Универзитет „Св. Кирил и Методиј" – Скопје

Филозофски Факултет – Скопје

Институт за безбедност, одбрана и мир

Влијанието на високо – технолошкиот тероризам врз националната безбедност на современите држави

(магистарска теза)

Ментор:

Проф. Д-р. Митко Котовчевски

Изработил:

Кристина Ганиќ-Јанушева

Скопје, 2017

Содржина

Глава прва

Глава втора

Глава трета

Глава четврта

Глава пета

Глава шест

Глава прва

Вовед

Почетокот на дваесет и првиот век, век на глобализација е окарактеризиран како век на тероризам. За многумина тероризмот преставува нешто непознато, но таквата општествена појава своите почетоци ги има уште од античко време, и како таква има значење на нешто неприфатливо, нечовечно, страотно. Глобализацијата, како процес на културно, политичко и економско поврзување е присутен во сите сегменти на современите држави. Иако самиот процес на глобализација сеуште неможе да се одреди, јасна е разликата на оние што го спровеле од другите кои го трпат. Голем е бројот на луѓе кои ширум светот себеси се доживуваат како жртви на глобализацијата или како субјекти на процес со негативен третман. Ако се погледне од аспект на општествено-економската и социо-културната улога на овој процес, многу субјекти себеси се сметаат за запоставени, оцрнети, експлатирани и со самото тоа загрозени, па како последица на таквото незадоволство се појавува насилството. Од тој аспект денес, се почесто се појавуваат радикални и етнички групи, па и цели држави кои на тероризмот гледаат единствен начин за борба на таквите хегемонистички сили.

Пред да се обидеме да го дефинираме високотехнолошкиот тероризам неопходно е да го поставиме прашањето: Зошто воопшто е потребно да се обидеме да го дефинираме тероризмот?

Одговорот на ова прашање е мошне едноставен но и суштински неопходен. Потребата за дефинирање на тероризмот произлегува од фактот дека е неопходно да се дефинира соодветното однесување кое не е прифатливо и кое се смета за противзаконско од страна на системот на криминалистичкото, односно кривичното право на секоја држава.Тероризмот неминовно доаѓа во судир со правниот поредок на секоја современа држава како мошне опасен извор на загрозување на нејзината национална безбедност. Тероризмот во суштина преставува криминална повреда на скоро секој национален или меѓународен правен кодекс.Постојат различни сфаќања при обидот за дефинирање на тероризмот. Најопшто се прави разлика помеѓу индивидуален тероризам (кој може да се јави во разни форми: терор според општото право, како општ облик на насилнички криминалитет, патолошки терор - како манифестација на растроено душевно здравје, политички терор зад кои стојат политички мотиви и сл.) и државен терор (насилство што го врши државата спрема своите граѓани, како што е примената на репресија без суд, прогонување на политичките противници или спрема други држави, како што е агресивната војна и другите напади врз интегритетот на други држави. Фасцинантноста на тероризмот, практично може да се следи од почетокот на историјата, идентично како и војната која го следи човекот од најстарите времиња до денес. Тероризмот како традиционална тактика на послабиот го следи развојот на човековата цивилизација најнапред во форма на атентати, киднапирања и земање заложници. Уште пред Христовото раѓање, извршениот атентата врз некој тирански владител не само што бил оправдуван, туку често пати бил и величен, пофалуван и почитуван како многу значаен и способен чин.

Тероризмот како глобален проблем е во постојана експанзија и трансформација, преминувајки од еден во друг облик, па поради таквата состојба е неопходно постојано следење и пронаоѓање на нови можности и механизми за успешни и ефикасно справување со овој вид на закана. Како глобален проблем и закана „современиот тероризам„ се карактеризира со висок степен на организација, конспиративност, нехуманост, злочин, глобализам, злоупотреба на најсовремените научно-технички и технолошки достигнувања, како и злоупотреба на верските чуства и верска припадност, голема финансиска моќ преку пороцесот на перење пари и разни манипулации во вид на подршка на пари од институции и мултинационални компании во многу држави.

Интернет технологијата со сите свои многубројни позитивни аспекти, во голем степен го промени човештвото, а со тоа предонесе и кон процесот на ефикасност и екфективност во делувањето на криминалните ораганизации. Во првата деценија на дваесет и првиот век компјутерскиот криминал и високотехнолошкиот тероризам преставува тема која избива во прв план на многу меѓународни конференции и во законодавствата на меѓународно кривично право. Пред се високотехнолошкиот криминал претставува искористување на информациите или телекомуникациските технологии, со што би се извршило кривичното дело против имоти, лица, организации или компјутерски системи, а кривичното дело на високотехнолошкиот криминал во суштина преставува традиционално или ново кривично дело сторено по пат или со помош на компјутерска мрежа или компјутерски систем, додека пак високотехнолошкиот тероризам преставува процврст компјутерски криминал поврзан со тероризам. На ваков начин тероризмот преставува поголема закана наспроти тероризмот на кој досега го познаваме, но поголема закана и од други облици на високотехнолошки криминал. За таа цел овој труд ќе ги разгледува новите степени на загриженост и закани од високотехнолошкиот тероризам кој својот замав како современа закана по безбедноста на современите држави од ден на ден се повеќе и повеќе го замислува и го прави се потешко за детектирање и превенирање. Ваквата загриженост во голема мера е помеѓу корпорациите, владите, војската и други организации кои во голема степен стравуваат по нивното делување. Денес современите општества се виртуелни во една ситуација на страв и паника од информатичките достигнувања каде технологијата е голем овозможувач, но во исто време може да биде и голем оневозможувач кога станува збор за извршување на функции со помош на истите. Секакви нагли промени во овој домен со себе носат и големи финансиски и национално безбдносни последици што го прават секое општество осетливо и ранливо, но и меѓузависно од мрежните поврзувања за вршење работи ден за ден како во банкарскиот сектор, така и во транспортиниот , енергетиката, водостопанството и сл.

За таа цел преку прашањата и дилемите кои ги актуелизирам во трудот се обидов преку проактивен пристап да ја потврдам и со самото тоа да ја доближам парадигмата за постоење на високотехнолошкиот тероризам, нагласувајќи ги неговите десегашни методи и техники кои во иднина, со достигнувањата на новите технолошки изуми би се развивал побрзо отколку би можеле да замислиме. Она што се надевам е

дека со помош на т.н. модел за спознавање на суштината на тероризмот успешно ќе биде разбран светот на високотехнолошкиот тероризам како нова димензија на закана и војување, а воедно и на одреден начин ќе потикнам идни истражувачки и аналитички достигнувања за да не остане нешто неразјаснето, па отука овој вид на тероризам-високотехнолошкиот тероризам да ги искористи сите слабости, а со тоа да земе поголеми размери во иднина.

Доколку бидат прифатени определените согледувања кои се резултат на истражувањето, тие ќе преставуваат одличен предуслов за градење на контратеристички методи и техники во одбрана на ваквите закани од високотехнолошкиот тероризам.

1.Формулирање на истражувачки проблем

Со појавата на новите технологии во 80-те години на минатиот век, особено со појавата на интернетот доаѓа до појава на информациски конфликт или ``Net Ware``, но исто така, и нови форми на тероризам во информацискиот простор (Cyberspace), или попознат како информациски тероризам. Информатичката револуција во денешно време ја трансформира светската политика. Пред четири века, англискиот државник-филозоф Франсис Бекон (Francis Becon, 1626) напишал дека знаењето е моќ[1], па отука и самиот факт дека реализацијата на новите изуми ја доведе денешната информатичка револуција која не застанува тука и секојдневно се движи во нагорна линија на нови и нови откритија. На почетокот од дваесет и првиот век (XXI век) голем дел од популацијата и во рамки и вон земјите имаше пристап до оваа моќ. Владите отсекогаш биле загрижени за протоколот и контролата на информациите, а тековниов период е прв на кој силно влијание имаат промените во информатичката технологија. Како што истакнуваат конструктивистите: брзите промени во информатичката технологија можат да доведат до важни промени кај идентитетите и интересите. Таквата информатичка револуција се заснова на брзиот технолошки напредок на: компјутерите, комуникациите и софтверот. Во средината на дваесетиот век, луѓето стравувале дека компјутерите и комуникацијата на тековната информатичка револуција би создале централна владина контрола. Масовните компјутерски ситеми се чинеа погодни да го унапредат централното планирање и да ја зголемат моќта на надзор на оние кои се на врвот на контролата на пирамидата. Сепак технологијата на ширење еволуира, и програмите им овожможија на корисниците анонимно да тргуваат со дигиталните информации. На ваков начин се постигна намалување на трошоците кои претходно натежнуваа на државите. Но како што компјутерската моќ ги намали трошоците, а димензиите на компјутерите се смалија, а со тоа станаа пошироко дистрибуирани, така нивните децентрализирачки ефекти натежнаа над нивните централизирачки ефекти. Интернетот создаде систем во кој моќта над информацијата е многу пошироко дистрибуирана. Во споредба со радиото, телевизијата и весниците, кои се контролирани од страна на издавачите, и радиодифузерите, интернетот создаде неограничена комуникација ``еден-на-еден``(преку e-mail), ``еден-на многу`` (преку лична веб страна или блог),``многумина-на-еден`` (преку електронско емитување), и можеби најважното, ``многумина-на-многумина`` (on-line chat room-простор за

[1] Нај, Џозеф С, Помладиот-Разбирање на меѓународните конфликти, Академски печат, Скопје, 2008, стр:298

дискусија или massage board, простор за пораки). Новите информатички технологии многу повеќе се стремат и ги потикнуиваат мрежните организации, новите типови на заедници и потребите за различни функции на владата отколку да ја зајакнат централизацијата и биократијата. Ова значи дека светската политика нема повеќе да биде делокруг само на државниот врв, туку поединци и приватни организации, па се до терористи, ќе имаат моќ директно да учествуваат во креирањето на светската политика, со што многу современи држави стравуваат по нивниот систем на национална безбедност. Ако вака е се позголемена зависноста на општеството од компјутерите и информатичката технологија, тоа од друга страна значи и негова зголемена ранливост, било тоа да е од физички, а пред се од т.н сајбер напади.

Во изминатите две декади, најшироко започна, а особено пишува во литературата за проблемот со високо-технолошкиот тероризам, но сепак авторите заземаат различни ставови во врска со неговото дефинирање.[2]

Во овој труд ќе се обидеме да ги согледаме празнините кои постојат во двата спротиставени ставови, и да го разгледаме и дефинираме високо-технолошкиот тероризам како можна современа тактика од една страна и веќе постоечките сајбер терористички напади, забележани во литературата кои укажуваат на тоа дека ваквата закана е реална и неизбежна, и преставува сериозна тактика-начин за рушење на системот на национална безбедност. За да можеме подобро и поцелосно да се разбере оваа релативно нова закана, ќе тргнеме од дефинирање на поимот „Тероризам`` која е добро проучен, дефиниран и документиран. Но, значењето на овој термин се менува со времето и политиката. Со ова не се сугерира дека оној кој за некого е терорист, за друг е борец за слобода, но се сугерира дека терминот тероризам во различни времиња, има различни/о значење. Алекс Шмид (Alex Schmid 1983,str.70-111) смета дека нејасната природа на тероризмот се должи на неговата геополитичка природа.[3]

``Тероризмот е анксиозно-инспиративен метод на повторени насилнички акции, сторени од страна на (полу)тајни поединци, групи или актери, за карактеристични, кривични или политички причини, при што-во контраст со атентатот-дирекните цели на насилството не се главните цели, туку непосредните човечки жртви на насилството обично

[2] Stohl,M., Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games? Crime, Law and Social Change, p. 223-238, превземено од http://www.5pringerlink.com

[3] Филип Рајкел, Прирачник за транснационален криминал и правда,``Датапонс``2009 г.стр.74

избрани по случаен избор (цели на можност) или селективно (преставник или симболични цели) од целната популација, кои служат како генаратори за порака. (Шмид, 1988).[4]

И покрај тоа што мотивите остануваат непроменети, денешницата и иднината носат нови и досега непознати облици. Разузнавачките системи, тактиките, безбедносните процедури и опремата, од кои порано се очекуваше да бидат средства за заштита на луѓето, системите и нациите, денес се немоќни против новите, современи облици на ова застрашувачко оружје. Освен тоа и методите за бораба против тероризмот во сите негови облици што светските експерти ги практикуваат во изминативе години, се покажуваат како неефикасно против ваков вид на непријател? Отука и прашањето како е тоа неможно да се види или да се насети напријателот?

