибертероризма, за разлику од класичног тероризма, прагматично може да се дефинише као *коришћење информационих ресурса у облику претње или уцене да би се остварио одређени терористички циљ.* Будући да, према садашњој дефиницији, таквом једном акту недостаје есенцијални елемент тероризма: *коришћење или претња коришћењем физичког насиља,*[5] намећу се бројна питања у вези с тим како се може изводити тероризам у виртуелном простору, у простору без људи, и како је могуће да интелигентна особа поверује да је електронско ремећење једнако терору.[6] То је крајње неуобичајена и сложена енигма и потребно је много знања, труда и времена да се она разуме и разреши. За сада, таква дефиниција је заснована на претпоставци да у информационом амбијенту није неопходно довођење јавности у стање страха, као ни уништавање добара и изазивање насиља над људима, да би се остварили одређени терористички циљеви. Све што треба урадити јесте спречавање приступа до база података и прекидање токова података: на тај начин се друштво онеспособљава без и једног једиког испаљеног метка, подметнуте бомбе или лансиране ракете.[7]

У кибертероризму, према томе, главни циљ ће бити *ремећење* уместо *деструкције,* мада ни она није искључена, јер у друштвима високо зависним од информационе технологије ремећење информационих система може да изазове краткорочне проблеме (сметње) различитог обима и интензитета, и, што је много значајније, дугорочно губљење поверења у способност и поузданост тих система. На пример, у случају

[5] S. Sloan, *Terrorism: how vulnerable is the United States?,* The Strategic Studies Institute of the U.S. Army War College, May, 1995, http://www.terrorism.com/terrorism/sloan.html

[6] *The mythology of terrorism on tne net,* исто.

[7] *The mythology of terrorism on the net,* исто; Thom G, *Web of fearcyber terror may be the price we pay for the growth of the internet,* Herald Sun 24/07/1999, p. 19, http://www.infowar.com/class_3/99/class3_080299a_j.shtml

месечног ометања банкарског система неке земље кроз понављање атака грађанима ће се сигурно у једном тренутку наметнути питање поузданости дигитализованог банкарског пословања дестабилизованог кибератацима. Због тога ће постајати нервозни и неповерљиви, а такви људи не инвестирају и не улажу новац у банке, посебно не у оне које су имале проблема. Последице таквих аката могу да буду веома озбиљне и дугорочне.[8] Због тога је неопходно да се коригује схватање тероризма, па чак и да се промени дефиниција традиционалног терористичког акта и прилагоди новонасталој ситуацији. У супротном, схватање тероризма као политички мотивисаног и насилног понашања може да ограничи могућност и способност бранилаца да предвиде терористичко насиље, конфронтирају се са њим и одговоре на адекватан начин.

На настајање, ширење и интензитет кибертероризма утичу два основна чиниоца: све већа зависност друштвене заједнице од информационе технологије, па самим тим и њена све већа осетљивост на поремећаје и деструкцију, и нови амбијент деловања, који, с терористичког становишта, садржи и нуди нова средства, методе и технике и нове високо вредне и веома атрактивне циљеве.

Осетљивост друштвене заједнице

Информациона технологија чини структуру модерног друштва крхком, екстремно осетљивом на поремећаје, а рачунари, и нарочито рачунарске мреже, могли би да буду његова слабост. На пример, оптички каблови омогућавају телефонским компанијама да користе једну линију за пренос десетине хиљада конверзација, за које су донедавно биле потребне хиљаде одвојених бакарних каблова.[9] Резултат је већа ефикасност, бољи сервис и нижи трошкови. Прогрес је повећао ефикасност инфраструктуре, али резултат редукције редундансе јесте осетљивост која инфраструктуру чини веома рањивом. За информационе економије рачунари и рачунарске мреже су апаратура управљања и контроле. Пошто је подела рада достигла ниво непредвидљиве сложености, најскупља катастрофа која може да се деси у тим економијама јесте комуникациони јаз, који би имао за последицу испадање из синхронизације појединих специјализованих сегмената. Тај јаз би се, на пример, могао изазвати физичким пресецањем оптичког кабла, што је већ демонстрирано у Јапану.

Због наглашене комплексности и чврсте међузависности, као и због постојања бројних критичних тачака, националне инфраструктуре

[8] D. Pettinari, *Cyber terrorism, information warfare, and attacks being Launched now and in the future in the heartland of America,* Pueblo County Sheriff's Department And Second Vice-President, Society of Police Futurists International, http://www.policefuturists.org/fall97/terror.html; R. Regan, *When terrorists turn to the internet,* The Cristian Science Monitor, 07/01/99, http://www.infowar.com/class_3/99/class3_070499a-j.shtml

[9] *Responding to terrorism,* Chapter 9 of the U.S. Department of Defense's 1997 Annual Defense Report, http://www.terrorism.com/terrorism/Rasponding.html

које повезују, покрећу и опслужују компјутери постале су изузетно осетљиве и, ако се организовано нападну, може да се изазове значајан поремећај или деструкција. Ти поремећаји или деструкције могли би се рангирати од озбиљних сметњи (неприлика) – као што се десило у САД 1998. године када је губитак једног јединог сателита изазвао застој у електронском пејџинг систему – до потенцијалних катастрофа.[10] У вези с тим, нереална је и неразумна претпоставка да терористи неће схватити да је национална инфраструктура високо вредан и осетљив циљ.[11] Према томе, све већа зависност друштва од информационе технологије води ка свету у којем ће разрешавање бројних будућих конфликата подразумевати активности у кибернетичком простору и атаке на државне информационе структуре.

Нови амбијент деловања

Амбијент тог новог виртуелног света има своје специфичности које га чине скоро идеалним за обављање разних илегалних, па и терористичких активности. Неке од њих су: програмска – аутоматска обрада података; симултани рад више програма (мултипрограмирање); истовремени рад више корисника (рад у режиму расподеле времена); истовремено коришћење истих података од стране више корисника (конкурентан приступ); рад у реалном времену; приступ подацима и манипулисање њима с удаљених локација (даљинска обрада); физичка дислокација база (дистрибуирана обрада), и трансакције које се обављају таквим брзинама да човек не може непосредно да их надзире или да управља њима. У таквом, до сада непознатом амбијенту ограничене су могућности за непосредно надгледање и контролу, и мала је вероватноћа за откривање илегалних активности, јер се оне, као и легалне активности, обављају помоћу механизама који су најчешће невидљиви за жртву, а о свему остаје веома мало или ни мало трагова, посебно на папиру. Велики део онога што се дешава унутар те технологије није видљиво и никада се не појављује на хартији, а и рачунар може да буде програмиран тако да „обрише“ сопствене трагове и тако отежа откривање илегалних активности.

