# САЈБЕР ТЕРОРИЗМОТ КАКО ЗАКАНА КОН БЕЗБЕДНОСТА НА ДРЖАВАТА

**Автор М-р Јасмин Калач,**

**Јануари 2017 година**

## Вовед

Огромните достигнувања и развојот на врвната технологија, софистицираните компјутерски системи го отворија новиот „сајбер простор“, кој постојано ги уништува старите традиционални форми на организација, однесување и верување. Сајбер информациите доведоа до сајбер револуција и до појава на информатичкото општество, во кое доминира трката за информации и за комуникациски технологии, паралелно со светската либерализација и слободна циркулација на луѓе,стоки и идеи.[1] Денес, триесетина години после воведувањето на терминот, концептот кибернетика, тој неизбежно стана примарна компонента на голем број значајни термини: сајбер општество, сајбер политика, сајбер економија, сајбер војна, сајбер тероризам, сајбер криминал, во чија суштина најскапоцена круна преставува сајбер информацијата. Изградбата на современи и флексибилни компјутерски комуникациски системи и поставување TCP/IP протоколот како универзален протокол за комуникација овозможија информациите низ светот да се движат со неверојатна брзина, пренесувајќи ги сите настани во една нова димензија на комуникација,наречена сајбер простор. Новите форми на војување, а и тероризмот како специфична, современа „форма на војување“ ќе коегзистираат во исто време со „сајбер просторните“ напади. Најголемиот проблем можеби лежи и во фактот што интернет просторот од правен аспект се уште не е регулирана материја и според некои експерти е дефиниран како ,,Ничија земја,,.

[1]Stern, Jessica. The Ultimate Terrorists. Cambridge, MA: Harvard University Press, 1999.p.204

Постоечките норми во меѓународното право и правилата во националните законодавства не можат целосно да ги опфатат сите тие феномени кои се случуваат. Потребни се нови концепти и реформа во однос на инкриминирање на ваков тип на форми на сајбер криминалитет.

## 1. Сајбер тероризмот како глобална безбедносна закана

Сајбер тероризмот претставува  една од главните глобални закани на современата безбедност. Системи за заштита од ваков вид на напади поседуваат меѓународните организации како НАТО и ЕУ и развиените држави како што се САД, Кина, Русија, Велика Британија и други. НАТО е единствената организација која на систематски  и стручен начин се занимава со заштита од овој тип на тероризам  и поседува развиен систем на сајбер одбрана. Како би останале во тек со рапидно променливите облици на закана и како би одржале силен ниво на сајбер одбрана, НАТО усвои нова и напредна политика и акционен план кој го подржаа сојузниците на Самитот во Велс во септември 2014 година. НАТО силите за одговор на компјутерски инциденти (The NATO Computer Incident Response Capability (NCIRC) ја штити сопствената мрежа нудејќи 24 часовна подршка во сајбер одбраната на разни сајтови на НАТО. НАТО Кооперативниот центар за сајбер одбрана ( The NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE)) во Талин во Естонија е најистакната од страна на НАТО акредитирана институција за истражување и обука, која се занимава со образование, консултации, размена на лекции и развој во врска со сајбер одбраната. Целокупниот овој систем е токму фокусиран и лоциран во Естонија, бидејќи оваа Балтичка држава Естонија во 2007 е нападната од страна на хакери кои ја блокирале буквално целата инфраструктура во земјата на определен период. Тогашните политички односи помеѓу оваа земја и Русија беа затегнати, можеби и поради фактот дека Естонија во 2004 година стана земја членка на НАТО, а се шпекулира и дека сајбер нападот е како резултат на Естонско-Рускиот спор за отстранувањето на бронзена статуа на која бил прикажан Советски војник од Втората

Светска војна во центарот на главниот град на Естонија - Талин[2]. Доколку пак ги мериме способностите за сајбер војување на определени држави, покрај САД, Кина, Русија, Израел и Франција, според проценитe на стручњаците постојат помеѓу 20 или 30 држави кои имаат респектабилни способности за сајбер војување (Тајван, Иран, Јужна Кореја, Индија, Пакистан..)[3]. Според тоа можеме да заклучиме и дека тие способности можат да бидат злоупотребени.