Ако непријателот во своите терористички намери досега бил виден во облик на актовки полни со Сари гас или нападот го реализираше со камиони наполнети со експлозиви, или пак со појас нареден со динамити, овде станува збор за напад со помош на единици и нули, на местото каде што сме најранливи, на точката каде што конвергираат Реалниот (физичкиот) и Виртуелниот свет.

✓ Физичкиот свет – се дефинира како материја и енергија - светлина, темнина, топло и ладно, целокупната физичка материја, она место во кое живееме и функционираме;

✓ Виртуелен свет – е симболичен, вистина - невистина, бинарно, метафорично преставување на информациите, она место во кое функционираат компјутерските програми и каде што се пренесуваат податоците.

Светот кој е компјутерски симулиран има тенденција да биде сличен на реалниот свет, со законитостите кои важат во реалниот свет, како што се на пример: гравитација, топографија, движење, акции во реално време и меѓусебна комуникација. Коминикацијата, се одвива во форма на размена на текст пораки, но во поново време на располагање е и говорна комуникација во реално време со користење на ГПИП (Говор преку интернет протокол).[5]

Физичкиот и виртуелниот свет по природа се неспоивли, но токму конвергенцијата на овие два света ја даваат можноста за развој и употребата на новото оружје во светот, попознат под поимот високотехнолошки тероризам. Честопати, голем број од неовластени навлегувања или пробивања се извршени од најразлични побуди, и за најразлични цели,

[4] http://web.archive.org/web/20070527145632/http://www.unodc.org/unodc/terrorism_definitions.html

[5] http://mk.wikipedia.org/wiki/Виртуелен_свет

тргнувајки од досада, заради забава или како што најчесто знаат да кажат самите хакери, едноставно за да докажат дека можат.Но прашањето е, дали ова е основната цел и основниот двигател на нападот на еден сајбер терорист? Дали сајбер терористот, неовластено навлегува на официјалната веб-страница на одредена влада, се со цел да го истакне своето незадоволство или да потенцира дека таквата влада е лоша?

Одговорот на сите овие дилеми е со негативен исход, бидејки овие примери се дел од активностите на така наречените хакери кои што постојат и дејствуваат на сличен начин ширум светот.Основите цели на дејствување на еден сајбер-терорист се многу поинакви од претходно наведените. За да се докаже на што точно се мисли кога велиме дека станува збор за високотехнолошки тероризам, во понатамошното елаборирање ќе разгледаме неколку потенцијални високотехнолошки (сајбер) терористички акти. Притоа ќе тргнеме од основната дефиниција за поимот тероризам, и во таа насока ќе определиме дали наведените примери навистина ги содржат конститутивните елементи за поимот тероризам, за да можеме да зборуваме за високотехнолошки (сајбер) терористички акти.

Сајбер терористот ќе го наруши работењето на банките, интернационалните финансиски трансакции и работењето на берзите во светот или во одредена земја со цел да предизвика дестабилизација на земјата и губење на довербата на граѓаните во нејзините економски ситеми;

✓ *Сајбер терористот, нема потреда да влезе во просториите на зградата за национални резерви, или слична на неа , бидејки секако дека на тој начин би се изложиле на негово откривање или во крајна цел и негово фаќање на лице место. Тој едноставно, по пат на компјутерски системи, ужива на некој континент, со еден збор ужива на безбедно место додека го врши делото;*

Сајбер терористот може да размести одреден број на компјутеризирани експлозивни направи низ еден град, кои едновремено или симултано ќе емитираат одредени нумерички низи, односно ќе следат одредени нумерички шеми, и доколку дојде до прекин на емитувањето на сигналот од некоја од нив, останатите ќе експлодираат едновремено;

✓ *Сајбер терористот не мора на себе да има врзано ниту еден од експлозивите направи;*

✓ *Бројот на експлозивни направи и нивната дисперзија во урбаниот простор се обемни;*

✓ *Шифрираните шеми не можат однатред да се предвидат ниту да се измени низата на емитување на сигналите;*

Сајбер терористот, со помош на далечинско компјутерско управување ќе навлезе во контролниот систем на одреден производител на земјоделски или житни култури, ќе го промени нивото на одредени хемиски супстанци, штетни за човековиот организам и на тој начин ќе предизвика болести или смрт кај припадниците на одредена нација, конзумент на таквата храна;

✓ *Сајбер терористот не мора да се наоѓа во близина, ниту да биде присутен во фабриката во моментот на извршување на делото;*

Сајбер терористот, навлегувајќи во компјутерскоит систем за контрола на воздушниот и железничкиот сообраќај ќе предизвика директен судир на цивилни воздухоплови, или пренасочување и уривање на воздухопловните летала, или на ист начин да предизвика судар на две возила;

✓ *Ваквото сценарио е секако реално, бидејќи станува збор за навлегување во компјутерски системи на воздухопловите во кабината за летање и контрола или неоспособување на сензорите на истите;*

Сајбер терористот може да одлучи по електронски пат да го промени притисокот во цевките на гасоводот, со што ќе предизвика оштетување на вентилите и ќе доведе до експлозија на цели населби или предградија. Истото се однесува и на можностите за напад на електричната мрежа.

Како последица на својот напад, сајбер терористот ќе се осигура дека населението на одредена држава ќе гладува, ќе останат без вода, ќе неможе да се движат или воопшто нама да опстанат. Освен тоа, оние кои се задолжени да ја заштитуваат замјата или нацијата не се предупредени за ваков вид на напад и најчесто е неможно фаќањето и лишувањето од слобода на сајбер терооистот одговорен за нападот, бидејќи истиот постои најголема *веројатност да е на другата страна на светот. Ваквите напади не се научно-фантастични*, тие се дел до реланиот свет во кој ние живееме и преставуваат сериозен проблем на целиот систен на национална безбедност на државите, во било кој дел од денот, месецот, годината.Како што е веќе познато, некои од нив веќе се имаат и случено во одредени земји, без притоа да се обрне посебно и посериозно внимание на ваквите случувања, или пак истите да бидат квалификувани во друг вид на закана. Дали сме подготвени за вакви сценарија? [6]

[6] Collin,C.,B.,The Futur of cyber-terrorism: Where the Physical and Virtual Words Converge, 11th Annual International Symposium on Criminal Justice Issues, Institute for Security and Intelligence, превземено од: http://afgen.com/terrorism1.html

2. Определување на предметот на истражување

2.1 Теоретско определување

Брзиот развој на информатичките и комуникациските технологии, како и широката употреба на услуги обезбедени од страна на сајбер просторот [7] отвори низа прашања: ``Како безбедноста на сајбер-просторот може да се обезбеди``?,``Дали воопшто можеме да се потпреме на компјутерската сигурност, и дали компјутерите ни ја овозможуваат``?. Инфотматичката технологија и критичните инфраструктурни мрежи се меѓусебно поврзани едни со други, а со тоа може да се пристапи од било каде во светот. Денес во информацискиот светот дејствуваат широк спектар на критични инфракструктури од снабдување со вода, за транспорт, до енергија за да комуницираат технологиите и сите тие се ранливи од сајбер напади.[8] Во светот, во секој момент, на интернет се приклучени милиони и милиони корисници. Ако и само мал дел од овие индивиди, ја поседуваат соодветната обученост, вештини, експертиза, и суштински потреби за да се изведе еден деструктивен високо-технолошки-сајбер напад, ова пак би значело дека постојат илјадници па дури и десетици илјади луѓе кои поседуваат ваков капацитет. Терористичките организации, ја препознаваат важноста и неопходноста на компјутерската обученост и активно регрутираат луѓе со вакви капацитети.[9]

Од ова се наметнува и прашањето: Кои се сајбер терористите? Каде и зошто дејствуваат? Многу напори и инвестиции се направени за да се спечи класичното терористичко насилство, но сепак во современите држави, па и во државите на балканот, останува високиот степен на став од ранливост од сајбер нападите, против компјутерските мрежи,

---

[7] Под сајбер простор се подразбира `` вид на заедница `` составена од мрежа на компјутери во која елементите на класничните друштва се во форма на битови и бајти, односно простор кој ги креира компјутерските мрежи. Терминот ``сајбер простор`` јасно укажува на комплексност, континуитет на интеракција, неограничен простор, неограничување на бојот на различни услуги за постојано истражување на нешто ново и неочекување во светот на компјутерските мрежи. Сајбер просторот е термин кој го означува online светот на интернетот (компјутерската мрежа), но и дигиталниот свет воопшто.
www.bos.org.yu/cepit/idrustvo/sk/cyberkriminal.pht
http://encyclopedia.msn.com/encyclopedia 761582824/Cyberspace.html

[8] http://www.ccdcoe.org/publikations/2011proceedings/DevelopingAninternational
http://www.ccdcoe.org пристапено:11,06,2012

[9] http://www.amazon.com/Black-Ice-Invisible-Threat-Cyber-Terrorism/dp/B000OGEKXS#reader_B000OGEKXS

кои се од клучно значење за националната и економската безбедност на современите држави. За разлика од другите терористички тактики, високо-технолошкиот тероризам е безбеден од аспект на оној кој го прави тоа, а воедно и профитабилен, но сепак доста тежок за сузбивање без потребната експертиза, знаење и што е најважно во овој случај разбирање на умот на сајбер терористот. Спојувајки ја зголемената ранливост со големите порасти на нивото на насилство, зголемената обученост и едуцираност на мадите членови на терористичките организации, согледуваме дека точката на спојување на физичкиот и виртуелниот свет, примената на старите методи на тактика, спречување и борба против тероризмот се застарени и надвор од употреба.[10] При разгледување на сајбер тероризам мора да се користи еден мултидимензионален пристап, и тоа поради фактот што, доколку високо-технолошкиот тероризам се гледа единствено од преспектива на потенцијална закана за безбедноста преку употребата на сајбер оружје, тоа значи дека набљудуваме појава која не се одвива во реалниот свет, туку во виртуелниот, па отука и погрешнито заклучок дела истата не преставува закана за безбедноста. Затоа високо-технолошкиот тероризам мора да се анализира преку целосно разгледување на опсегот на сите можни сајбер напади, па дури и нивната улога на давање подршка на реалните физички напади. Високо-технолошкиот терористички напад мора да биде изанализиран не само од аспект на начинот на кој е изведен нападот, туку и од аспект на целите што се постигнуваат и ефектите од таквиот напад. Она што ја прави една земја сила, секогаш не е нејзиниот народ, нејзината војска и нејзините вредности, туку тоа се и хардверот, софтверот и финансиската инфраструктура која го подржува нејзиниот економски развој и благосостојба. Целта на современите терористички организации, е токму уништување или загрозување на економијата и економската стабилност на земјата, а со тоа и поткупување на довербата и подршката што нејзините граѓани ја положиле во институциите, и секако нивниот начин на живот. Токму следниот терористички напад би можел да биде изведен (целосно или делумно) во сјабер просторот, бидејки голем дел од економијата зависи од непреченото функционирање на овој дигитален медиум. За да се изведе конвенционален терористички напад, сличен на оној од 11 Септември 2011 година, непријателот без оглед дали се работи за странска влада или терористичка организација, би требало да обезбеди физичко присуство на лицата кои ќе бидат ангажирани за изведување на нападот во земјата кој е цел на тој терористички чин. Таквото присуство

[10] Collin, B.,The Future of Cyber-Terrorism: Where the Physical and Vitrual Worlds Converge, 11th Annual International Symposium and Intelligence. Превземено од : http://afgen.com/terrorism1.html

може да биде директно преку влез на терористите на територијата на државата, или преку користење, односно активирање на т.н заспани келии (sleep cells)[11], што подразбира обезбедување на инфраструктура, финансиски планирања, со што значајно се зголемува ризикот за откривање и фаќање на терористите. За разлика од конвенционалните напади, сајбер нападите можат да бидат изведени по пат на далечинско управување од растојание одалечено со илјадници километри, со што е намалува можноста за фаќање на напаѓачите. Идните терористи може нема да бидат волни да го жртвуваат својот живот за целите на организацијата, или ќе подлегнат на искушението да го изведат терористичкиот напад, па засолнети некаде на некое далечно и безбедно место, по пат на стабилна интернет врска ќе го извршат истото.[12] За жал, поради широко распространетото несваќање, односно неразбирање на високо-технолошкиот тероризам и модерните терористички организации, се оди кон ситуации во кои изостанува правилното и навремено дејствување, односно се останува на едно пасивно ниво. Терористите се стратешки актери... Тие промислено ги одбираат своите цели и таквиот нивен избор се заснова на слабостите и пуканатините што ќе ги воочат во нашите одбранбени ситеми, и нашата подготвеност да се браниме против широко распространетата лепеза од средства и методи за напад. Терористите продолжуваат со употребата на конвенционални оружја за напад и притоа паралено се здобиваат и ги усовршуваат експертските знаења и вештини за изведување на поинакви напади како што се сајбер нападите.[13]