Једна од последица наглог развоја и примене информационе технологије јесте и претварање света у огромно електронско глобално село, у којем класични термини државна граница, гранични прелази и царина губе сваки смисао. Захваљујући електронским путањама које повезују све делове тог села, као и брзинама на тим путањама, које су несхватљиве обичном човеку, сваки и најзабаченији заселак је сваком становнику тог села практично надохват руке, и то у реалном времену. Такође, бројни рачунари, којима се обављају најсложеније функције и повезују, покрећу и опслужују витални системи унутар националних инфраструктура, обезбеђују кибертеристима право богатство избора места,

[10] *Tenet warns of cyber terrorism, June 25, 1998,* http://www.infowar.com/class_3/ /class3_062998a-j.html-ssi

[11] *Responding to terrorism,* исто.

циља, времена и начина напада. Информатизација друштва је праћена и са два додатна, упоредна процеса који ће сигурно значајно утицати на настајање и ширење кибертероризма: ширење информатичке писмености и увећавање моћи појединаца.

Ширење информатичке писмености веома је уочљива појава, због које примитивне рачунарске средине сваким даном постају све ређе а број лица стручних за коришћење рачунарске технике све већи. То најбоље потврђују чињенице да се информатика све масовније уводи у школске програме и да се одржава дугогодишња висока стопа раста продаје рачунарске технике, посебно персоналних рачунара. Због тога способност коришћења информационе технологије постаје масовна карактеристика и престаје да буде привилегија мањих (елитних) група специјалиста.

Динамичне промене на пољу информационе технологије, са снажним комерцијалним примесама, значајно поједностављују и олакшавају њено коришћење, чак и нетехничком кадру. Тако се повећава број оних којима постаје доступна „компјутерска моћ", а ту моћ нико не би смео да потцењује. Због велике брзине обраде, обима и разноврсности података који могу да се обухвате том обрадом, као и због разноврсности начина обраде (селекција, сортирање, поређење, укрштање, повезивање, копирање, брисање, модификација итд.) рачунари, које инструише појединац, могу да се користе за обављање веома сложених илегалних процедура. У таквим условима драстично се повећава моћ извршилаца терористичких дела, односно њихов криминални потенцијал, јер рачунар којег криминално инструише један човек може да има криминалне „способности" (могућности) десетине, па и стотине, класичних криминалаца. Према томе, потенцијал терористичких организација и екстремних појединаца у будућности ће се стално увећавати због промене у технологији, која ће обезбедити следећим генерацијама много веће могућности од оних које имају садашњи најпросвећенији и најобученији класични терористи. Нова генерација терориста, наоружана информационим оружјем, моћи ће да се ангажује у акцијама драматичнијим и деструктивнијим него што је била намера терориста приликом подметања бомбе у Оклахоми.[12]

Посебно значајан елемент с терористичког аспекта јесте висок степен *анонимности* корисника Интернета, што је додатни квалитет који терористи високо вреднују. Управо та чињеница ће у будућности бити веома значајан мотивациони чинилац многима да се упусте у терористичку авантуру, иако у класичним условима на то никада не би ни помислили. Боравећи у хотелској, радној или спаваћој соби, с персоналним рачунаром, модемом и телефонском линијом, или мобилним телефоном, укључивањем у Интернет терориста може на миру да бира где, шта и када да нападне, укључујући и циљеве на другој страни планете, удаљене хиљадама километара.

Анализа блиске прошлости и садашњости показује да тероризам значајно еволуира и мења форму. Оно што се сада догађа подразумева

[12] S. Sloan, *исто*.

примену информационих ресурса за остваривање одређених терористичких циљева, што не значи да су се терористи у потпуности одрекли претходних приступа, већ само да ће се тежиште њиховог деловања вероватно све више померати ка информационом амбијенту. Према томе, подметање бомби остаће најопштији тип напада, узимање талаца и киднаповања биће основа терористичког репертоара, а отимање авиона је увек могуће. Аутоматске и полуаутоматске пушке и пиштољи, уз вероватно проширење арсенала, остају и даље оружје избора.[13] Међутим, информациона технологија терористима пружа једну потпуно нову глобалну арену, с новим садржајима и могућностима деловања, и они ће ту прилику сигурно искористити. Дакле, еволуција тероризма и његово прилагођавање променама које настају у амбијенту деловања трајан су процес и оно што се сада догађа наговештава постепен, али сигуран, прелазак на примену информационих ресурса у остваривању одређених терористичких циљева. При томе, постоје четири основна начина на која терористи у свом деловању могу да користе информационе ресурсе ради остваривања одређених терористичких циљева:[14] комуникациони медиј, приручни алат, објект напада и средство напада.

Комуникациони медиј. Терористичке групе користе Интернет за пропагирање, преко *web* сајтова, без цензуре и сличних ограничења, својих идеја и пласирање својих хорор „прича" директно до публике, коју чини огромни глобални аудиторијум. Тиме, поред постизања одређеног пропагандног ефекта, утичу и на традиционалне информативне медије, односно на начин на који ће обавештавати јавност о њиховим терористичким актима. Осим тога, Интернет користе за регрутовање и окупљање нових чланова и присталица, прикупљање финансијских средстава (обично су то добротворни прилози, али и рекет), прикупљање и размену обавештајних података и координирање својих акција.

Коришћење електронске поште, *meiling* листи, анонимних *remailer*-а, дискусионих група, електронских огласних табли *(BBS)* итд. може да служи и као *колективна терористичка меморија,* која омогућава свим странама да се детаљно упуте у расположива знања и информишу о свакој еволуцији у тактици, техници и технологији.[15] На пример, довољно је да се у неку Интернетову машину за претраживање *(Yahoo, InfoSeek, WebCrawler, AltaVista,* па и наша *Крстарица)* унесу кључне речи *„pipe bomb"* и добиће се на стотине, па и хиљаде страна на којима се, између осталог, налазе и детаљна упутства за ручну израду бомби.

Процењује се да на Интернету тренутно има око 30.000 хакерски оријентисаних сајтова,[16] који скоро свима омогућавају коришћење алата

[13] S. Sloan, *исто.*

[14] H. Kazaz, *Cyber sabotage is not a farfetched realyty for turkey,* The Turkish Daily News (TDN), 11/07/1998, http://www.infowar.com/class_3/class3_071598a_j.html-ssi

[15] M. Wilson, *исто.*

[16] Y. Alexander, *Computer terror can't be ignored,* Monday, June 14, 1999, http://www.infowar.com/class_3/99/class3_061699a_j.shtml; G. Barker, *Australia: internet terrorism escalates the new info-war,* AGE (Melbourne) 13/07/1999, p. 9, http://www.infowar.com/class_3/99/class3_071699b_j.shtml

за ометање и деструкцију. На пример, на једном од њих, базираном у Њујорку, постоји упутство за писање вируса, инструкције како да се загуши мрежа, сајтови за хаковање и, чак, зборне тачке у градовима широм света где хакери могу да се контактирају ради размене знања и искустава. Доступност објашњења за коришћење новог оружја (вируси, црви, Тројански коњ, логичка бомба итд.) допринеће да се та форма ратовања стално примењује на међународној сцени. Многи значајни модели деловања могу да буду унапред урађени и уграђени, уз обезбеђену обуку и упутства за њихово коришћење, а све то може да буде јавно публиковано на мрежи и приступачно свим корисницима Интернета, или може да има рестриктиван карактер и да буде намењено затвореном кругу корисника. За размену оперативних информација постоји снажан заштитни алат у облику дигиталне криптографије. Поруке могу да буду заштићене коришћењем криптолошке технологије с јавним кључем. Та технологија је приступачна свима који је желе, чак и у „изворном коду“,[17] што омогућава софистицираним корисницима да обављају тестирања и уносе промене како би били сигурни да нису обманути.