Сајбер тероризмот е значаен подсистем на сајбер војувањето, и е многу потежок за откривање и спротивставување, бидејќи е скоро неможно да се одреди политчката припадност или спонзорите на неговите извршители. Кога се зборува за поимот сајбер тероризам, според Федералното истражно биро – ФБИ овој феномен се дефинира како: „предумислени, политички мотивирани напади против информации, компјутерските системи, компјутерските програми и податоци што резултираат со насилство против цели кои не се воени од страна на суб – националните групи или тајни агенти“. [4]

Сајбер војувањето е насочено спрема информациите и информативните системи што даваат подршка на цивилните и воените структури на противникот. Тоа навлегува во сфера која е многу посуптилна од физичките напади и уништувања, односно дејствува врз протокот на информациите во мрежите и манипулира со нив (прекинува, видоизменува, додава и слично). Неговите активности се насочени првенствено кон информациите кои се пресудни за функционирање на цивилните и воените системи како и контролата на авиосообраќајот, стоковите берзи, меѓународните финансиски трансакции,логистичките потреби и цели.

Можностите за енормно нарушување на националните компјутерски системи и можноста да го загрозат нормалното пулсирање на општествениот живот, како и опасностите за масовно загрозување на животите на луѓето придонесуваат терминот

[2] Hower, Sara; Uradnik, Kathleen (2011). *Cyberterrorism* (1st ed.). Santa Barbara, CA: Greenwood. pp. 140–149. Retrieved 4 December 2016.
[3] Idem, p. 127-128.
[4] Според Федералното биро за истрага – ФБИ (http://searchsecurity.techtarget.com/sDefinition/0.,sid14_gci771061,00.html)

„сајбер тероризам“ да биде опколен со чуство на страв и завиткан со велот на мистериозност.[5]

Ако војувањето со информации , без сомнение , ќе преставува начин за војување во иднина, тогаш и иднината на тероризмот ќе биде суштински детерминирана со појавата на сајбер тероризмот. Привлечноста на војувањето со информации спонзорирани од државата е толку голема што многу нации не ќе можат да одолеат на овој„предизвик и искушение“. Меѓутоа, сајбер тероризмот во иднина ќе преставува нова „фатална привлечност“, за голем број на терористи и терористички организации. Овој тероризам е нај јасен пример за глобализацијата на светот, но и истовремено негово „вонбрачно палаво дете “, кое опасно ќе ги загрозува комуникациите во воената сфера, службите за итна медицинска помош,системите на сообраќај од различен вид ,телекомуникациите и другите добра. Исто така, неговите „хакерски игри“ може да предизвикаат хаос и анархија преку нападите на банкарите и други финансиски и компјутерски врски и тотално да го парализираат животот во големите урбани центри на најразвиените држави.[6]

Во нивниот широк дијапазон на активности спаѓаат и користењето на приватните информации во функција на изнудување исти форми на сајбер криминал, преку влегување во мрежите, како и физичко и електронско уништување на дигиталниот информациски систем. Веќе не постои дигитален уред кој не може да стане жртва на компјутерските вандали и терористи. Сите уреди поврзани со компјутерите можат да станат цел на хакерите, кои преку глобалната компјутерска мрежа можат да внесат дигитален код што ќе го наруши нивното регуларно и нормално работење. На секој уред што се поврзува во мрежа можат да му испратат низа дигитални команди што ќе направат уредот да работи онака како што ќе посака креаторот на тие команди. Класичните системи за заштита се речиси беспомошни во поглед на методите што ги користат денешните хакери и сајбер терористите.

Главна опасност денес преставуваат хакерските кодови, кои користејќи ја секоја пригода се импементираат во некоја затворена компјутерска мрежа, креирани се така што можат самите да се активираат и да биде ефектот уште постршен, самите да го изнаоѓаат

[5]Митко Котовчевски “Борба против тероризмот”, Македонска цивилизација -Скопје.str 182
[6]Badey, Thomas (ed.). Violence and Terrorism 05/06. Dubuque, IA:McGraw-Hill/Dushkin, 2005.p.152