2.2 Појмовно определување-категоријален апарат

Сајбер просторот

Сајбер просторот е термин кој прв го употребува Вилим Гипсон во 1984 г.(Wilim Gibson,1984) во неговиот научно фантастичен роман ``Neuromancer`` како поим за доменот кој ја опфаќа мрежната комуникација поставена на компјутерите, за што најистакнат пример е Интернет. Алтернативен опис за овој поим е ``on-line``, кој укажува на начинот на комуникација на која се пренесуваат информациите низ телефонските линии. Во речникот се дефинира како поим за околината на појавување на комуникацијата низ компјутерските мрежи. И двете дефиниции укажуваат на тоа дека сајбер просторот е

[11] http://www.globalsecurity.org/military/world/para/al-qaida-sleeper-cells.htm
[12] http://www.amazon.com/Black-Ice-Invisible-Threat-Cyber-Terrorism/dp/B000OGEKXS#reader_B000OGEKXS
[13] National Strategy for Homeland Security: The White House, July 2002 достапно на: http://www.whitehouse.gov/issise/homeland-security

илузија или постои само во теоријата. Затоа Интернетот ќе го сметаме како модел за сајбер простор. Најчесто се нарекува сајбер простор (Cyberspace) и е најголемата компјутерска мрежа. [14]

Сајбер просторо е простор односно средина во која со дигитализираните информации се комуницира преку компјутерските мрежи.[15]

Сајбер просторот е ``Интернационална компјутерска мрежа која ги снабдува со електронска пошта и информации од компјутерите, едукативните институции, владини агенции, индустријата, и ги прави достапни за целокупната јавност преку модем.``[16]

Информациско-компјутерски систем

Информациско-компјутерски систем е каков било уред или група на меѓусебно поврзани уреди од кои, еден или повеќе од нив, врши автоматска обработка на податоци според одредена програма.[17]

- Информационен систем е секоја напишана, електронска или графичка метода на комуникациски информации. Основата на информационен систем е делење или обработка на информации и идеи. Компјутерите и телекомуникациската технологија се важни компоненти на информционен систем[18].

Безбедност

Безбедност е правно уреден и обезбеден општествен однос и воспоставена општествена состојба во државата која овозможува ефективна заштита на државата и граѓаните кои во неа живеат од сите (надворешни и внатрешни), противправни акти (активности) со кои се загрозува уставниот поредок, сувереност, независност и територијалната целовитост на државата, работењето на државните органи, извршувањето на стопанските и општествените активности и остварувањето слобода, права и должности на човекот и граѓанин; [19]

---

[14] Лазарова, М., Слободата на изразувањето во сајбер просторот, превземено од http://www.ii.edu.mk/.../Слободата%20на%20изразувањето%20во%20сајбер%20просторот.pdf

[15] Joint Publication 1-02,``DOD Dictionary of Military and Related Terms``,April 2001 превземено од http://www.dtic.mil/docrtine/jel/new_pubs/jp1_02.pdf

[16] The New Dictionary of English, Oxford English Dictionary, превземено од http://www.oed.com/

[17] Камбовски, В., Кривичен Законик, Интегрален текст, Предговор, кратки објаснувања и Регистар на поими, ЈП Службен весник на Р.М, Скопје, 2009 стр.126, Чл. 122, став 26

[18]http://e-biznis.net/indeks.php?option=com_content&view=article&id=283:2009-10-16-16-12-39&catid=73:2009-10-19-20-53-47&Intemid=98

[19] Слободан Милетиќ, Појмовник полициског права-значење 650 појмова из области унутрашњих послова, Службени гласник,Београд, 2001, стр.6

Национална безбедност

Национална безбедност преставува дејност на националните држави со кои тие во согласност со своите општествени и национални можности во сегашноста и иднината земајки ги во предвид глобалните промени и развојот, го заштитуваат сопствениот идентитет, опстанокот и интересите. Националната безбедност се однесува на самостојна држава која се грижи за заштита на целокупниот физички интегритет и територијалната целокупност;

Информациска безбедност

Денес е општоприфатена дефиницијата за тоа што е информатциска безбедност т.е. општоприфатени се критериумите кои треба да се исполнат за да имаме, постоење на безбедносна информација а тоа се:

Доверливост (Confidentiality)- информацијата треба да биде креирана и користена од субјекти кои имаат право да тоа го прават;

Комплетност (Integrity)- информацијата треба да биде секојпат во нејзината изворна форма (без неовластени промени), комплетна (ништо да не е неовластено одземено) и точно;

Достапност (Accessibility)- информацијата треба да биде секојпат достапна до сите кои се овластени;

Комплетот на безбедносните критериуми имаат општо прифатени синоними - *C.I.A* Бројот на идентификувани и регистрирани прекршоци на безбедносните критериуми е во експоненцијален пораст во сите држави на светот, а особено на т.н.``многу штетни`` прекршоци (пр. деструкција на битни општествени инфракструктурни системи: комуникациски ситеми енергетски системи, транспортни системи).[20]

[20] Трајковски, Љ., Смерници за подготовка на Национална Стратегија за Информациска Безбедност на Република Македонија, Version 0.0, IT Association, MASIT, Macedonia, 2007, стр.4

Сајбер напад

Сајбер напад ги подразбира сите дејствија кои имаат за цел нарушување, блокирање, деградирање или уништување на информациите складирање во компјутери и компјутерски мрежи, или на самите компјутери и компјутерски мрежи,[21] а дел од овие напади се и:

Активизам- се однесува на нормалниот и ненасилен начин на користење на интернетот заради подржување на одредена агенда или кауза, како на пример: разгледување и листање на мрежите и конструирање на веб-сајтови, постирање на материјали и информации на истите, пренос на електронски публикации и писма преку електронска мрежа (e-mail) и користење на интернетот за дебати и дискусии, формирање на сојузи и коалиции и палнирање и координирање на активностите.[22]

Хактивизам- се однесува на единственото од хакирање[23] и активизам; на пример: употреба на техники за хакирање против одреден интернет сајт односно страница, која е земена како мета, со цел нарушување на нормалното нејзино функционирање, но нема за цел предизвикување на сериозни штета. Виртуелните блокади, автоматските е-маил ``бомби``, веб-хаковите, неовластеното навлегување во компјутериските системи, и компјутерските вируси и црви, сето тоа се примери за хактивизам.[24]

---

[21] Deparment of Defense Dictionary, превземено од http://www.dtic.mil/doctrine/je/doddict/data/c/01168.html

[22] Trends in terrorism series, Canadian Center for Intelligence and Security studies, The Norman Paterson School of International Affairs, Carleton University, Volume 2006-2, str.3

[23] Терминот ``хакер`` се однесува на луѓе кои се обвинети за сајбер криминал. Овие луѓе користат различни техники и програми за да пронајдат начин за нарушување на сигурност без значење на корисникот. Ова најчесто се случува преку користење на друг компјутер во мрежа или преку користење на еден од следниве методи: тројанци, вируси, црви, скенирање на ранливост на компјутерите во мрежа (особено оние кои се во комуникација со други компјутери), откривање на лозинка (преку таканаречените ``снифер`` програми), добивање лозинка од некого (во текот на разговорот, или едноставно преку набљудување на кориснокот кој ја внесува лозинката), превземено од http://www.ucenje.org.mk

[24] Trends in terrorism series, Canadian Center for Intelligence and Security studies, The Norman Paterson School of International Affairs, Carleton University, Volume 2006-2, str.3

Тероризам

Терминот тероризам, потекнува од латинскиот збор terrere, што значи, плаши или заплашува, односно ужас, страв и трепет, примена на застрашување, политичко насилство.[25]

Тероризам е секое умислено незаконско дејствие, опасно за човековиот живот или јавната безбедност кое има за цел застрашување или присилување на цивилното население или на влада.[26] Тероризмот преставува калкулирана употреба на насилство или закана на истото, со цел да предизвика страв, за да се заплашат или присилат влади или општества, заради постигнување на зацртаните цели кои најчесто се политички, религиозни или идеолошки.[27]

Тероризмот е метод на повторена насилна активност, потикната од вознемиреност, а извршен од страна на (полу) тајни поединечни, групни или државни актери, од криминални или политички причини, каде што за разлика од атентатот, дирекните цели на насилство, не се главни цели. Човечките жртви, обично се бираат по слободен избор (случајни цели), или по некои критериуми (репрезентативни или симболични цели) од целното население, и служат за пренесување на некаква порака.[28] Под тероризам, односно под терористички акт се подразбираат секоја организирана и поединечна, незаконска употреба на сила, изразена со примена на оружје (биолошко, хемиско, радиолошко, нуклеарно) или закана со употреба на сила, против луѓе или имот, заради принудување или заплашување, како средство за постигнивање политичка, етничка, религиозна или идеолошка цел.[29] Тероризмот е инкриминиран во Кривичниот Законик на Република Македонија, Чл.394-б, каде што, основниот облик на делото тероризам се дефинира како ``Тој што ќе изврши едно или повеќе дела на убиство, телесно повредување, грабнување на лице, уништување на јавни објекти, транспортни системи, објекти на инфраструктура, информациски системи или други објекти во општа употреба, грабнување на авиони или други средства за јавен транспорт, производство, поседување или трговија со нуклеарно оружје, биолошко, хемиско, опасни радиоактивни, отровни или други опасни супстанци, или предизвикување пожар или експлозија, уништување на постројки за снабдвање со

---

[25] Мала енциклопедија-ИП Просвета, Београд.1970, стр.94
[26] GAO Report,``Information Security: Computer Attacks at Department of Defence Pose Increasing Risks`` на www.fas.org/irp/gao/aim96084.htm.
[27] Bradly, K., A., Anatomy of Cyberterrorism: Is America Vulnerable?, Maxwell AFB, AL, February, 2003, p..6
[28]Гелке, А.,*Новата ера на тероризмот и меѓународниот политички систем*, Магор, Скопје, 2009, стр.20
[29] З. Димовски, *Тероризам*, Графотранс, Скопје, 2007, стр.10

вода, енергија и други основни природни извори, со намера загрозување на животот и телото и создавање чуство на несигурност или страв на граѓаните, ќе се казни со затвор од најмалку 10 години или доживотен затвор.``[30]

Терористичка организација

Во Кривичниот Закон на Република Македонија, во чл.394-а инкриминирано е создавањето на Терористичката организација, која гласи ``*Тој што создава група, банда или друга злосторничка организација за извршување на кривични дела: увиство, телесно повредување, грабнување на лица, уништување на јавни објекти, транспортни системи и други објекти во општа употреба, грабнивање на авиони или други средства за јавен транспорт, производство, поседување или трговија со нуклеарно оружје, биолошки, хемиски, опасни радиоактивни, отрови и други опасни супстанци, или предизвикува пожар или експлозија, уништување на постројки за снабдување со вода, енергија или други основни природни извори, со намера загрозување на животот и телото и создавање на чуство на несигурност и срав кај граѓаните, ќе се казни со казна затвор од најмалку 8 години.*[31]

Терористички цели

Од самото дефинирање на Тероризмот како поим и се она што под него се подразбира, произлегуваат и **терористичките цели** кои најчесто се произлезени или предизвикани од политички, етнички, религиозни или идеолошка природа.

Високо технолошки тероризам

Во однос на терминот *Високо-технолошки (сајбер) тероризам*, во светот не постои една општо прифатена дефиниција кој ќе може во целост да даде објаснување на самиот термин, туку различни автори различно го дефинираат.

- Сепак, како една од најцитираните дефиниции на поимот е онаа дека ``Високо-технолошкиот или уште како би се нарекол *сајбер* тероризам е конвергенција од тероризмот и сајбер просторот. Генерално земено, овде станува збор за незаконските напади или закани од напади против компјутери, мрежи и информациите скадирани во

[30]В. Камбовски, Кривичен - Законик, Интегрален текст, Предговор, Кратки објаснувања и Регистар на поими, ЈП Службен весник на Р.М,Скопје,2009 стр.312, Чл.394-б, став 1.
[31] В. Камбовски, Кривичен Законик, Интегрален текст, Предговор, Кратки објаснувања и Регистар на поими, ЈП Службен весник на Р.М, Скопје, 2009 стр.311, Чл.394-а, став 1.