Приручни алат. Терористи могу да користе информационе ресурсе као приручни алат за планирање и организовање својих програма рада и за обављање других „споредних“ активности и функција. На пример, у компјутерима држе своје финансијске књиге, терористичке планове, потенцијалне циљеве, дневнике присмотре, планове напада, листе придружених конспиратора, и друго. Предност тога је лакше, брже и поузданије руковање подацима у дигиталној форми и знатно боља заштита, а по потреби могу брзо и ефикасно да их униште.

Објекат напада. Циљ кибертерористе могу да буду информациони ресурси, односно њихов потенцијални циљ може да буде све што повезују, покрећу и опслужују компјутери: војни компјутерски системи, системи државне управе, системи за контролу ваздушног и железничког саобраћаја, системи фармацеутске индустрије и за индустријску производњу хране, снабдевање гасом, водом и електричном енергијом, болнички и научноистраживачки системи, као и системи помоћу којих се опслужују велики јавни догађаји, као што су, на пример, Олимпијске игре. С обзиром на то колико таквих система има, посебно у информационо развијеним земљама, за које и какве функције се користе и колика је њихова осетљивост на поремећаје и деструкцију чињеница је да информациони амбијент нуди терористима право богатство избора веома атрактивних и високо вредних циљева.[18]

Средство напада. Кибертерористи могу да користе информационе ресурсе и као средство за обављање својих терористичких активности, било на основу неовлашћеног приступа (хакинг) до циљних система, било коришћењем оружја информационог ратовања (вируси, црви, Тројански коњ, логичка бомба, *E-mail* бомба итд.) ради покретања

[17] M. Wilson, *исто.*
[18] S. Sloan, *исто.*

ланца догађаја у којима би се каскадним ефектом изазвао колапс, на пример, сервисне мреже, линије снабдевања енергентима или система за контролу ваздушног саобраћаја.[19]

Могућим сценаријима који се односе на акте кибертероризма обухваћено је мноштво разноликих напада на деликатну међузависну инфраструктуру модерног информационог друштва. Примери из прошлости су већ показали да се и у том амбијенту могу применити класичне методе терористичког деловања,[20] али се у информационим сценаријима иде даље од подметања бомби или лансирања ракета и укључује се потенцијално катастрофална деструкција информационих супер аутострада технолошке инфраструктуре. Резултати могу да се рангирају од масовних незгода до опасности или катастрофе.[21]

За остварење те врсте терористичких активности могу да се користе веома суптилне методе и технике, које се тешко откривају јер не ометају редован рад система, а често се могу доказати једино ако се открију у тренутку извођења. Информациона технологија омогућава примену метода и техника које су доскора биле незамисливе. Уградња „Тројанског коња", „логичке бомбе" и „тајних врата", дистрибуција компјутерских вируса, црва и *E-mail* бомби само су део могућности за извођење операција и са велике дистанце и са временским одлагањем од неколико дана, недеља, па и година. За атаке на информационе циљеве постоје разни сценарији, од којих би неки могли да буду следећи:[22]

– измена формула за лекове у фармацеутским фабрикама и у фабрикама за производњу хране. На пример, постоји могућност да кибертерористи даљински приступе контролним системима за прераду житарица, промене ниво гвожђа у произведеној дечијој храни и тако изазову обољења или смрт деце;

– саботирање глобалног финансијског система ометањем међународног трансфера фондова. Кибертерористи могу покушати да поремете функционисање банки, међународних финансијских трансакција, размену робе итд., да би изазвали дестабилизацију већег обима и изазвали незадовољство и неповерење грађана у економски систем земље;

– ометање функционисања контроле ваздушног саобраћаја и преусмеравање путничких возова с катастрофалним последицама. Напади кибертерориста на контролне системе ваздушног саобраћаја и изазивање судара цивилних авиона реалан су сценарио, а много тога већ може да се уради и у железничком саобраћају;

– „обарање" телефонског система, промена притиска у гасоводима, прекид у снабдевању водом и искључивање електричне енергије, јер кибертерористи могу даљински да утичу на снабдевање гасом, водом, струјом итд.

---

[19] *Responding to terrorism, исто.*
[20] A. Alper, *Terrorist threat spurs growth in access control system mart,* Computerworld, september 15, 1986, стр. 106.
[21] S. Sloan, *исто.*
[22] Y. Alexander, *исто,* C. B. Collin, *исто.*

Наведени примери вишеструког угрожавања здравља и живота људи нису само научна фикција. Сви ти сценарији већ могу делимично да се остваре, неки од тих инцидената су се већ десили,[23] а многи се могу десити у скорој будућности. Јер, ако тинејџери могу да компромитују мреже коришћењем основних вештина и алата расположивих на Интернету, питање је шта могу да ураде терористичке групе или државе са много већим ресурсима и мотивацијом.[24] Све то указује на потребу (и намеће обавезу) правовремене изградње и развоја одговарајућег система заштите информационог амбијента. Неопходна су, пре свега, стручна, целовита и свеобухватна решења, којима треба обухватити све аспекте заштите, укључујући нормативни, организациони, кадровски, физичко-технички и логички аспект. То је једини начин заштите, јер све друго би било импровизација и/или би чинило половична решења с потенцијално катастрофалним последицама.

Међутим, иако су кибертерористички атаци веома моћни, мало коштају, могу да се реализују на свакој дистанци, обезбеђују потпуно изненађење и изводе се брже него што противник може на одговарајући начин да одговори на њих,[25] поставља се питање да ли коришћење те форме тероризма има смисла, на пример, за терористичке групе каква је Бин Ладенова, или им је примеренији визуелни утицај експлозије бомбе у некој згради.[26] Све терористичке групе које се сада појављују веома су склоне визуелним ефектима, али се не би смела занемарити чињеница да постоје и терористичке групе које неће тежити визуелним ефектима, већ ће желети суптилнији приступ.