патот за своето размножување,ширејќи го „злобниот код“. Исто така и принтерите кои постануваат се пософистицирани, надградени со побројни софтверски апликации за подршка може да бидат искористени за хакерски сајбер терористички упади во мрежите.[7]
Во правна смисла, сајбер тероризмот преставува намерна злоупотреба на дигиталниот информациски систем, мрежа или компонента што ја заокружува или комплетира терористичката борба и активност. Последица од злоупотребата на системот нема да биде директно насилство против луѓето (што не е ислучено на пример со паѓање на авиони, хаос во болниците и слично),но сепак ќе може да предизвика страв, зголемување на светскиот криминал со најбрзо темпо, најголема стратешка ранливост на сите витални општествени функции, огромни човечки страдања но и жртви како „колатерална штета“. Во овој контекст,уште пострашен е и фактот што овие суптилни дејства може да иницираат и кибернетичка војна или да “наместат“ определени држави да отпчнат класична војна, како одговор на сајбер дејствата “преземени од друга страна“. Според определени американски размислувања само е прашање на време кога САД може да го искусат “сајбер перл харбур“, кои би имале опустошувачки резултати, кражби на електронски фондови на податоци со кои би се подржале терористичките информации,препраќање,пренасочување на пратките со оружје и слично. Но веројатно најопасна е евентуалната симулација на “сајбер Чернобил“ хаварија.

## 2. Методи за извршување на сајбер тероризам

Во општествата на третата технолошка револуција постојат две основни методи преку кои терористите можат да извршат терористички напади.
Првата метода е кога самата информациска технологија преставува цел на терористичките напади. Со изведување на определени саботажи (електронски и физички) врз информацискиот систем, ќе се обидат да го уништат или да извршат прекин во функционирањето на информацискиот систем и информациска инфраструктура, во зависност од самата конкретна цел.[8]

[7]Tuchman, Barbara. The Proud Tower. New York: Macmillan, 1967.p.52
[8]White, Jonathan. Terrorism: An Introduction. New York: Thompson-Wadsworth, 2003.p.89

Втората метода е кога информацискиот напад преставува средство-чекор за спроведување на поголема операција. Овој чин имплицира дека терористите ќе прават напори за манипулација и експлоатација на информацискиот систем, кражба на информации како алтернатива или принудување –“програмирање“ на системот да врши функција за која не е наменет.

Под поимот компјутерски вируси се мисли на програми кои несовесни поединци ги пишуваат за да нанесат што поголема штета на многу компјутери врзани во мрежа како на пример на глобалната Интернет-мрежа. Нивни основни одлики се: се копираат самите себеси на секој компјутер со кој ќе дојдат во контакт. Не се забележливи, односно најчесто се невидливи за корисникот на компјутерот, посебно ако на компјутерот не е инсталиран специјализиран софтвер за нивна детекција. Автоматски извршуваат одредени команди како бришење на корисни податоци на компјутерот на жртвата, или пак ги испраќаат податоците на одредена друга локација на мрежата без знаење на сопственикот на компјутерот.

Покрај хакерите и групите што тие ги организираат за неовластено навлегување во заштитени системи, на денешно време постојат и специјализирани тајни владини служби кои преку навлегување во компјутерскиот систем на другите држави прибавуваат податоци од разузнавачкаприрода. Така под поимот компјутерска шпионажа може да се дефинира еден однајмодерните облици на разузнавање, но исто така постои и индустриска шпионажа која е само од комерцијална природа. Компјутерска саботажа имаме во случај кога некој ќе уништи, избрише, промени, прикрие или на друг начин ќе онеспособи податок, програма или ќе го оштети компјутерот кој е од значење за државен орган,институција, јавна служба.

Нападот со информатичката технологија е лесно изводлив,со примена на евтини средтва кои лесно се прикриваат и виртуелно се недофатливи. Ако е познато дека терористите “лудуваат“околу нивната медиумска промоција, ако е познато дека нај посакувана цел на терористите се медиумите , тогаш со сигурност можеме да констатираме дека можностите на терористите за несметан упад во осетливата информациска технологија енормно ги зголемува нивните можности за “информатичко војување“.Тоа е само уште едно совршено оружје во богатиот арсенал на оружје на терористите кои неуморно ги следат сите современи трендови и во оваа значајна сфера.

Мотивациите за извршување на вакви напади се секако добро познатите барања за политички промени, социјални промени или економски промени.

Ако денес постојат огромен број на објективни и субјективни пречки за отпочнување на сајбер војни од поголеми размери(пример меѓународната економска зависност,ескалацијата и одговорот од другата страна со воен конфликт , немање на технолошка подготвеност), тогаш за новите "терористи" не постојат никакви пречки, нити"црвена линија"за отпочнување на сајбер тероризмот на глобален план.