истите, кои се вршат со цел застрашување или присилување на владата во одредена земја или нејзиниот народ, заради остварување на политички или општествени цели. Понатаму, за да се оквалификува нападот како високо-технолошки тероризам, истиот треба да предизвика со помош на високата технологија или комуникацијата во виртуелниот свет, насилство врз луѓето или имотот, или барем да предизвика доволно штета со тоа што ќе генерира став. Нападите кои резултираат со смрт, телесни повреди, експлозии, авионски несреќи, загадување на водата или тешки економски загуби, би биле конкретен пример``[32]

- Сајбер тероризмот е конвергенција помеѓу сајбер просторот и терористичките активности; соодветно на ова а изразено преку пример е следното: политички мотивирано хакирање, кое има за цел да предизвика сериозни штети како загуба на човечки животи или сериозни економски последици.[33]

- Високо-технолошкиот тероризам подразбира користење на компјутерски мрежи како алтки за уништување или онеспособување критични витални национални инфрастуктури (како енергија, транспорт, владини операции), или заради заплашување на влада или цивилно население.[34]

- Високо-технолошкиот тероризам е релативно нов термин и под истиот се подразбира незаконска употреба на сила или насилство врз лице или имот, со цел да се заплаши или присили одредена влада или цивилно население, поради остварување на политички или општествени цели.... преку експлоатација на информатичко-компјутерските системи.[35]

- ФБИ (Федерално истражно биро), го дефинира високо-технолошкиот-сајбер тероризам како умислени политички напади врз информациите, компјутерските системи, компјутерските програми и податоци, што резултира со насилство против цели кои не се воени, од страна на субнационални групи или такви агенти.[36]

---

[32] Dorothy E. Denning, CYBERTERRORISM Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, May, 2000 превземено од http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

[33] Trends in terrorism series, Canadian Center for Intelligence and Security studies, The Norman Peterson School of International Affairs, Carleton University, Volume 2006-2, str.3

[34] Lewis, A., J., Assessing the risks of Cyber Terrorism, Cyber War and Other Cyber Threats, Center for Strategic and International Studies, Washington DC, December, 2002, str.1

[35] ``Overview of Cyber-Terrorism- превземено од http://www.cybercrimes.net/Terrorism/overview/page1.html

[36] Pollitt. M., M., ``A Cyberterrorism Fact of Fancy?`` Proceedings of the 20th National Information Systems Security Conference, 1997, str. 285-289, како и The Terrorism research center http://www.terrorism.com , исто види http://searchsecurity.techtarget.com/sDefinition/0..sid

Недоволно правна регулатива

- Освен конвенцијата за компјутерски криминал од 2001година, донесена од страна на Советот на Европа и нејзините допоплнителни протоколи за криминалните акти, од расистичка и ксенофобична природа, кои беа ратификувани во 2004 година [37], во Зконодавството во Република Македонија не постои законска рамка, односно останува неинкриминирано кривичното дело Високо-технолошки или поточно сајбер тероризам.

2.3 Операционално определување

Предметот на истражување ќе биде операционализиран преку следниви димензии:

- Анализа на досегашните случаи на високо-технолошкиот тероризам во светот и начините на (не) времена реакција на соодветните структури.

- Дефинирање на сајбер нападите како облик на криминал и тероризам, и нивната поврзаност.

- Дефинирање на поимот високо-технолошкиот тероризам по пат на приказ на теоретско-методолошките пристапи кон сваќањето на високо-технолошкиот тероризам како реална закана за националната безбедност на современите држави.

- Анализа на соодветните компоненти на моделот, со цел да се добијат одговори на основните прашања: кои, каде, како, што, зошто и кога?

- Проценка на високо-технолошките-сајбер терористичките можности во светот, преку модел на проценка кој се базира на неколку фактори: постоење, можности, намери, историја (монато) и цели.

- Конструирање на модел, кој ја опишува анатомијата на високо-технолошкиот тероризам.

- Утврдување на врската помеѓу високо-технолошките нападите, т.е. обичниот високо-технолошки криминал и тероризмот по пат на споредување на матриците на истите во однос на: сторители, место, дејствие, цели, средства, здружување, мотивации и техники.

[37] http://www.pravo.org

- Високо-технолошкиот тероризам како реално очекувана закана по безбедноста во сајбер просторот во светот како и во Република Македонија и потребата да се унапреди безбедноста во сајбер просторот со цел поуспешна одбрана од новиот облик на тероризам.

- Преку разбирање на наведените основни столбови, да се осознае суштината на високо-технолошкиот тероризам.

- Примена на таквиот модел, за проценка на можните сајбер терористички закани од страна на терористичката организација Ал Каеда.

2.4 Дисциплинарно определување

Предметот на истражување е мултидисциплинарен, што ќе рече дека истиот треба да биде опфатен од акпект на повеќе научни дисциплини. Имено ќе бидат искористени веќе проверени научни сознанија, значајни за оваа проблематика од областа на безбедносните науки, криминологијата, криминалистичката и кривичното право, и секако од областа на информатичките науки.

3. Цели на истражувањето

Не можеме доволно добро да ја разбереме суштината и опасноста од дејствувањето на високо-технолошкиот тероризам како и начинот и методите со кои треба да одговори нападнатата држава, се со цел обезбедување на мир, безбедност и благосостојба, всушност да ги заштити своите витални вредности, односно да го зачува системот на национална безбедност, доколку не се откријат причините и појавните облици на високо-технолошкиот тероризам, на национално, регионално и меѓународно ниво. Конкретно, истражуавњето има за цел да даде придонес во објаснувањето на едно од поновите безбедносни закани на современите држави, како и на меѓународната соработка на државите во спречувањето на оној вид закана. Истаражувањето за значењето на меѓународната соработка во спречувањето на сајбер тероризмот има основна, научна, општествена цел и практична цел.

Основна цел на ова истражување е добивање на сознанија за високо-технолошкиот тероризам и неговите носители-актери, како најопасен вид на општествено недозволено и криминално однесување со несогледливи негативни последици на современите држави.

Научан цел на ова истражување е да се изврши научна дискрипција и научно објаснување на феноменот ``високо-технолошкиот тероризам``, како и научно објаснување

на методите и облиците на спротиставување на заканите и опасностите кои можат да бидат предизвикани од ваквиот вид на тероризам.

Практична цел на ова истражување е обезбедување на основни сознанија со кои може реално да се согледа и процени состојбата со високо-технолошкиот тероризам, да се процени улогата и значењето на меѓународната соработка во спречување на овој вид закана, со што ќе се овозможи навремена изградба на соодветна политика за негово спречување, со што ќе може да се заштити целиот систем на национлан безбедност на државата. Изградбата на ваквата политика е потребна, првенствено од аспект да влијае во спречувањето на условите за појава и развој на ваквиот вид на теоризам, или да создаде соодветни услови за репресивна реакција на државата за негово спречуавње.

Врз основа на поставените цели ќе произлезат следниве задачи:

- Да се согледаат основните видови и облици на овој нов облик на закана;

- Да се согледаат фактите за појава на високо-технолошкиот тероризам;

- Да се согледа општествено-политичките, економските, социјалните и другите фактори кои придонесуваат за можните закани од високо-технолошкиот тероризам;

- Да се дојде до сознание дали успешното спречуавње на овој вид на тероризам ќе придонесе кон јакнење на националната безбедност на регионално и меѓународно ниво.

- Да се согледа и нивото на меѓународна соработка и потреба од нејзино продлабочување, со цел постигнување на успешни резултати на полето на спречување на високо-технолошкиот тероризам;

- Да се согледа ниво на соработка и кординација со цивилното општество и неговите придонеси во спречување и откривање на високо-технолошкиот тероризам;

- Да се согледа нивото на едукација, квалитетот и стручноста на професионалците од безбедносниот сектор.

4. **Хипотетичка рамка**

Врз основа на поставените цели на истражуавњето би ја поставиле следнава општа хипотеза:

Општа хипотеза

Високо-технолошкиот тероризам е современ облик на тероризам и современ облик на закана која има големо влијание врз националната безбедност на современите држави.

Посебни хипотези

- За развојот и влијаните на високо-технолошкиот тероризам голема улога има големиот напредок на информациските и комуникациските технологии;

- За разлика од веќе добро познатите терористички методи, високо-технолошкиот тероризам е безбеден и профитабилен и секако тежок за сузбивање;

- Поаѓајки од неговата природа, на многу начини, сјабер просторот т.е. интернетот е идеалната арена за активностите на терористичките организации.

- Се поголемата достапност и застапеност на современите технички средства со кои може да се изврши упад во мрежите или инфомрациските системи на инфраструктурите од витално значење;

- Основните начини на користење на компјутерите каде се јавуваат како објект на напад т.е средство за извршување, прикривање и раководење, а пред се како алатка преку која се врши измама, регрутирање и финансирање ја показува тесната поврзаност со криминалните активности;

- Неовластеното навлегување и добивање на пристап до одреден информационен систем, а со тоа и можност на модифицирање, фабрикување, пресретнување и прекинување на податоци и информации е потенцијалана закана за националната безбедност на современите држави;

- Ефикасното спречување на високо-технолошкиот тероризам во голема мера е детерминиран и од целосната поставеност на државите и нејзините институции.

- Отсуството на стратегија за борба против високо-технолошкиот тероризам влијае врз идните можни такви сценарија.

4.1 Варијабли

Независна варијабла:

- Високо-технолошкиот тероризам е конвергенција помеѓу сајбер просторот и терористичките активности; соодветно на ова а изразено преку пример е следното: политички мотивирано хакирање, кое има за цел да предизвика сериозни штети како загуба на човечки животи или сериозни економски последици.[38]

- Отука високо-технолошкиот тероризам е конвергенција од тероризмот и сајбер просторот. Генерално земено, овде станува збор за незаконските напади или закани од напади против компјутери, мрежи и информациите скадирани во истите, кои се вршат со цел застрашување или присилување на владата во одредена земја или нејзиниот народ, заради остварување на политички или општествени цели. Понатаму, за да се оквалификува нападот како високо-технолошки тероризам, истиот треба да предизвика со помош на високата технологија или комуникацијата во виртуелниот свет, насилство врз луѓето или имотот, или барем да предизвика доволно штета со тоа што ќе генерира став. Нападите кои резултираат со смрт, телесни повреди, експлозии, авионски несреќи, загадување на водата или тешки економски загуби, би биле конкретен пример``[39]

Како независна варијабла во овој труд се јавува комплексноста на високо-технолошкиот тероризам и неговата се поголема застапеност преку развојот на новите технологии во современите држави ;

Зависна варијабла:

Националната безбедност преставува дејност на националните држави со кои тие во согласност со своите општествени и национални можности го заштитуваат сопствениот идентитет, опстанок и интересите, т.е целокупниот физички интегритет и територијално целокупност;

---

[38] Trends in terrorism series, Canadian Center for Intelligence and Security studies, The Norman Peterson School of International Affairs, Carleton University,Volume 2006-2, str.3

[39] Dorothy E. Denning, CYBERTERRORISM Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, May, 2000 превземено од http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

Кога говориме за безбедноста на државата тоа преставува правно уреден и обезбеден општествен однос во државата во која се овозможува заштита на самата држава и нејзините граѓани, па отука анализирањето на сајбер терористичките методите и техники се од големо знаење за понатамошниот опстанок на државата и нејзината национална безбедност;

Како зависна варијабла во овој труд се јавува се позачестените упади во компјутерските системи на современите држави и рушење на нивната национална безбедност преку разни методи и техники;

5. Методи на истражување

Согласно веќе поставените хипотетичка рамка, предметот и целта на истражувањето беа применети следниве истажувачки постапки:

Дискриптивен метод- ќе се користи за детално да се опише високо-технолошкиот тероризам;

Компаративен метод- ќе се користи во сите сличаи кога ќе биде потребно да се споредуваат податоци од неопределен број случаеви или истите извори на информации со цел да се добијат релевантни податоци на истражувањето;

Анализа на содржина- ќе се користи анализа на соодветни текстови, книги, анализа на научни трудови како и документи релевантни за дефинирање на поимот високо-технолошкиот тероризам со кој би се дошло до податоци за состојбата на системите за информациска безбедност и безбедносните закани. (сепак овде станува збор само за информации од јавен карактер)

* стручна литература која ја третира конкретната проблематика и се однесува на високо-технолошкиот тероризам објавени во мас-медиумите, списанијата и др. публикации (книги,брошури, публикации)

* материјали кои произлегуваат од интернет страни и од низа други достапни истражувања спроведени во оваа област (веб страни, форуми и сл.)

6. Општествена и научна оправданост за истражувањето

Кога историчарите ќе ја истражуваат втората половина на дваесет и првиот век сигурно ќе биде дека тие го проучуваат периодот на информатичката револуција. Бидејќи човештвото во последниве педесет години доста има напреднато како никогаш досега, па затоа поголем е бројот на предизвици за борба против некои штетни влијанија кои можат драстично да им го променат или уништат животот. Еден од таквите предизвици е борбата со феноменот на еден нов модел на тероризам во светот, познат како високо-технолошки тероризам. Високо-технолошките терористичките напади не само што се зголемуваат по бројност, туку она што загрижува е нивната се поголема софистицираност и организираност.