Колико је широј јавности познато, до сада ниједна од група које су конвенционално дефинисане као терористичке, није користила информационо оружје против инфраструктуре,[27] па зато и није било атака већег обима на системе за контролу ваздушног саобраћаја, дистрибуцију гаса и електричне енергије, телефонске системе, и слично. Мада су хакери извели хиљаде упада, можда и милионе, ипак је Интернет, према неким проценама,[28] само једном „бачен на колена": када је Роберт Морис пласирао црва. Али ни то није било намерно изведено. Такође, било је нарушавања инфраструктуре, али то нису биле претње групе или појединца с таквом намером, а за то постоји више разлога. Наиме, ниједна терористичка организација није до сада прихватила ту нову форму тероризма због тога што терористи морају да разумеју начин коришћења новог оружја и да верују у његову примену, будући да прихватају само оружје које су сами израдили и истестирали, и за које знају да је поуздано. Друго, морају знати, веровати и, што је и најваж-

[23] C. B. Collin, *исто, The mythology of terrorism on the net, исто.*
[24] *Counter-terrorism, исто.*
[25] M. Wilson, *исто.*
[26] J. Borland, *Analyzing the threat of cyberterrorism,* Tech Web News, 23/09/1998, http://www.infowar.com/class_3/class3_102898b_j.shtml
[27] J. Borland, *исто.*
[28] D. Pettinari, *исто.*

није, морају осећати да је то за њих. Пре него што је склопила мир, IRA била је на ивици примене кибертероризма. Они су имали компјутерски оријентисане ћелије и већ су атаковали на инфраструктуру подметањем реалних или лажних бомби у електране да би проверили да ли могу да искључе осветљење Лондона.[29] Али, још увек су наклоњенији и више верују у класично оружје.

За разлику од других форми тероризма, кибертероризам је поуздан, ефикасан, профитабилан и веома се тешко спречава. Информациона технологија будућим терористима обезбеђује готове и сигурне алате, и бројне могућности да значајно ојачају своје ограничене ресурсе. Незнатна опасност од хватања, потенцијал за изазивање максималне штете без губитка живота, енормна пропаганда и могућност врбовања само су неки разлози због којих је кибертероризам веома атрактиван за екстремне појединце и терористичке организације.[30] Због свега тога, комбинујући све већу осетљивост са наглим увећањем нивоа насиља, вештина и знања расположивих унутар терористичких организација кроз „нову крв" која ће пристизати приступањем младих информатички образованих људи заједници терористичких група, може се са великом сигурношћу тврдити да је транзиција терористичких група на нову форму тероризма (кибертероризам) само питање времена.

Профил кибертерористе

Информациона технологија и њен амбијент пружају терористима мноштво погодности и могућности којих није било у прошлости:[31] глобална повезаност, неограничен простор деловања, велики избор атрактивних циљева, могућност вишеструког деловања, анонимност и лична безбедност, нове методе и технике, јефтино, снажно и широко расположиво информационо оружје, деловање на дистанци у реалном времену, драстично увећање моћи појединаца, колективна меморија, и разноврсна и заштићена комуникација.

Због свега тога за многе терористичке организације и екстремне појединце кибертероризам ће бити атрактивна алтернатива традиционалним формама тероризма, што ће утицати и на профил терористе 21. века. То би могао да буде појединац који није придружен организованој групи и који очигледно није агент неке државе спонзора, већ делује као *слободан стрелац*. Такође, то може да буде појединац који има подршку групе, али делује независно од ње.[32] Наравно, и даље ће бити чврсто организованих група, које ће као такве и деловати.

У информационој ери на кибертерористичкој сцени, поред постојећих препознатљивих екстремистичких група, могу се очекивати и разни проблемскоријентисани покрети, као што су радикални покрет за

[29] J. Borland, *исто.*
[30] G. Thom, *исто.*
[31] H. Kazaz, *исто.*
[32] F. R. Perl, *исто.*

заштиту човекове околине и екстремистичке групе за заштиту животиња. Искрснуће нове групе жељне да користе кибертероризам да би изразиле негодовање, незадовољство и бес, реално или имагинарно.[33] Такође, информациона технологија пружа велике могућности отуђеним, фрустрираним и поремећеним појединцима да директно утичу чак и на државне интересе.[34] Могућност једног информационог *Unabomber*-а и све што то подразумева убрзо ће постати реалност, јер технолошки развој све више омогућава „слабима" да атакују на „јаке" и онима који су традиционално били на маргинама друштва да играју значајну улогу на националном или светском нивоу. Постојаће и „армија" хакера, чији је потенцијал већ практично демонстриран. Реч је о веома добро обученим појединцима који користе комбинацију вештина социјалног инжењеринга и своја информатичка знања. Процењује се да у свету сада има више од 100.000 хакера. Тренутно су хакери аматери највећа претња на Интернету и одговорни су за око 90 одсто свих хакинг активности. На потенцијалне професионалне хакере отпада 9,9 одсто, а на киберкриминалце светске класе 0,1 одсто.[35] То су високо обучени професионалци које је веома тешко зауставити јер користе најразличитије начине приступа, што је, вероватно, највећа претња у киберпростору.[36]

Многи појединци с обавештајним искуством добро знају да је значајан предуслов успешне реализације неке акције ангажовање сарадника, који се у њиховом жаргону често назива *олакшивач*[37] Потенцијални „олакшивачи" у киберпростору су управо хакери, који су, и поред честе ароганције, лаке мете за ангажовање, посебно стога што многи од њих припадају популацији која је легално још малолетна.[38] Баш као што цивили могу релативно лако да се преведу у војнике, тако и хакери могу да се окрену кибертероризму. Разлози за такву промену могу да буду веома различити, али ће, вероватно, најчешћи мотиви бити новац и престиж, а обично хакери неће ни бити свесни преласка у кибертеористе.

Организација

У новом информационом амбијенту уочавају се извесне индикације да ће доћи до одређених промена и на том плану. Стари модели хијерархијске или „ћелијске" структуре полако ишчезавају, јер у новим условима постају застареле, неефикасне и веома осетљиве на откривање, а све ће више бити заступљене слободне групе с „флуидном организационом формом", без структуре и структуре дубоке само један ниво, што омогућава директну контролу или надзор и знатно виши

[33] S. Sloan, *исто.*
[34] *Responding to terrorism, исто.*
[35] *Statics on cyber-terrorism,* http://www-cs.etsu.edu/gotterbarn/stdntppr/stats.htm
[36] J. Borland, *исто.*
[37] *The mythology of terrorism on tne net, исто.*
[38] M. Wilson, *исто.*

степен безбедности. Нови начин деловања терористе одвијаће се, у извесном смислу, у стилу „добро организоване дисорганизације", што указује на чињеницу да потреба за организацијом у савременим условима, за разлику од прошлости, неће бити велика.[39] Стога ће тероризам – и традиционални и кибертероризам – све више и чешће бити акт појединца. Претње таквих појединаца или „бутика" тероризма распростираће се широм света, што не значи да поједине државе неће имати одређену улогу и у кибертероризму. Она ће само бити другачија од оне коју су имали у прошлости. Државе ће сигурно, када је то у њиховом интересу, налазити начине да охрабре то понашање. У одређеним ситуацијама, користиће подстрекачку реторику да би распалиле страсти и изазвале бес код многих појединаца, који ће тада бити више него спремни да изведу неки кибертерористички акт.[40] Према томе, подстрек и смернице ће пре потицати од „генералних изјава" лидера,[41] него из формалне команде. Такви акти државу ништа не коштају, а она увек може одговорно да тврди да са њима нема ништа (на пример, подметање бомби у књижарама у САД након смртног указа ајатолаха Хомеинија Салману Руждију).[42] Спонтаних реакција бројних појединаца, које ће се испољити кроз предузимање кибернапада на одређене циљеве, биће и на одређене појаве и догађаје у свету. Најбољи пример за то су атаци југословенских хакера на системе НАТО-а због агресије на Југославију, као и атаци кинеских хакера на америчке системе због бомбардовања њихове амбасаде у Београду.