Невидливиот непријател вооружен единствено со лап топ персонален компјутер,конектиран на глобалната компјутерска мрежа,"вооружен"со огромно човечко знаење трансформирано во дигитален код, кој одлучува со огромна деструктивна енергија и огнена желба да ги оствари своите мрачни цели, впловува во напад со тешко препознатлив правец,но со единствена цел: електронски атак врз државната информациска мрежа од огромно стратегиско значење за несметано функционирање на сите витални општествени функции.[9]

Тоа е злокобното лице на сајбер терористот и на сајбер тероризмот, опасна закана за националната безбедност на определени држави,смртна закана и за глобалната безбедност во наредниот период. Тоа е опасност блиска до атомска бомба.Инвазијата на сајбер просторот и понатаму продолжува со огромна брзина, со брзината на развојот на моќната офанзивна компјутреска технологија.Светот повторно се наоѓа пред уште еден нов и мошне опасен сериозен безбедносен предизвик од најголемото зло-тероризмот.

## 3. Цели на напад на сајбер тероризмот

Во денешно време, најсовременото оружје е компјутерот. Секој добро обучен компјутерџија е добар војник. Секое дете кое што добро го разбира концептот на компјутерите и начинот на работа на некои програми е потенцијална опасност за целиот свет. Во светот постојат многу примери на компјутерски напади, при што жртви на таквите напади се најразлични компании или владини институции. Се поставува прашањето која е целта на таквите напади? Што се постигнува со тие напади? Во многу

[9]www.ict.org.il

случаеви со таквите напади се крадат информации од воени институции со кои што директно се загрозува безбедноста на одредена земја. Во други случаи се крадат кодови од некои програми кои што се во развој, а во трети случаеви пак нападите се извршуваат едноставно за забава (или пак тренинг). Ова ќе се разгледа преку примери за компјутерски напади во кои што се нападнати сервери од една земја од страна на компјутерции од друга земја.

Во 1997 година ИРА ја шокираше англиската јавност со упатување на закани дека покрај бомби атентати и други облици на терористички напади ќе почне да користи и електронски напади на службените и владини компијутерски системи.

Искуствата со Ал-каеда и ИСИЛ исто така покажаа дека припадниците на овие терористички организации се служат со софистицирани техники на заштита на своите канали на комуникација преку Интернет , секојдневно поставување на нови веб локации на коишто ги пропагираат своите фундаменталистички идеи , а кај некои од уапсените терористи се пронајдени компјутери со шифрирани фајлови.[10]

Нападот на Светскиот Тровски Центар во Њујорк знаеме сите добро како заврши. Меѓутоа интересно беше нешто друго. Непосредно со нападите, беше блокиран и официјалниот сајт на Светскиот Трговски Центар. Тешко е ова да се нарече случајност. Непосредно по овој напад, во САД се стравуваше од повторен напад, но овој пат компјутерски. Според мислењето на американските стручњаци успешноста на ваквиот напад би ја парализирал целата држава. За нивна среќа ваков напад не следеше (барем не успешен). Меѓутоа од превентивни мерки, Пентагон беше „откачен“ од Интернет. САД се спремаше за „електронски Перл Харбур“. Штетите од ваквиот напад би биле непроценливи. Имено пред неколку години во САД, извесен Robert Moris, син на некојод директорите на Агенцијата за национална безбедност, во мрежата уфрлил програм кој што во потполност ги парализирал компјутерите во некои од најважните федералнии универзитетски институции (за тоа добил казна само од 10 000 долари и 3 години условен затвор).[11]

Изразива „сајбер“ војна се водеше помеѓу Кина и САД во мај 2001 година (причината беше сударот на кинески авион со амерички шпионски авион). Веднаш после