Па отука, со помош на овој труд, се надевам дека ќе направам еден мал чекор кон јасно дефинирање на високо-технолошкиот тероризам, неговите методи, потенцијали, опасности како и предлозите за соодветен пристап кон намалување на опасностите од него.Одтука произлегува и потребата да се укаже на сериозноста која со себе ја носи заканата, па очекувам дека преку елаборирање на самите случувања и веќе наведените дефиниции ќе укажам на незаштитеноста на информатичкиот систем од една и софистицираноста на терористичките организации во светот од друга страна, што ќе продуцира превзенање на контра мерки за измена на постојната правна регулатива и инкриминирање на делото во Кривичниот закон на Република Македонија. Трудот ќе понуди и материјал за понатамошна анализа од стана на научната јавност која се занимава со конкретната проблематика, со цел навремено да се превземат сите соодветни мерки и активности за поголема и поактива ангажираност на државните институции и секако нивна поголема меѓународна соработка.

Она на што се надевам и очекувам е дека со помош на т.н модел за спознавање на суштината на тероризмот исто така ќе понудам сознанија преку кои успешно ќе биде разбран светот на високо-технолошкиот тероризам, како нова димензија на закана и војување, а воедно и на одереден начин ќе ги потикнам идните истражувачи и аналитичари за понатамошни, подлабоки и поголеми методолошки зафати во оваа област, за да не остане нешто неразјаснето, па отука овој вид на тероризам „ високо-технолошкиот тероризам„ да ги искористи тие слабости, па да земе поголеми размери во иднина.

Втора глава

1. Безбедност

Во науката и литературата, државата е дефинирана како посебна општествена творба, и како таква сама по себе преставува најважен облик на политичко организирање во едно општество. Државите ги дефинираат своите витални вредности и интереси кои ги истакнуваат како приоритетни и кон кои ги насочуваат безбедносните активности, стремејќи се кон нивна заштита. Ваквата заштитна на овие витални вредности секогаш е условена од карактерот на општеството, т.е од економските односи, од степенот на развој на производните сили, од односот на општествените класи и правната и политичката надградба. На нивното зачувување, развивање и заштита им се посветува особено внимание, бидејќи со нивниот опстанок, државите го остваруваат и својот опстанок и развој. Секое загрозување на тие вредности, дали тоа да се поединечни или групни, преставуваат истовремено и загрозување на државата, нејзината стабилност и суверенитет.[40] Бидејќи, основан цел на секоја државна политика е опстанокот на државата и нејзиното општество, отука, согласно ова, целта на дејствувањето на сите државни институции е насочена кон остварување и кон зачувување на нејзината безбедност. Ваквата поставеност на институциите преставува рамка на безбедносната политика, која има за цел создавање на услови за остварување на внатрешната и надворешната безбедност на државата.

Безбедноста е еден од феномените на човековото општество и како повеќеслојна појава таа е во сите фази на неговиот развој. Безбедноста во современите држави се манифестира преку неколку облици како социјален безбедност, како здравствена заштита, како сообраќајна безбедност, како заштита на животната средина. Но, во ниеден случај не смеат да се занемарат и основните права на слободно изразување на политичките и верските ставови, право на заштита од прогон од структурите на државата заради разликите во мислењето и изразувањето на личните ставови, секако правото за остварување на сопствен начин на живеење на граѓаните од границите кога со нивното однесување нема да ги загрозуваат правата и безбедноста на другите.

Безбедноста како функција е неразделен атрибут на секоја држава. За безбедносната функција на државата може да зборуваме како за услужна функција, од причини што таа и ја пружа „ услугата„- безбедноста на заедницата внатре во државата. Безбедносната функција на секоја држава има два облика на делување: *превентивен облик,* во секоја ситуација кога државата со своето постоење и правовремено ангажирање преставува инструмент за одвраќање од сите облици на загрозување и *репресивен облик,* со отстранување на причините на опасноста и со елиминирање на нивните носители по пат на примена на сила на правно дозволен начин.[41] Одговорноста на државата за безбедноста на нејзините граѓани е неделива, непрекината и независна од политичките, од социјалните и до другите случувања, бидејќи во спротивно, може да дојде до дезорганизација на системот, од задоволување на политичко-партиските, групните или поединечните интереси и од деструкција која

[40] Стајић Љ. Гилановић Ч.-*"Основи безбедности"*, Полициска академија у Београду, Београд 1994.
[41] М. Котовчевски.- *"Националана безбедност"*, Филозофски факултет, Скопје, 2011.

првенствено и најтешко го погодуваат ``обичниот граѓанин``. Безбедносната функција понекогаш може да се идентификува и како принудна фунција на самата држава, особено во спречување на екстремни општествени девијации, се со цел, зачувување на нејзините витални вредности- суверенитетот, територијалниот интегритет и независноста.[42] Безбедноста на држават како референтен објект, но и како субјект на меѓународната заедница, вклучувајќи ги и нејзините витални интереси, се загрозени од повеќе надворешни и внатрешни чинители кои се водени од различни мотиви. Безбедноста, пак како атрибут на секоја држва не преставува само безбедност од војна, туку таа преставува и безбедност на поединците, па отука и прашањето на/за безбедноста секогаш треба да се постави двострано. Имено, тоа би значело дали некој не загрозува нас и на кој начин го врши тоа, и секако, дали ние, пак, со своите постапки можеме да загрозиме некој друг.

Ниту едно општество не може да оствари безбедност во голем степен, ниту пак апсолутна слобода, од причини што за тоа е потребно да се обезбеди рамнотежа помеѓу безбедност и заштитата на основните права и слободи на граѓаните и интереите на државата, па затоа неопходно е слободата и безбедноста да бидат сфатени како варијабилни величини.[43]

Универзалните видови на системот на безбедност во современите држави се познати како: *државна, јавна и воена безбедност.* Според објектот на заштита постојат *пет* видови безбедност и тоа: *државна, јавна, колективна, лишна и имотна.*[44] Со оглед на фактот дека безбедносните појави функционираат по принципот на сврзани садови, денес е невозможно безбедноста да се лоцира и да се практикува само во една земја, само за една група граѓани, или само за еден поединец, туку напротив - безбедноста треба да се разбере како индивидуална, национална и меѓународна безбедност.

Безбедносната политика не е создадена и не секогаш се базира само врз сфаќањето за и околу приоритетите и потребите на нациналната безбедност, туку на истата влијаат и низа надворешни чинители, притисоци и обврски кои произлегуваат од тоа. Таа е многу потесна од општат концепција, а многу поширока од уставно – правната конципција на безбедноста. Согласно политиката која ја гради Република Македонија во сферата на безбедноста, под поимот безбедност подразбираме: одредена достигната или проектирана состојба на безбедноста и преставува функционално подрачје на дејствување на различни безбедносни институции заедно со вкупните општествени настојувања на полето на постигнување на безбедносните цели и, на крајот, безбедноста ги опфаќа сите безбедносни институции поврзани во определен систем на односи.[45]

---

[42] Jaganjac J. –" *Sigurnost u sistemu znatnosti",*Odjek, Sarajevo, 2009.
[43] Masleš R. – " *Teorije i sistemi sigurnosti",* Magistrat, Sarajevo, 2001
[44] Поопширно во книгата на М. Котовчевски–*''Национална безбедност",* Филозофски факултет Скопје, 2011год.
[45] Бакрески О. –*"Контрола на безбедносниот сектор"*,Филозофски Факултет – Скопје, 2008

1.1. Терминолошко определување на безбедноста

Безбедноста како поим има повеќе значења од причини што истата преставува многу сложен и комплексен општествен феномен. Во стручната литература ваквото определување оди во насока на тоа како да се ослободиме од страв, ослободување на различни закани или, пак, ослободување од класични физички и психички насилства или злоупотреби. Така, според ваквото определување, терминот безбедност подразбира и ги вклучува моралните, идеолошките и нормативните елементи, што во голема мера го отежнува неговото дефинирање. Безбедноста како поим во теоријата, практиката и во доктрината, се користи за да се одбележат или да се именуваат со него разновидни елементи или односи. Во современите држави, безбедноста претставува глобален предизвик и еден од главните мотиви за човековите и општествените активности.

Етимолошки гледано, поимот за безбедноста некои теоретичари и научници го поврзуваат со латинскиот збор „securitas–atis," што значи сигурен, постојан, автентичен, константен, верен и сл., додека други – поимот за безбедноста го поврзуваат со латинскиот збор „sinecure" што значи да се живее „без грижа". Терминот „без грижа" е еластичен од една причина што „грижата" некогаш може да биде продуцирана од силен страв, а некогаш и од сосема мала фрустрација или безначаен настан. За поимот безбедност, во англискиот јазик се користат два изрази и тоа: „security" и „safety". Изразот „security" најчесто се користи за објаснување на поимот национална безбедност, што од своја страна имплицира заштита и чување на државниот или на националниот интерес. Наспроти ова, пак, изразот „safety", има значење за превентивно дејствување за да не дојде до несакана безбедносна ситуација.

Поимот безбедност, се до неодамна означувал разгледување и разрешување на определен проблем кој бил настанат како резултат од воени причини, а денес опфаќа лепеза од различни аспекти на човековото општествено живеење, творење и дејствување. Своето влијание безбедноста, без разлика дали станува збор за национална безбедност или индивидуална безбедност, го има не само во воените, туку и во економските, политичките, социолошките, еколошките, културолошките, образовните, здравствените и други аспекти на современото живеење.[46]

Според Котовчевски, воените, политичките, економските, социјалните и еколошките сфери ќе ги претставуваат петте витални подрачја на безбедноста на современите општества, но и на глобалната безбедност во иднина.[47]

Поимот безбедност е повеќезначаен во теоријата и во практиката и се користи за да се означат разновидни елементи и односи.[48] Во теоријата постојат различни мислења и

---

[46] Buzan B.-"Peoples, States and Fear: An Agenda for International Security Studies in the Post Cold War Era" London, 1991.

[47] Котовчевски М.- *„Национална безбедност"*, Филозофски Факултет, Скопје, 2011.

[48] Гоцевски Т., Бакрески О., Славески С., Георгиева Л.- *„Интересите на Република Македонија во градењето на европската безбедност"*, МАНУ – Центар за стратегиски истражувања, Филозофски факултет, Скопје, 2008.

толкувања на поимот безбедност, поради што нејзиното определување е многу сложено. Денес, безбедноста преставува феномен кој е комплексен и повеќе димензионален. Таа преставува определена состојба на заштита на основните вредности на државата, односно активности за заштита на тие вредности, соодветна организација, функција, систем или сето тоа заедно. Ваквото определување е пред се условено и зависи од аголот на набљудување, а тоа укажува на тоа дали поимот безбедност се врзува за заштитната функција на државите за одредени дејствија и активности, за политичките и за сличните гледишта на нив.

Котовчевски ја дефинира безбедноста како состојба во која е осигуран, урамнотежен физичкиот, духовниот и материјален опстанок на поединецот и на општествената заедница во однос кон другите поединци, општествени заедници и природата, или безбедноста во суштина преставува иманентен структурен дел на општеството што во себе вклучува определена состојба, односно определени особини на состојбата, а исто така и дејност, односно систем.[49]

Според, Архолд Волферс, безбедноста може да се дефинира како отсуство на закани кон усвоените вредности, а според Дејвид Болдвин, како мала веројатност за нанесување штети врз тие усвоени вредности.[50]

Маслеша смета дека безбедноста е основната цел на секое современо општество, без која нема опстанок на истото, па безбедноста како поим се употребува во скоро сите области на живот и на работа. Отука и сите настојувања се движат во правец за воспоставување на релевантна рамнотежа помеѓу човекот и безбедноста.[51]

Согласно дефиницијата на ООН од 1985 година, безбедноста преставува состојба во која државите сметаат дека нема опасност од воен напад, политички принуди или економски присили, така што истите ќе можат слободно да се развиваат.

Безбедноста во најширока смисла преставува состојба на стабилност во природата и во државата која е насочена кон вршење на превентивни подготовки за одбрана и заштита, пред се од различните извори на загрозување, за да не предизвика нерамнотежа во природата и во општеството, со што би се загрозил физичкиот, општествениот и духовниот интегритет на поединците.[52]

Со зголемувањето на интересот за невоените закани, дојде до промена на вредностите кои се опфатени со поимот за безбедноста. Традиционалниот концепт за безбедноста, во центарот на внимание секогаш ја наведува заштитата на националната држава и нејзините основни атрибути на суверенота првенствено со воени средства, а новиот концепт, или т.н концепт на човекова безбедност не го оспорува значењето на националната држава, туку ја нагласува важноста од заштита на луѓето, нивните

---

[49] Котовчевски М. – "*Национална безбедност на Република Македонија*,, (прв дел), Македонска цивилизација, Скопје, 2000

[50] Baldwin D. - „*The Concept of Security", Review of International Studies, Vol.*23,1997.