Супротстављање кибертероризму

Драматични догађаји повезани са тероризмом чине да тај феномен добија највећи значај за јавни интерес, посебно због тога што су глобалне терористичке претње сада много комплексније, екстремније, софистицираније, раширеније и транснационалније у поређењу с онима пре десет година. У супротстављању класичном тероризму примењује се мноштво дефанзивних и офанзивних опција, од дипломатије и међународне кооперације до економских санкција, тајних акција, физичке заштите и војне силе. При томе, према општој сагласности, најефикаснији начин борбе против тероризма јесте обавештајни рад,[43] кроз који се, најчешће пенетрацијом терористичких мрежа, обезбеђују обавештајни подаци који омогућавају да се поремете терористички планови и организација пре него што почну да делују. Управо због тога је проблем сузбијања тероризма постао најзначајнији у плановима и програмима скоро свих обавештајних служби.

[39] S. Perry, *Terrorism: a frightening new perspective,* http:/nsi.org/Library/Terrorism/110501.htm; Regan R, *исто.* M. Wilson, *исто.*
[40] R. Regan, *исто.*
[41] S. Perry, *исто.*
[42] R. Regan, *исто.*
[43] K. S. Niazi, *The dynamic history and causes of terrorism, http://niazi.com/dynamic.htm;* М. Милошевић, Љ. Стајић, В. М, Петковић, *исто,* F. R. Perl, *исто.*

Због технолошког развоја, односно промене природе и повећања интензитета нових терористичких претњи, намеће се питање да ли су постојеће политике и организациони механизми адекватно усмерени на борбу са оним што може да буде нови знак терориста: неко ко не ради за неку одређену организацију и ко није агент неког посебног државног спонзора, а ипак поседује потенцијал за извођење терористичких атака.[44] Наиме, уколико се теорија о кибертероризму сматра истинитом, начини за борбу против њега морају да се мењају. У оквиру тога, постаје најзначајнија правовремена револуција антитерористичке политике, организационе структуре и спремности да се одговори на главне терористичке инциденте информационог доба.

У информационом амбијенту контрола физичког простора није више начин за спречавање терористичких атака. Јер, виртуелни простор је ново место догађања, у којем делују нови опасни играчи, према новим правилима и новим и нефамилијарним оружјем. Стога обавештајне и криминалистичке службе, тактике, заштитне процедуре и опрема, од којих се очекивало да заштите људе, системе и нације, постају беспомоћни против новог типа противника и његовог пустошећег оружја, а методе контратероризма, које су светски стручњаци годинама изграђивали, постале су неефикасне против тог непријатеља, који не напада камионима напуњеним експлозивом, актен-ташнама са сарином, нити динамитом причвршћеним за тело фанатика. Тај непријатељ напада јединицама и нулама, на месту где смо најосетљивији: на тачку на којој се преклапају физички и виртуелни свет.[45]

Због свега тога, обавештајне и криминалистичке службе ће у новим условима имати тежак задатак да пронађу нова средства, развију нове, одговарајуће и ефикасне методе и изграде тимове за супротстављање кибертероризму. Мораће да се науче нова правила и овлада новим технологијама, *јер за ту врсту тероризма треба се добро припремити и борити, пре свега, знањем и добром организованошћу.* С обзиром на динамику развоја информационе технологије и промена које она доноси, изградња тимова за борбу против кибертероризма мора да буде целовита, реална у времену и динамична. Јер, за разлику од других терориста, кибертерориста неће умрети ако не успе, већ ће научити где је погрешио и шта није добро радио, па ће те информације користити у следећим нападима.[46]

Откривање извршилаца терористичких атака у киберпростору може да буде веома тешко због високог степена дигиталне анонимности, па је често и немогуће утврдити да ли су кибер-атак организовале непријатељски настројене државе, неке терористичке организације или пар несташних дечака. На пример, према „Вашингтон посту", почетком 1998. године 11 система америчке армије било је изложено „електронском нападу". Извођачи у почетку нису били познати зато што су

[44] F. R. Perl, *исто.*
[45] C. B. Collin, *исто.*
[46] *The mythology of terrorism on the net, исто.*

прикрили своје трагове тако што су напад извели преко компјутерских система у Уједињеним Арапским Емиратима. Иако се радило о отвореним системима и подацима, ти системи су, ипак, били централно језгро података потребних за руковођење војним снагама. На крају, откривена су два млада хакера из Калифорније који су извели атак преко система у Уједињеним Арапским Емиратима према директивама хакера из Израела.[47]

Проблем посебно отежава чињеница да је кибертероризам значајан подскуп информационог ратовања,[48] једне веома изазовне форме међудржавне конфронтације у којој специјализоване обавештајне институције неких земаља усмеравају организоване и хармонизоване наоружане акције ка држави жртви ради изазивања кризних ситуација. У вези с тим, на затвореном брифингу у Конгресу, шеф ЦИА Георг Тенет рекао је да најмање „туце" земаља, од којих су неке непријатељски расположене према САД, развијају програме за атаковање на информационе и компјутерске системе других земаља. Међу њима су наведене Кина, Либија, Русија, Ирак и Иран.[49] Своју тврдњу Тенет је поткрепио и примерима.[50] У интервјуу датом крајем 1997. године један виши руски официр је коментарисао да би један атак против једног националног циља, као што је систем за транспорт или систем за дистрибуцију електричне енергије *„... на основу његових катастрофалних консеквенци, комплетно преклопио коришћење (оружја) масовне деструкције"*. У чланку у кинеским новинама „People's Liberation Daily" наводи се да *„противник који жели да уништи САД мора само да унесе неред у компјутерске системе њених банака помоћу високе технологије. Ово би пореметило и уништило америчку економију. Ако превидимо ову тачку и једноставно се ослонимо само на изградњу скупе стационарне армије... је управо толико добро колико и изградња савремене Мажино линије"*. У војној публикацији једне треће земље наводи се да ће *Информационо ратовање бити највиталнија компонента будућих ратова и поремећаја"*. Аутор претсказује конфликте *„без крви"*, пошто – *„само информационо ратовање може одлучити исход"*.