[10]Списание, декември 2001: Одбрана бр. 68
[11]http://www.terrorism.org/

сударот почнаа напади најпрвин од кинеска страна. Цел на таквите напади беа серевери ширум САД, а страдаше и страницата на Американкиот конгрес. Карактеристично е тоа што при овие напади не се направија некои поголеми штети, туку само се изменисодржината на некои страници (најчесто се испишуваа кинески симболи). Меѓутоа и хакерите од САД на овие напади не останаа должни. Тие одговорија со напади на веб страниците на покраинските власти во некои од покраините во Кина, како и на корејските компании Samsung i Daewoo Telecoma. (интересно е тоа што во оваа„сајбер“ војна, на страната на американците беа хакерите од Саудиска Арабија,Пакистан, Индија, Бразил, Аргентина и Малезија, а на страната на кинезите хакерите од Јапонија, Кореја и Индонезија). Очигледно беше дека државите ги финансираа ваквите напади, бидејќи двајца „големи“ хакери беа задолжени за припрема на серверите во САД од можни напади.[12] На 1 јули 2001 година, во Мексико бил уапсен некој мексикански тинејџер кој бил обвинен дека извршил напад врз НАСА. Тој успеал да влезе во серверот, модифицирал некои фајлови и креирал некои нелегелни акаунти. Интересно е тоа што во одбраната, мексиканскиот тинејџер се бранел со тоа дека немал никаква врска со компјутери, и дека лажно е обвинет. Дали со тоа државата сака да влее страв помеѓу хакерите за успешно нивно гонење? Дали државата се служи со лажни обвиненија? Зошто се тие лажни обвиненија ? Докажувањето на овој тип на криминалитет е многу тежок и секако дека на правосудните органи им е недвосмислено потребна стручна помош од стручни лица кои што добро ја разбираат и се упатени во оваа проблематика, поготово што заканите во сајбер просторот се во постојана еволутивност.

## Заклучок

Развојот на современата технологија ја зголемува одбраната од терористичките закани, но исто така ги зголемува и можностите на терористите за успешно остварување на нивните цели.Терористите денес многу лесно оперираат во кибернетскиот простор така што уништуваат определени податоци, но и манипулираат со значајни податоци. Денешните “ компјутерски крадци “ со терористичките намени можат да влезат во

[12]Богоев Славчо,Колективните системи на безбедност: процес и критериуми на интеграција на Република Македонија во НАТО, Правен факултет, 2010 стр 63

најбезбедните банки на податоци со цел да извршат кражба на безбедносно осетливи информации и да ги уништат или блокираат. Овие можности ги зголемуваат шансите терористите да манипулираат на берзите во свој интерес, да предизвикаат определен финансиски застој или да го забрзаат процесот на инфлација.

Значајно е да се каже дека сајбер тероризмот во иднина ќе претставува многу опасна форма на политичко насилство. Ниту Македонија не е имуна на овој тип на сајбер напади на инфаструктурата кои би можеле да се случат. Сите надлежни институции во овој контекст како што се МВР, Министерството за информатичко општество, Центарот за управување со кризи и други надлежни органи треба да превземат мерки со цел зајакнување на безбедносниот систем одо овој вид на сајбер напади. Со оглед на фактот дека овој тип на тероризам претставува сериозна глобална закана, Република Македонија треба да ја зајакне меѓународната соработка во овој контекст и да превземе соодветни мерки и стратегии за заштита од овој вид на сајбер тероризам. Се наоѓаме во период и во време кога националната безбедност е секојдневно присутна тема во медимумите па со тоа и во јавноста ширум Европа и светот. Во тој контекст, сајбер безбедноста и градењето на добра и ефикасна стратегија за имплементација на истата претставува можеби и клучен елемент на кои се базира успешноста на одбранбениот систем на една земја. Целокупната може да се каже инвазија на сајбер просторот се шири со огромна брзина и во иднина можеме да очекуваме се повеќе сајбер напади. Тероризмот во иднина или иднината на тероризмот треба да претставува значаен патоказ за современите влади во која насока ќе треба да се организира борбата против тероризмот, а посебно против сајбер тероризмот.

## КОРИСТЕНА ЛИТЕРАТУРА


Stern, Jessica. The Ultimate Terrorists. Cambridge, MA: Harvard University Press, 1999.p.204

Hower, Sara; Uradnik, Kathleen (2011). *Cyberterrorism* (1st ed.). Santa Barbara, CA: Greenwood. pp. 140–149. Retrieved 4 December 2016.

Idem, p. 127-128.

Според Федералното биро за истрага – ФБИ (http://searchsecurity.techtarget.com/sDefinition/0.,sid14_gci771061,00.html)

Митко Котовчевски "Борба против тероризмот", Македонска цивилизација -Скопје.str 182

Badey, Thomas (ed.). Violence and Terrorism 05/06. Dubuque, IA:McGraw-Hill/Dushkin, 2005.p.152

Tuchman, Barbara. The Proud Tower. New York: Macmillan, 1967.p.52

White, Jonathan. Terrorism: An Introduction. New York: Thompson-Wadsworth, 2003.p.89

www.ict.org.il

Списание, декември 2001: Одбрана бр. 68

http://www.terrorism.org/

Богоев Славчо,Колективните **системи на безбедност: процес и критериуми на интеграција на Република Македонија во НАТО, Правен факултет, 2010 стр 63**