[51] Masleša R.-" Teorije i sistemi sigurnosti" , Magistrat, Sarajevo, стр. 2001год.

[52] Нацев З. Начевски Р. - „Безбедноста и националната одбрана, ,- Македонска ризница, Куманово, 2001год.

заедници и животната средина, како подеднакво важни. Од ова произлегува дека денес безбедноста се фокусира кон новите предизвици, а тоа се заканите насочени кон човечките животи. Безбедносните закани не секогаш доаѓаат само од другите држави, туку тие настануваат и од големиот број природни и општествени процеси и појави кои ги минуваат националните граници.

Хорхе Неф ја утврдил човековата безбедност како систем составен од *пет* меѓусебно поврзани подсистеми - животна средина, стопанство, општеството, политичките заедници и културата. Според Џорџ Меклин, човековата безбедност ја опфаќа безбедноста на поединците во непосредното опкружување, заедницата и животната средина, како и безбедноста од кршење на основните човекови и колективни права, од епидемии, насилство, принудна миграција на населението, политичка корупција, криминал, тероризам, прекумерно користење на природните ресурси и загадувањето.[53]

Безбедноста на луѓето мора да биде поприоритетна од безбедноста на државата, од логични причини, зошто каква би била безбедноста на државата ако нејзините граѓани би се чуствувале небезбедно.

За првпат индивидуалната безбедност (human security) се споменува во 1994 година во ООН, во рамки на УНДП Програмата за развој (UNDP-United Nations Development Programme), каде се наложува потребата од пронаоѓање нов концепт за безбедност на поединецот и државата. Според комисијата за човекова безбедност (Commission on Human Security) постојат *две* причини за развојот на концептот за индивидуалната безбедност и тоа *првата* се однесува на неможноста на државата секогаш да обезбеди безбедност на граѓаните, а *втората* причина укажува на тоа дека државите понекогаш преставуваат закана за своите граѓани. Таа е во согласност со концептот на национална безбедност и за човекови права, што е содржана во дефиницијата на ООН дека индивидуалната безбедност преставува безбедност од закани како што се глад, болест и репресија, како и заштита од неочекувани и од опасни прекини со секојдневниот живот.[54]

Националната безбедност е функција на секоја држава и таа во основа треба да одговори на сите безбедносни предизвици и ризици и да обезбеди слобода на граѓаните, заштита на човековите права и слободи, непречено функционирање на државата и општеството во целина, заштита на суверенитетот и територијалниот интегритет во рамки на меѓународните ангажмани прифатени од државата, стабилен економски развој, функционирање на правната држава, заштита на државниот и на имотот на граѓаните.

Националната безбедност сфатена како состојба на безбедност на определен народ, односно нација, е изразена во рамките на различните потенцијални и вистински

---

[53] King G. and Murray C. – *"Rethinking Human Security"*, Politicak Science Quarterly, Vol.116, No.4,2001-2

[54] UNDP – "Human Development Report" New York: Oxford University Press (online) достапно на: http://hdr.undp.org/en/media/hdr_1994_en_contents.pdf.

небезбедности, кои произлегуваат од меѓународното „непријателското„ опкружување. Загрозувањето кое доаѓа однадвор се подразбира како функција на дел од претпоставени и дел на вистински услови. Вистинската разлика помеѓу претпоставените и вистинските услови на загрозување е неможна да се утврди.[55]

Националната безбедност во современи услови е многу комплексна појава која е потребно да се истражува, имајќи ги предвид следниве фактори: систем на одлучување во областа на безбедноста; меѓународна, геостратегиска и воено-политичка положба на државата; историски искуства; големина и облик на државата; права и должности на државата кои произлегуваат од нејзината положба во меѓународната заедница; степен на нејзиниот стопански и општествен развој; карактеристики на нејзиниот систем на национална безбедност; големината на финансиските средства наменети за националната безбедност; вилјанието на јавното мислење и сл.[56]

Во почетоците кога за првпат беше определено терминолошкото значење на националната безбедност таа во себе ги опфаќаше следниве дефинирања како отсуство на каков било страв од напад, од загрозување на интересите или од закани од друга држава или држави. Развојот на случувањата во светот доведе до тоа сите проблеми во меѓународното опкружување да стануваат и потенцијални проблеми за државата, а со самото тоа и за нејзината национална безбедност. Кон крајот на осумдесетите годнини од минатиот век, воената компонента во дефинирањето на поимот национална безбедност го губи своето важно место, со што безбедноста или поимот за безбедноста се повеќе ги вклучуваше другите сегменти на државата и на општеството. Така сега националната безбедност подразбира: определена состојба на безбедноста како функционална подрачје на дејствување на различни безбедносни институции заедно со вкупните општествени заложби насочени кон постигнување на националните цели и интересите на тие безбедносни институции, кои се наоѓаат во системска симбиоза. Националната безбедност треба да создаде состојба во која ќе бидат обезбедени: слободата на државата и општеството, територијалниот интегритет и суверенитет на државата во рамки на меѓународно прифатените норми, политичката и социјалната стабилност, стабилниот економски и стопански развој, функционирањето на правната држава, стабилниот јавен поредок, личната сигурност и слобода и права на луѓето, како и здравите и стабилни еколошки услови.[57]

За националната безбедност Котовчевски вели дека таа е безбедност која се однесува на општеството/државата во која се инкорпорирани внатрешната и надворешната безбедност.[58]

Така, современата национална безбедност во современите држави со напреднат индустриски развој е политичко и приватно добро што се реализира како основно човеково право.

---

[55] Tatalović S. Griyold A. Cvrtila V. – *"Suvremene sigurnosne politike",* Zagreb, 2008
[56] Исто.
[57] Tatalović S. Bilandiž M. – "*Osnove nacionalne sigurnosti",* MUP R., Hrvatske, Zagrb, 2005.
[58] Проширено во книгата на Котовчевски М.- *„Национална безбедност„* Филозофски Факултет Скопје, 2011год.

2. Извори и облици на загрозување на националната безбедноста

Националниот систем за безбедност, во сите современи држави се состои од две главни елементи и тоа: национална безбедносна политика и националните безбедносни структури кои ја гарантираат безбедноста на сите членови на општеството. Националната безбедносна структура е конципирана да го обезбедува општеството како целина, во суштина е различен во секоја држава, па отука, без оглед на тоа на кој начин и со која цел се организирани, системите на безбедност, преставуваат облик на организирање на општеството за заштита на наговите витални вредности.

Кога говориме за обликот на организирање секогаш поаѓаме од две основни прашања: од кого и од што треба да се штити државата и на кој начин треба да се изврши насочувањето на елементите на системот на безбедност за да се оствари основната цел – безбедноста на државата. Одговорите на овие прашања преставуваат основа за сите превземени мерки и активности во безбедносна смисла, бидејќи преку нив се врши дефинирање, калсифицирање и објаснување на појавата, на времетраењето и на дејствувањето на општествено штетните и опасни појави во одбрамбено – заштитна смисла. Ова пред се, се мисли на поседувањето знаења за разните облици и извори на општествените судири, деструктивни дејствија, како и за сите општествени, природни и технички појави кои ги загрозуваат државите. Појавите на загрозување на виталните интереси на држвите се јавуваат истовремено со нивното создавање, најнапред загрозувајќи го нивниот опстанок, а подоцна и преку загрозувањето на општествено-економскиот и културен развој.

Денес, под поимот загрозување се подразбираат општествените појави или однесувања настанати со дејствување на човекот, природата или техничките системи во подолг временски период и во поголем обем, при што може да предизвикаат штетни последици по суверенитетот и интегритетот на државата и нејзините институции.

Во кривично-правна смисла, загрозувањето преставува опасност, додека во социолошка смисла појавите на загрозувањето се поврзуваат со општествените судири и со општествено опасните однесувања, кои како такви можат однапред да се предвидат.

Согласно ова, загрозувањето преставува секој вид општествена, природна и техничка опасност од голем обем со која во голема мера се загрозува интегритетот, слободата, имотот и здравјето на луѓето, како и територијалниот интегритет и суверенитет, уставниот поредок и правото на државата, нацијата или општествените групи и поединци.[59]

Во врска со поимот загрозување, неопходно се јавува и потребата за разгедување на изворите и облиците на загрозувањето на националната безбедност, за да можеме да дадеме и одговор на прашањето кое само по себе се наметнува кога станува збор за загрозување на безбедноста на современите држави, а се мисли на тоа кои се општествените вредности кои се предмет на заштита.

---

[59] Проширено во книгата на Котовчевски М.- „*Национална безбедност*„ Филозофски Факултет Скопје, 2011год.

2.1. Извори на загрозување на националната безбедност

Денес, сите современи држави, стравуваат од загрозување на нејзините витални вредности, така што, на тој начин им се загрозува и нивната национална безбедност. Современите теоретичари го третираат поимот на загрозувањето како резултат на одредени општествени појави кои зависат од многу фактори, а таквата зависност се манифестира на повеќе начини, како на пример, она што за една држава може да биде појава на загрозување, за друга пак таквото загрозување не мора да преставува потенцијал на нарушена безбедност, или пак, неограничената слобода за еден човек може да биде ограничување, или неограничување на таквата слобода за друг итн. Секојдневните, а и многу бројни појави на загрозување кои го следат развојот на секоја современа држава/општество, како одговор имаат создавање на соодветен заштитен систем во вид на организиран национален систем за безбедност. Ваквите негативни појави на загрозување и покрај превземените мерки сепак се чуствуваат и не секогаш се под контрола на државните институции задолжени за нивното препознавање, спречување и елиминирање.

Изворите на загрозување може да бидат константни во однос на врметраењето на појавите на загрозување, а во зависност од прифатените критериуми, можат да се класифицираат како општествени, природни и загрозувања од техничко-технолошка природа.[60]

ООН во рамки на УНДП Програмата за развој (UNDP-United Nations Development Programme) во 1994 година, деференцираа листа од седум извори на небезбедност и тоа:

1. Економска небезбедност, која се огледа преку заканите од невработеност, несигурност на работното место, лоши услови за работа, нееднаквости во поглед на приходите, инфлација, слаба мрежа на социјално осигурување и немање покрив над главата (бездомништвото);
2. Небезбедност во поглед на храната, се однесува на пробленте кои се однесуваат на физичкиот и на економскио пристап кон храната;
3. Здравствена небезбедност, се однесува на заканите по животот и здравјето на луѓето, заради инфективните и паразитските болести, ХИВ и други видови вируси, болести предизвикани од загадениот воздух и водата, како и од неадекватната можност за приод до здравствените служби;
4. Небезбедност во поглед на животната средина, се огледа преку деградација на локалните и глобалните еко-системи, недостигот на вода за пиење, поплавите и другите катастрофи, нерационалната сеча на шумите, како и загадувањето на водата, воздухот и почвата;
5. Лична небезбедност, е карактеристична за заканите со физичко насилство од страна на државата, од криминалните структури, или внатре во семејството, на работното место, како и закани предизвикани од сообраќајни и индустриски несреќи;

---

[60] Стајић Љ. Гилановић Ч. *"'Основи безбедности"*, Полициска академија у Београду, Београд, 1994 год.

6. Небезбедност на заедницата, предизвикана од закани од етнички тензии и насилни судири;

7. Политичка небезбедност, предизвикана од закани државна репресија и од оние субјекти кои ги загрозуваат човековите права;

Позачестеното постоење на се повеќе групи на извори на загрозување предизвикува проблем во нивното разграничување и објаснување од причини што еден облик на загрозување може да води потекло од повеќе извори, а и загрозувањето може да биде со различен интензитет.

Вака веќе споменатите извори на загрозување на националната безбедност, на глобално ниво егзистираат и глобалните закани кои ги загрозуваат глобално егзистенцијалните и есенцијално виталните функции на меѓународната заедница. Глобалните закани ја загрозуваат глобалната безбедност, но, исто така тие индирекно влијаат, т.е преставуваат сериозна закана и за националната безбедност на современите држави во меѓународната заедница. Глобалните закани преставуваат збир на факти, околности, последици и појави кои продуцираат значајно влијание на глобалната безбедност, односно ја детерминираат глобалната безбедност.[61]

2.2. Облици на загрозување на националната безбедност

Ниту една држава денес не е имуна од загрозување на нејзината безбедност кои повеќе или помалку се појавуваат во разни облици, кои доаѓаат однатре и чии основни елементи и носители на загрозувањата се наоѓаат во самата држава или надворешни, кои се организирани и насочени однадвор. Овие загрозувања во случај да не бидат елиминирани или доведени на најниско ниво, се до одреден степен на безбедност, каде не би преставувале сериозен проблем за државата, во голема мера го доведуваат во прашање развојот и самиот опстанок на државата.