Сједињене Државе, као водећа технолошка сила у свету, те проблеме је толико озбиљно схватила да је формирала Центар за заштиту националне инфраструктуре *(Nacional Infrastructure Protection Centre)*, који запошљава више од 500 експерата за заштиту из ЦИА *(Secret Service)*, НАСА, НСА и ДОД. Циљеви под њиховом присмотром обухватају телекомуникације, енергију, банкарство и финансије, системе за снабдевање водом, системе за контролу ваздушног саобраћаја и

[47] *Tenet warns of cyber terrorism, исто.*
[48] Р. С. Петровић, *Информационо ратовање – будућност која је почела*, „Безбедност" год. XLI, бр. 5, 1999, стр. 635–654.
[49] D. Pasternak, B. Bruce, B. B. Auster, *Terrorism at the touch of a keyboard possible targets: anything run by computers*, „World Report", 7/13/1998, http://www.infowar.com/class_3/class3_071098a_j.html-ssi
[50] *Tenet warns of cyber terrorism, исто.*

владине сервисе и сервисе за ванредне ситуације.[51] Такође, поједине владине организације су формирале своје групе за кибер-тероризам. Централна обавештајна агенција – је формирала сопствену групу – Центар за информационо ратовање *(Information Warfare Center)*, са око 1.000 људи, који раде непрекидно, а Федерални истражни биро истражује хакере и сличне случајеве. Тајна служба прати банкарске случајеве, проневеру и прислушкивање. Ратно ваздухопловство је формирало сопствену групу *(Electronic Security Engineering Teams – ESETSs)*. Тимови од два или три члана који по случајном избору обилазе сајтове Ратног ваздухопловства и покушавају да добију контролу над њиховим компјутерима, имали су у 30 одсто случајева успеха у задобијању комплетне контроле над системима.[52] С друге стране, они увелико раде и на развоју кибероружја.[53] Иако је потпун обим америчког киберарсенала међу најбоље чуваним тајнама националне безбедности, извештаји указују на мноштво оружја у развоју, укључујући компјутерске вирусе или логичке бомбе за обарање противникових рачунарских мрежа, пласирање дезинформација ради изазивања конфузије и обликовање видео слика на страним телевизијским станицама ради обмане. Октобра 1999. Пентагон је објавио да је испланирао како офанзивне, тако и дефанзивне кибероперације под командом генерала са четири звездице.[54]

Будући да су САД формирале своју прву малу групу информационих ратника или, како је назива Министарство одбране *ћелију за информационе операције*, неки експерти одбране су поверовали да су оружане снаге током 78 дана агресије на Југославију водиле и кибернетички рат против Србије.[55] Иако су званичници то негирали, пензионисани генерал-мајор Дојл Ларсон, који је био командант Команде за електронску заштиту ваздушних снага осамдесетих година, каже да је био уверен да САД користе тактику киберрата за атаке на српске информационе системе, указујући да су и САД биле „све време атаковане од хакера". Како су изјавили неки виши официри Пентагона,[56] током агресије НАТО-а на Југославију, Пентагон је разматрао хакирање српске компјутерске мреже да би ометао војне операције и основне цивилне функције. Један високи официр је изјавио да је у случају Југославије заједнички план за предузимање информационих операција био коначно припремљен и одобрен средином агресије. Били су предвиђени и многи традиционални елементи информационог ратовања – психолошке операције, акције обмане, електронско ометање радара и радио-сигнала. Једна од тактика било је бомбардовање југословенског руководства факс-порукама и други облици узнемиравања.

[51] G. Barker, *исто.*
[52] *Cyber-terrorism,* http://www-cs.etsu.edu/gotterbarn/stdntppr/
[53] Р. С. Петровић, *исто.*
[54] B. Graham, *Military grappling with rules for cyber warfare,* „Washington Post", Monday, November 8, 1999; Page A1, http://www.washingtonpost.com/wp-dyn/articles/A35345–1999Nov7.html
[55] B. Brewin, *Dod may have waged first cyberwar in Serbia,* Federal Computer Week, September 23, 1999, http://www.fcw.com/pubs/fcw/1999/0920/web-io-09-23-99.html
[56] B. Graham, *исто.*

Америчке снаге су гађале неке компјутере који су контролисали југословенске системе противваздушне одбране, изјавили су званичници, али су атаци предузимани с авиона за електронско ометање радије него преко компјутерских мрежа. Од таквих акција Пентагон се уздржао због сталне неизвесности и ограниченог амбијента у којем би се реализовао тај облик киберратовања. С друге стране, званичници Министарства одбране су рекли да је легалност била један од разлога зашто су се амерички ауторитети уздржали од кибернапада на Југославију. Други разлози су били то што је амерички киберарсенал био у зачетку и недовољно истестиран, као и децентрализована природа неких југословенских система, који нису били погодна мета за компјутерски напад.[57] Од свих разлога који се наводе као објашњење због чега нису предузети кибернапади против Југославије најприхватљивији је онај да Југославија још увек не користи високу технологију на интегрисан начин и у мери која би оправдала примену кибератака.

У вези с агресијом НАТО-а на Југославију интересантан је и податак да је средином агресије Министарство одбране САД издало смернице *(An Assessment of International Legal Issues in Information Operations)* у којима је било упозорење да би употреба кибератака могла изложити ауторитете САД оптужби за ратни криминал.[58] Смерницама је сугерисано командантима да на компјутерске атаке примењују исте принципе „закона рата" као приликом коришћења бомби и ракета, што је подразумевало да се гађају само војни циљеви уз минималну колатералну штету и избегавање насумичних атака. Званичници кажу да тај документ, који није добио велики публицитет у јавности, одражава колективно размишљање правника Министарства одбране о киберратовању и означава први формалан покушај америчке владе да се поставе легалне границе за војно укључивање у операције компјутерског напада. Командантима се налаже да буду опрезни приликом гађања институција које су првенствено цивилне, као што су банкарски системи, берза и универзитети, чак и у случају да се кибероружјем може обезбедити да се то уради без проливања крви. Документом се сугерише да у ратном времену компјутерски атаци и друге форме оног што војска назива *информационе операције* треба да обављају само чланови наоружане силе, а не и цивилни извршиоци. Такође, формулисано је да пре започињања неког кибернапада команданти морају пажљиво да процене потенцијалну штету за одабрани циљ као што се у Пентагону процењују губици у људству од напада бомбама.

Различите компјутерске нападе компликује потреба за мноштвом детаљних обавештајних података о циљним хардверским и софтверским системима на основу којих би команданти могли (и морали) знати не само где да нападну већ и да предвиде све последице таквих атака. Када је реч о легалном уређењу те области, став Пентагона је да су постојећи закони и међународни споразуми довољни за регулисање информацио-

[57] B. Brewin, *исто*, B. Graham, *исто*.
[58] B. Graham, *исто*.