Според проф.Д-р.М. Котовчевски, облиците на загрозување на националната безбедност може да се поделат и според начинот на нивното остварување, односно дали се користат или не се користат вооружените сили за остварување на поставените цели. Според него, постојат вооружени облици кои користат исклучиво воена сила и невооружени облици кои не вклучуваат воена сила за остварување на слични, а во некои случаи и исто поставени цели.[62]

Причините кои го предизвикуваат постоењето на загрозувањата ги наоѓаме во меѓународната и во геополитичката положба на државите, во територијалните аспирации на соседите, во внатрешната нестабилност, во неразвиеноста на демократијата и демократските институции во државите, во спротиставените интереси,

---

[61] М.Котовчевски - *„Национална безбедност на Република Македонија`` (прв дел)*, Македонска цивилизација, Скопје, 2000 год.

[62] Проширено во книгата на М. Котовчевски - *„Национална безбедност„* Скопје, 2011 год.

во се поголемото постоење на сецоностичките и сепаратистичките барања на различни етнички групи во повеќенационалните држави.

3. Потенцијални закани по националната безбедност на современите држави

Во изминатите децении, главните безбедноси закани за националната безбедност на државите секогаш водеа во насока на закани од воена природа, т.е. закани од војна и опасност од вооружен напад, а додека денес тој тренд на потенцијални закани или закани од невоена природа, води низ широкиот спектар на опасности од кои стравуваат современите држави, и кои интензивно своите потенцијали ги насочуваат кон нивно сузбивање градејќи соодветни стратегии на национална безбедност.

3.1. Закани од воена природа

Државите се наоѓаат под воена закана и се воено загрозени во ситуации кога некои други држави појавуваат низа свои аспирации за зголемување на својата моќ, гледајќи се себеси како силна држава, преку искористување на секојдневно нови ресурси, па така насочени со цел свој потенцијал одат кон освојување на туѓи територии и народи. Заканите од воена природа доколку бидат остварени во насока која е претходно смислена и очекувана, преставуваат најголема закана за светскиот мир, безбедноста, независноста и слободата на многу држави во светот со цел остварување на хегемонистички интереси на политиката со вооружена сила.

Од причини што државите и понатаму претставуваат референтен објект на безбедноста, а фокусот и понатаму останува на заканите од страна на други држави, воената одбрана се чини и понатаму незамислива. Од овие причини и поборниците за општат безбедност се залагаат за „неофанзивна одбрана" (non-offensive defence – NOD), позната уште како „дефанзивна одбрана" или „непроактивна одбрана".[63] Така, функцијата на армијата с одбрана на општеството од воените ризици и закани по безбедноста, со задача да оневозможи загрозување на државната територија од вооружен напад. Оваа функција подразбира нејзино ангажирање во превенција и во совладување на надворешните закани со употреба на воена сила во војна или при превентивното дејствување, што го нагласува значењето на воената безбедност.

Облиците преку кои ги препознаваме воените закани се: вооружена агрсија, која според дефиницијата на ООН од 1974 година значи:

[63] Moller, Bjorn: Common Security and Non-Offensive Defense. A Neorealist Prespective (Boulder, CO: Lynne Rienner, 1992); idem: Resolving the Security Dilemma in Europe. The German Debate on Non-Offensive Defence (London: Brassey`s, 1991); и idem: The Dictionaryof Alternative Defence (Boulder, CO: Lynne Rienner, 1995); или Bahr, Egon & Dieter S. Lutz (eds.): Gemeinsame Sicherheit.

~ употреба на сила на една држава против суверенитетот, територијалниот интегритет или политичката независност на друга држава;

~ воена интервенција која преставува недозволено мешање на една или на група држави во внатрешните работи на други држави притоа употребувајќи вооружена сила;

~ гранични вооружени судири кои настануваат како резултат од нерасчистени и нерешени проблеми со државните граници; или

~ заради остварување на помали територијални претензии и востановување нови граници.[64]

Во сите националните стратегии за безбендост, кога станува збор за закани по безбедноста од воена природа се вели дека ризиците од избувнување на војни и други воени судири како на глобално ниво, па се до регионално на национално иако се намалени, не се целосно елиминирани. Од ова произлегува и фактот дека воените закани се, или латентни, или се „замрзнати„ што значи дека во одредена ситуација, под одредени околности, во иднина истите би можеле да преставуваат одредена закана за безбедност на државите.

Според, Проф.Др.Л. Георгиева, воените закани имаат највисок приоритет во однос на национално-безбедносните проблеми од причини што употребата на вооружена сила може да предизвика брзи и насакани промени. Поради фактот што се употребува директна вооружена сила, воените закани преставуваат специјална категорија закани за националната безбедност.[65]

Од причини што воените закани по својот карактер се меѓународни, односно ги минуваат границите на една држава, се налага и политичкиот одговор на државите кон нив да биде мултилатерален, а не во склад со надминатите државно-безбедносни операции.

Денес, воената безбедност преставува одржување на физичката сигурност на општеството, на неговите економски интереси и на сите други витални вредности кои се од големо значење, а се потенцијална цел од надворешни загрозувања. Главниот субјект на државата/безбедноста, не се стреми кон водење војна или кон остварување на мир, туку кон овозможување на благосостојба на граѓаните во општеството. Ова особено се истакнува поради апстракноста на мирно временската состојба, која е директно поврзана со војна, т.е со состојба на отсуство на војна.[66]

---

[64] Т. Гоцевски - „*Основи на системот на национална одбрана*", Филозофски факултет – Скопје, "Киро Дандаро", Битола, Скопје, 2005 год.

[65] Л. Георгиева - „*Менаџирање на ризици*",Филозофски факултет - Скопје, - „Југореклам„ - Скопје, 2006 год.

[66] Paleri P. - „*National Security - imperatives and Challenges*", Tata McGraw – Hill Publishing Co Ltd, New Delhi, 2008, p. 125-132.

3.2. Закани од невоена природа

Историски гледано, прашањето врзано за безбедноста отсекогаш било доведувано во врска и анализирано во однос на воените закани. Избледувањето на воените закани, последователно е проследено со поексплицитно манифестирање на други видови закани, кои што според својата важност ги надминаа воените закани.[67] Иако, се уште постојат намалени ризици од воените закани, големиот број експерти се согласни дека во моментов неопходно е да се обрне поголемо внимание на широкиот спектар на невоените закани и на асиметричните закани,[68] кои преставуваат сериозен атак врз економијата, политичката стабилност, социјалната, животната средина, како и атак врз здравјето на граѓаните. Колку што овие закани стануваат тесно поврзани , толку одговорот на нив станува се посложен во однос на решавање или целосно елиминирање на истите. Невоените закани се скоро исти за сите држави, без оглед на нивното општествено уредување или на нивната геостратегиска положба во кои се тие, и најчесто се манифестираат преку организираниот криминал, верскиот и политичкиот екстримизам, тероризам, преку миграција на населението од повеќе причини, загрозување на животната средина и сл. Од сите овие невоени закани, две се издигнуваат – организираниот криминал и тероризмот- како битни и секојдневни закани кои имат приоритетен третман при изготвување на националните стратегии за безбедност на секоја држава.

Проф.Д-р Котовчевски М., во својата книга „Национална безбедност„[69], облиците на невоени закани кои можат да влијаат на загрозување на националната безбедност на државите ги групира како надворешни, внатрешни и глобални.

Под надворешни невоени закани истиот ќе каже дека тоа се неконвенционалните дејствија, психолошко-пропагандните дејствија, информациско-комуникациските закани, разузнавачките операции, неконтролираните имиграциски процеси, а со нив и неконтролираниот прилив на бегалци, политичките и економски санкции, еко заканите, како и техничко-технолошките несреќи.

Под внатрешни невоени закани, ги наведува, организираниот криминал, корупцијата, тероризмот, геноцитот и етничкото чистење, насилниот радикализам и екстремизам, шовинизмот и иредентизмот, деструкција на суверенитетот, анархијата, новиот тоталитаризам, сиромаштијата, еколошките закани, и техничко-технолошките несреќи.

Глобаните закани ја загрозуваат глобалната безбедност, но, исто така, тие индирекно преставуваат и сериозна закана за националната безбедност на современите држави. Во определувањето на глобални невоени закани, професорот Котовчевски ги истакнува глобалниот организиран криминал, информатичката војна,

---

[67] Л. Горгиева,-*„Творење на мирот„* Студио АДА, Скопје,1999 год.

[68] Најактуелните безбедносни закани во литературата на денешницата се познати под називите: невоени, асиметрични, алтернативни, меки, нетрадиционални, неконвенционални или современи закани.

[69] Проширено во книгата на М.Котовчевски, - *„Национална безбедност„* Скопје, 2011 год.

неоколонијализмот, економскиот, општествениот и културниот империјализам, авторитарните држави, слабите и најсилните држави, масовните неконтролирани меѓународни миграции, сиромаштијата, нееднаквиот пристап до ресурсите, глобалните пандемии, глобаните еко-закани и големите техничко-технолошки несреќи и катастрофи.

Сите невоени закани денес имаат неколку заеднички карактеристики по кои тие се идентификуваат, а тука се наведуваат, актерите на ваквите закани не се државите, туку тоа се неформални организации или групи, кои настојуваат да воспостават некој вид на контрола над јавните институции за да можат долгорочно и ефикасно да ги продолжат своите активности, како и фактот што нивниот идентитет флуиден и не е секогаш извесен. Друга каратеристика која ја квалификува невоената закана е фактот што денес безбедноста на современите држави е загрозена, пред се, од внатрешните фактори какви што се алтернативните форми на владеење и слабите и корумпирани државни институции. Имено, слабоста на државните институции во современите држави произлегува, пред се, од фактот што владите на тие држави се создаваат врз основа на коалициски компромиси помеѓу политичките партии, претходно усогласени според нивните идеолошки интереси, а не врз основа на политичката волја на граѓаните. Вака создадените државни институции, не секогаш одговараат на ставовите и барањата на граѓаните, туку на тој начин политичките елити се борат за опстанокот на политичката сцена, притоа создавајќи неприродни компромиси со коалициските партнери или со други влијателни поединци или групи. Од тие причини ваквите неприродни коалиции кои партиципираат во државните институции не се во можност да обезбедат државна и општествена стабилност, а со тоа помалку пак индивидиална безбедност за своите граѓани.

По завршувањето на студената војна, безбедноста на државите беше под влијание на пет нејзини основни димензии: воената, политичката, економската и општествената, како и безбедноста која се однесува на животната средина.[70] Во согласност со тоа, тероризмот како невоена закана има големо и значајно влијание на секои од овие димензии. Основните извори на современиот тероризам, голем број на автори ги наоѓаат во напластените и длабоки општествени, економски, етнички, верски и политички противречности и во несаканите општествени услови кои заговорниците на терористичките методи настојуваат да ги сместат по секоја цена, притоа не осврнувајќи се на кршење на човековите права и слободи, како и на интересите на останатите луѓе и на општеството во целина. Денес, кога во светот се заговар мир и демократија, присутни се разновидни облици на терористички активности кои тероризмот го преставуваат како најбрутален облик на манифестирање на насилство. Покрај користењето на насилство за остварување на своите цели, терористичките структури прибегнуваат и кон употреба на невооружени методи, како на пример фалсификување на пари и нивно пуштање во промет, се со цел рушење на економскиот и финансискиот систем на нападнатата држава, како и преку изведување на саботажи во енергетскиот,

[70] Buzan B., Weaver O., and de Wilde J., (1998), Security: *A new Framework for Analysis,* London: Lynne Rienner Publishers.