ног ратовања. Друге агенције америчке владе слажу се са тим ставом, али такво мишљење не дели и Русија.[59] Током 1998. године Москва је покушала да у УН обезбеди подршку за резолуцију којом би се обезбедиле нове међународне смернице и забранило посебно опасно информационо оружје. Русија је упозорила да информационе операције *„могу водити ескалацији трке у наоружању"*. Она сматра да *„савремени међународни закон практично нема начина да регулише развој и примену таквог оружја"*. Али руска иницијатива није добила потребну подршку. Амерички званичници су је оценили као покушај да се спречи развој у области оружја у којој Русија заостаје за Сједињеним Државама. У формалном одбијању руског предлога Клинтонова администрација је заузела став да би сваки покушај свеобухватног формулисања принципа информационог ратовања био преурањен. *„Прво, ви имате огромну разлику у софистицираности овог типа технологије у различитим земљама"*, рекао је званичник Министарства спољних послова САД који је био укључен у то питање. *„Такође, технолошке промене су тако рапидне да компликују напоре покушаја да се ове ствари дефинишу"*. Уместо скретања питања кибернапада у правцу контроле оружја, америчка администрација је више волела да их међународно третира као основни интерес криминалистичких служби. Због тога су званичници САД подржали неколико напора кроз УН и друге организације да би олакшали међународну кооперацију у гоњењу компјутерских криминалаца и терориста.

Закључак

На крају, не може се избећи питање где смо ми у свему томе. Наведене неостварене намере САД да изведу кибернападе на нашу земљу само потврђују да нисмо, нити ћемо бити изузеци. У претходној Југославији динамика увођења информационе технологије била је достигла завидан ниво. Међутим, бурни догађаји на овим просторима после распада СФРЈ, а посебно санкције уведене нашој земљи, драстично су успорили, а у неким сегментима и зауставили примену информационе технологије и развој информационих система у нашој средини. Због тога смо се у тој области, у односу на остатак света, нашли у веома незавидном положају. Ипак, укидањем санкција и повезивањем с Интернетом створени су неопходни предуслови да се изгубљено надокнади.

Број рачунара с тенденцијом сталног раста (око 500 великих и средњих и око 450.000 персоналних рачунара), број корисника Интернета, који се увећава по стопи од 10 одсто на месечном нивоу (крајем 1995. године у Југославији није постојао ниједан официјелни и овлашћени корисник Интернета, крајем 1996. године било је око 3.000 прикључака са око 10.000 корисника, а сада их има више од 100.000), доградња и развој националне телекомуникационе мреже и повећање броја телефонских прикључака недвосмислено указују да се стање

[59] B. Graham, *исто*.

значајно побољшава. Дакле, и поред свих недаћа кроз које је у последњих десетак година прошла, и још увек пролази, наша земља се убрзано информатички описмењује и информатизује. Али, у силној жељи да се изгубљено што пре надокнади и да се на том плану умањи разлика у односу на информатички развијене земље, у други план су потиснуте неке значајне компоненте рационалног развоја, међу којима је најкритичнија безбедносна компонента. Због повезаности с Интернетом, као и коначног укидања санкција, ми више, посебно у информатичком смислу, нисмо изоловани. Напротив, све више и чвршће постајемо повезани и унутар земље и са светом, па пропорционално томе и зависни и осетљиви. Будући да се налазимо у центру једног од најнестабилнијих региона у свету, можемо бити сигурни да ћемо, уз садашњи темпо информатизације, у веома блиској будућности бити суочени и с реалним претњама кибернапада, а ми за тај тренутак нисмо довољно спремни. Управо стога морамо, и то веома брзо, схватити да су проблеми који произилазе из тамне стране информационе технологије толико озбиљни, сложени и опасни да сви резултати постигнути у примени те технологије могу веома лако да се доведу у питање, чак толико да последице осетно надмаше остварене резултате. Морамо схватити да будући непријатељ (нације, групе или појединци) може тежити да нам нашкоди на начин који није традиционалан. Те чињенице су свесни и други, па многе нације разматрају пораст сопствене зависности од информационих система, за војне и цивилне потребе, истражују своју зависност и развијају начине да се заштите. Ми морамо да урадимо исто, јер ако то не учинимо правовремено и на одговарајући начин могли бисмо да се нађемо у веома неповољном положају у односу на оно што може да буде кључна заштита у следећој деценији. Зато је сада, када због још увек релативно ниског нивоа информатизације и интеграције информационих ресурса нема озбиљне непосредне опасности, прави тренутак да се покрену сви релевантни чиниоци како би се стање на том плану значајно променило.

Интернет је благодет, али наша жеља да што пре и што више искористимо све оно што он пружа има своју цену, а од нас зависи колика ће она бити. Кибератаци су врста цене која ће сигурно морати да се плати за укључивање у Интернет, који је због своје глобалне природе постао толико осетљив да оно што је виђено као његова снага сада постаје извор његових слабости. При томе посебно забрињава чињеница да су многи у друштву толико занесени, па и заслепљени потенцијалним погодностима Интернета да потпуно заборављају на велике ризике од његовог коришћења. Људи су најчешће свесни позитивних, али не и негативних аспеката,[60] због чега је широј, а и знатном делу научне и стручне јавности релативно непознато колико смо као друштво зависни од компјутера и њихове осетљивости. Чињеница да много људи не може узети наведене претње довољно озбиљно, због непознавања и неразумевања проблема, цео проблем само усложава.[61]

[60] G. Thom, *исто.*
[61] S. Sloan, *исто.*

Решење је у покретању широке акције безбедносног образовања у цивилним, војним и полицијским школама и на факултетима и академијама ради подизања на знатно виши ниво информатичке безбедносне културе младих и свести о потреби заштите информационог амбијента. Дугорочно, то би била најкориснија и најисплативија инвестиција у изградњу и развој једног конзистентног нивоа свести и контрамера, поготову стога што су висока свест и стална приправност одлучујући у одвраћању и спречавању кибератака. Такав дугорочно осмишљен приступ је много бољи, рационалнији и ефикаснији од било које прекомерне реакције која се може јавити након појаве појединачних инцидената. Такође, друштво би морало стално да едукује и култивише национални информациони амбијент кроз организовање и одржавање научних симпозијума, семинара, курсева и разних других образовних облика у вези с том темом и да тако олакша разумевање претњи које постоје у том новом амбијенту и, колико је могуће, помогне у спречавању те врсте нежељених појава. Будући да кибератаци постају све већи проблем и реална опасност у друштву, сви би требало да буду свесни шта је то и какву опасност представљају, а имаоци и корисници информационе технологије би морали да се едукују о потенцијалним опасностима, барем толико да релативно лако могу да препознају претњу и да упозоре на појаву нарушавања заштите.

Како информациона технологија полако, али сигурно, креира друштво екстремно зависно од знања, постаје изузетно значајно правовремено организовање добро осмишљене и целовите стручне обуке ради оспособљавања кадра који може успешно да разрешава обимне и сложене проблеме који произилазе из тамне стране информационе технологије. Ту обуку, која се не може обавити преко ноћи јер је реч о дуготрајном процесу, који ће захтевати много креативног рада (учења), труда и времена и који би требало да се реализује кроз редовну наставу и разне врсте специјалистичких курсева, требало би, због мултидисциплинарности проблема, организовати на правном и електротехничком факултету, Факултету организационих наука, Факултету цивилне одбране и Војној и Полицијској академији, јер је на њима концентрисан кадровски потенцијал који не би смео да остане неискоришћен.

С обзиром на то да постоје нације, групе и појединци, с веома различитим циљевима, мотивима и ресурсима, који су реална претња и који могу атаковати на нас, потпуно је извесно да нас у блиској будућности очекују кибератаци различитог обима и интензитета, уз примену свих врста информационог оружја, и с потенцијално катастрофалним последицама. Управо због тога, предстоји нам тегобан и перманентан задатак *континуираног сагледавања стања и процењивања осетљивости националног информационог амбијента* на будуће претње и кибернападе. Такве процене су неопходне, пре свега, онима који су одговорни за националну одбрану и безбедност земље, јер треба да им омогуће да виде даље од непосредних претњи или тренутних инцидената.

Стога те процене морају да буду засноване на примени *стратешког обавештајног рада*,[62] форми која интегрише политику, социјалне студије и студије технологије, и која званичницима треба да обезбеди дугорочне прогнозе због чега има знатно ширу примену од оперативног или тактичког обавештајног рада, форми анализирања информација повезаних с непосредним претњама и суженим захтевима.

У оквиру тога, креатори националне политике и доносиоци одлука морали би, према својим овлашћењима и одговорностима, по хитном поступку да размотре сврсисходност (која је недвосмислена) и могућност да се при државним органима одговорним за безбедност и одбрану земље (првенствено министарства одбране и унутрашњих послова) формирају информатичка језгра, чији би превасходни задатак био заштита цивилне и војне информационе инфраструктуре. Реч је о сталном, веома значајном и озбиљном, одговорном и у стручном смислу изузетно сложеном мултидисциплинарном и мултидимензионалном задатку, за који су неопходни врхунски стручњаци различитог профила. Њихово деловање мора да буде потпуно интегрисано и синхронизовано, јер је изузетно опасна неактивност (пасивност) или било каква импровизација на том плану. Та језгра би била *аналитичко-оперативно-информационо-упозоравајући* центри. У оквиру њихове активности подразумевала би се примена оперативно-тактичког обавештајног рада ради процењивања намера, могућности и потенцијалних циљева постојећих и будућих противника, било да је реч о екстремним појединцима, терористичким групама или непријатељски настројеним државама, праћења критичне инфраструктуре, евидентирања нарушавања компјутерске заштите, анализирања случајева и одређивања питања која утичу на заштиту. Самостално или у сарадњи с другим субјектима требало би да изналазе одговоре и преносе их имаоцима и корисницима информационе технологије, и да иницирају, организују и подстичу размену идеја и информација (знања и искустава) и израду и развијање упутстава, смерница и препорука. *Превидети то сада значило би бити одговоран за последице у будућности.*

Литература:

1. W. M. Beale, *Technology association responds to cyber-attacks,* E-Commerce Times, February 10, 2000, http://www.ecommercetimes.com/news/articles2000/000210–7.shtml
2. M. Campbell, *Us at mercy of cyber terrorists,* Washington, May 17, 1998, http://www.infowar.com/class_3/class3_052798a_j.html-ssi
3. J. Carlin, *Us fears'electronic Pearl Harbor',* United Kingdom, Indepedent on Sunday, February 12, 1997, p. 12, http://www.infowar.com/class_3/class3_u.html-ssi
4. J. F. Cilluffo, *Cyber attack: the national protection plan and its privacy implications",* February 1, 2000, http://www.csis.org/goc/test02012000.htm

[62] *Исто.*

5. *Cyber terrorism,* American Banker, Mon, Sep. 08, 1997, http://www.infowar.com/CLASS_3/class3_091697a.html-ssi
6. *Cyber-terrorism „not welcomed“,* Jan 16, 2000, http://www.june4.org/news/database/jan2000/cyber.html
7. G. M. Devost, Houghton K. B., Pollard A. N., *Information terrorism: can you trust your toaster?* Terrorism Research Center, http://www.terrorism.com/terrorism/itpaper.html
8. L. Enos, Study: *Cybercrime continues to boom,* E-Commerce Times, March 22, 2000, http://www.ecommercetimes.com/news/articles2000/000322-7.shtml
9. S. Gold, *World cybercrime treaty may be underway,* Newsbytes, Special to the E-Commerce Times, January 14, 2000, http://www.ecommercetimes.com/news/articles2000/000114-nb2.shtml
10. W. Knight, *Experts warn of multiple computer attacks, zdnet,* Oct. 04, 2000, http://www.zdnet.co.uk/news/2000/39/ns-18252.html
11. J. Lamb, Etheridge J., *Dp: the terror target,* Datamation, February 1, 1986, str. 44–46.
12. M. Lawlor, *Tenacious security vigilance disarms technology terrorists,* Signal Magazine, July, 1998, http://www.infowar.com/class_3/class3_070698a-j.html-ssi
13. R. Lemos, *Hackers: uncle sam wants you!,* ZDNet News US, Mon, Jul 31, 2000, http://www.zdnet.co.uk/news/2000/30/ns-16974.html
14. W. C. Madsen, *The world meganetwork and terorrism,* Computers & Security, vol. 7, no. 4, 1988, str. 349.
15. I. McPhedran, *Australia „not ready“ for cyber-war,* Australia/New Zeland, The Canberra Times 16/09/97 p. 3, http://www.infowar.com/CLASS_3/class3_091997a.html-ssi
16. B. Menkus, *Notes on terrorism and data processing,* Computers & Security, vol. 2, no. 1, 1986, str. 13.
17. G. Morgan, *Digital crime plans come under attack,* IT Week, Oct. 16, 2000, http://www.zdnet.co.uk/news/2000/41/ns-18470.html
18. Р. С. Петровић, *Компјутерски криминал,* Министарство унутрашњих послова Републике Србије, Београд 2000, 398 ст.
19. R. S. Petrović, *Some aspects of cyber-terrorism,* Nauka, Bezbednost, Policija (NBP), Beograd, vol. V, no. 11, 2000, str. 27–48.
20. B., Sullivan, *EU pact criminalising security research?* Pt I & Pt II, MSNBC, Thu, 26. Oct. 2000, http://www.zdnet.co.uk/news/2000/42ns-18691.html
21. *Terrorism in the United States,* http://www.studyworld.com/Terrorism_In_The_United_States.htm
22. *Terrorism: motivations and causes,* Commentary No. 53 a Canadian Security Intelligence Service publication, January, 1995, http://www.csis-scrs.gc.ca/eng/comment/com53e.html
23. *Terrorist activities on the Internet,* Winter 1998, http://www.adl.org/Terror/focus/16_focus_a.html
24. K. Wong, *Computer crime – risk management and computer security,* Computers & Security, vol. 4, no. 4, 1985, str. 291.