комуникацискиот, информатичкиот и во други системи кои се витално значење за националната безбедност на државата.[71]

3.2.1. Тероризам

Една од првите појави на тероризам, историјата забележала на Средниот исток, во Палестина, во првиот век по Христа. Сектата на зелотите сочинува една од првите групи, која ја практикувала техниката на терор на систематски начин и за која денес постои пишана трага. Така Јосиф Флавиј во неговите дела *„Еврејски антики,,* и *„Војната на Евреите,,* ќе истакне дека Зелотите уште се нарекувале и Сикарии, кои за првпат се споменуваат во 4-та г.н.е., кога се организирале за да се борат против империјалните сили поради тоа што вршеле попис врз Еврејското население, на што, Евреите гледале како понижувачки и потчинувачки чин. Во однос на другите еврејски верски движења од тоа време, Зелотите се однесувале како реформисти и сметале дека сметки му полагаат единствено на Бога. Еврејските елити не ги прифаќале Зелотите зошто со нивните дејства тие го загрозувале еврејскиот статус и безбедност на богатите, но затоа пак уживале меѓу народот, а особено меѓу младите чија поддршка им била потребна за да се борат против непријателот. Но и покрај ова, се смета дека основачи и водачи на Зелотите биле лица од богатиот слој. Тие имале двојна цел. Како религиозна организација се обидувале да наметнат, па и на сила, одредена строгост во религиозната практика, а како политичка, пак, имале цел да добијат независност за својата земја. Затоа и почнале да се користат со терор. Преку некои аспекти оваа партија е блиску до милениумските современи аспекти, само од нив се разликува по политичкиот проект кој се истакнува во нивните акции што ја објаснува народната подршка која ја уживала и одлучноста за која сведочеле нивните членови во несреќата.[72]

Освен Зелотите други класични примери за терористичка организација преставуваат и Асасините, и за нив, за разлика првите, постојат повеќе текстови од кои дознаваме за нивните дејствувања. Како и секоја општествена организација, така и религиозната партија на почетокот била природен противник на политичката моќ. Таа била поинтензивна кога овие религии имале универзален облик, како што е случајот за христијанството и исламот. Организациите кои ги создавале овие религии на почетокот се интересирале за религиозните и филозофските проблеми. Како што се зголемувале и колку повеќе и се верувало, толку нивното влијание се пренесувало и на други полиња на општестената организација за најпосле да сака да ја воспостави крајната контрола врз општеството: политичката моќ. Меѓу големите монотеистички сеопшти религии, исламот е оној кој најдобро знаел да ги интегрира стрикните теолошки прашања со нештата кои спаѓаат во делот на политиката. Христијанството, пак, секогаш било засегнато од теолошките проблеми, и затоа постојано постоеле кавги што станале белег

[71] Sačić Ž.,- " *Organizovani kriminal - metode suzbijana* " – Informator, Zagreb, 2001год.
[72] Шалијан, Жерар и Блин, Арно, *Историјата на Тероризмот,* Скопје, Табернакул,2009 год, стр.61-65

на неговата историја. Оваа дихотомија која ги разделува христијанството од исламот е фундаментална, што овозможува да разбереме зошто Асасините се појавиле во исламскиот свет, а нема трага во христијанството. Асасините биле дел од една организација, чија логика била борба за политичка моќ. Да се избере тероризмот за оружје, како и кај Сикариите, за Асасините било логичен избор. Преку неговата ефикасност тоа станало оружјето кое преовладувало во нивниот арсенал на стратегии, а на крај, оттука дошло и до дефинирање на самата суштина на оваа секта за генерациите кои следуваат. Тероризмот кој го практикувале Асасините е многу поблизок до модерниот тероризам, отколку со тираницидот. Тие ги напаѓале личностите поврзани со моќта, а не затоа што имале лична омраза против некој од нив.[73]

Со појавата на државата, како првобитна политичка институција, се појавува и владеачка класа која го наметнува својот авторитет, што и овозможува легитимност за владеење. Античката политичка мисла, која на политиката гледа и како на владеење на човек врз човек, го разгледувала и узурпирањето и злоупотребата на политичката власт на поединецот. Тој поединец, владеел во лицето на обичните граѓани секогаш бил тиранин кој ги угнетува или им ги зема производите, наплаќа такси, малтретира луѓе и сл., па оттука најголемиот дел од мислителите од тој период, оваа фаза кога поединец ќе извршел терористички акт врз владетелот, ја нарекувале тираницизам или тираницид. Во Античка Грција и Рим, убиците на „тираните„ биле издигнувани на пијадесталот на херои, а нивните постапки биле величени. Во средниот век, секој оној што ќе извршел некаква акција врз „тиранинот„ бил оправдан. Овој вид тероризам бил оправдан се до 50-те год. н IX век, кога се случувале повеќе индивидуални акции-атентати на кралеви.

Подоцна своето значење тероризмот го менува за време Француската Револуција, каде и самиот термин „тероризам„ беше популаризиран; тоа всушност е и период на пресвртница во историјата на тероризмот. Во тоа време тероризмот има позитивна конотоција. Системот или режимот на теророт од 1793-1794 г. беше прифатен како воспоставување наредби за време на транзитот анархистички период на немир и востание што ги следеше востанијата од 1789 год. и многу други револуции. Оттука, за разлика од денешното значење како револуција или антивладини активности преземена од недржавни или субнационални ентитети, режимот на теророт беше инструмент на владата држен од неодамна воспоставената револуционерна држава. Беше дизајниран да ја зацврсти новата владина моќ со застрашуавчки, против револуционерни субверзивни и други дисиденти на кога новиот режим ги назначи како „непријатели на луѓето„. Затоа и во овој период теророт е наречен државен тероризам.

Иронично, но тероризмот во неговиот оригинален контекст беше близок до идеалите за квалитет живот и демократија. Револуционерниот водач Максимилијан Робеспјер фамозно апелираше за „квалитет без кој теророт е зло; терор кој без

[73] Шалијан, Жерар и Блин, Арно, *Историјата на Тероризмот,* Скопје, Табернакул, 2009 год, стр.66-68

квалитет е беспомошен„ и прокламираше: „Теророт е ништо освен правда, поттик, строг и крут; тој е еманципација од квалитет„.[74]

Современиот тероризам е различен. Тој по своето значење не е религиозен-верското се појавува на површина во контекст на тероризмот во текот на првата половина на XX век. Ваквиот тероризам го практикувале некакви честопати маргинални групи, кои секогаш немале јасно дефинирана политичка цел. Тие биле од најразлични струи кои делувале како анархисти, нихилисти, популисти, марксисти, фашисти, расисти итн.

Во првата светска војна, тероризмот сеуште ја има својата револуционерна конотација. За ова време растечкиот немир падна со деценискиte Отоманска и Хабзбуршака Империја. На пример, во 1880-те и 1890-те год., милитантските ерменски националистички движења во Источна Турција следеа терористичка стратегија против Отоманските владеења што подоцна ќе биде прифатена од повеќето етно-националистички/сепаратистички движења од после Втората светска војна. Ерменските цели беа истовремено да зададат удар на деспотскиот „странски„ режим низ повторувани напади на администрацијата и сигурносните сили, со цел да се собере домашната поддршка, и да се привлече меѓународно внимание, симпатија и поддршка.

За време на 1930-те год.,поимот тероризам повторно доживува промена. Во овој период се помалку се користи ваквиот термин да револуционерните движења и насилството против владата и нивните водачи, а се повеќе да се објасни праксата на масивно-задушувачка служба на тоталитарните држави и нивните диктаторски водачи против своите граѓани. Според тоа терминот повторно се стекнува со својата поранешна конотоција за злоупотреба на моќта на власта, и беше употребувана посебно за авторитарниот режим кој владееше во Фашистичка Италија, Национал-социјалистичка Германија и Сталинистичка Русија.[75]

За време на Втората светска војна, во следниот замав на значењето, тероризмот повторно се стекнува со револуционерна конотација, и беше користен примарно за означување насилен револт. Државите, како Израел, Кипар, Кенија и Алгерија, својата независност ја должат, барем делумно, на националистичките политички движења кои го употребуваа тероризмот против колонијалните сили. Симпатијата и подршката за бунтовниците се прошири до сегмент на колонијалната популација, создавајќи потреба за помаку расудување, а повеќе политички неутрален јазик, отколку „терорист„ и „тероризам„ да ги опишуваат овие револуции и насилства што ги вршат за праведна „борба за слобода„. Многу нови независни држави и комунистички држави делумно го усвоија овој домашен говор, расправајќи се дека секој или секое движење што се бори против „колонијалното„ угнетување и/или Западната доминација, не треба да се именува како „терористи„ туку како „борци за слобода„. Оваа позиција можеби најдобро беше објаснета од шефот на Палестинската Либерална Организација (ПЛО) Јасер Арафат, кога се обрати до Генералното собрание на ООН во ноември 1974 год:

---

[74] Bruce Hoffman, *Inside terrorism, revised and expanded edition*, June 2006, p.3
[75] Исто, стр.11

„Разликата помеѓу револуционерите и терористите лежи во причината зошто тие се борат. Без разлика кој стои зад таа цел и се бори за слобода за себе и својата територија од непријателите,колонијалистите и населението, не можат едноставно да се наречат терористи``.

За време на 1960-те и 1970-те години, почнаа да се вклучуваат и национални и етнички сепаратистички групи надвор од колонијалната и неоколонијалната рамка, како и радикални идеолошко мотивирани организации. Азилантите и малцинствата лишени од државјанство –ПЛО(Палестинската либерална организација), ЕТА(терористичка организација) и др.- го посвоија тероризмот како начин да се предизвикаат внимание врз себе и нивните цели, во многу случаи се специфични цели како и нивните предци, за да привлечат меѓународна подршка и симпатии.

Во раните 1980-ти год., тероризмот значеше дестабилизирање на Западот како дел од глобалниот заговор. Владите на голем број држави кои ги подржуваа и финансираа терористичките инциденти извршени од различни групи растурени низ сите земји, беа поврзувачки линк до масовно прикриената завера. Со тоа тероризмот стана на некој начин маска или имитација на војна со која слабите држави можеа да се спротистават на големите ривали без разлика од ретрибуција.

Во почетокот на 1990-те год.,значењето на тероризмот стана нејасно поради појавата на наркотероризмот и т.н. феномен на сива зона. Сите криминални организации сега коваа стратешки алијанси со терористите и герила организациите или сами употребуваа насилство за специфични политички цели. Влијателната моќ на Колумбиските картели за кокаин, нивните блиски врски со лево-ориентираните терористички групи во Колумбија и Перу и нивните повторувани обиди за го соборат изборниот процес како и владата, можеби е најпознатиот пример за овој континуирачки тренд.[76]

Терористичките напади врз САД на 11.09.2001 година, уште еднаш го редефинираа тероризмот. Четирите самоубиствени бомбашки напади на четирите авиони брз различни таргети, од кој еден неуспешен, со масовни и досега невидени последици, бараше еднакво разбирлив и повлијателен одговор. Тогаш Американскиот претседател Џорџ Буш се изјасни дека, иако американската нација кога би била толку и дотолку ужасна нема да дозволи да и понатаму биде тероризирана, ниту од Ал Каеда, ниту од која и да било друга терористичка организација. Терористичките организации, скоро без исклучок, сега постојано селектираат имиња за себе, што потсвесно го избегнуваат терминот тероризам во секоја форма. Наместо тоа, тие предизвикуваат слики за себе како: слобода и независност, војска или други воени структури, самоофанзивни движења и праведна одмазда, или намерно избираат имиња што се децидно неутрални и лишени од сите најбезопасни сугестии и асоцијации. Терористите се перцепираат себеси како неволни војници, поттикнати од безнадежноста-и недостаток на некаква алтернатива- за да вршат насилство брз репресивните држави. Тие никогаш нема да

[76] Bruce Hoffman, *Inside terrorism, revised and expanded edition*, June 2006, p.16-18

признаат дека се терористи, секогаш ќе се расправаат дека општеството или владата или социо-економскиот систем и неговото право се всушност вистинските „терористи„.[77]

3.2.2. Терминолошко определување на тероризмот

Современата состојба во науката и практиката, кога е во прашање тероризмот и неговото спречување, сузбивање и превенирање, се наоѓа во потполна спротиставеност со основната девиза во науката според која битна претпоставка за спречување на секоја негативна појава е јасно и потполно дефинирање на појавата. И денес науката е во спротивност со оваа девиза, бидејќи за така масовна, општествена опасност и сложена за откривање и сузбивање криминална појава, не постои јасна дефиниција.[78]

Кога е во прашање дефинирањето на тероризмот, во него се внесува многу идеологија и политика, поради што не може да се дојде до посеопфатен пристап кон негово изучување. Во досегашната научна мисла постојат повеќе обиди за дефинирање на тероризмот, но до сега ниедна дефиниција не е прифатена , секогаш поради некој недостаток во објаснувањето на овој феномен, а особено поради непостоењето политички консензус кој е condition sine qua non за спречување и казнување на сите облици, видови и модалитети на терористичка активност.

Етимологијата на зборот „терор„ доаѓа од латинскиот збор „terrere„ што значи „предизвикување силен страв„ па отука, тероризмот преставува употреба на насилство со умисла или закана за употреба на насилство заради заплашување, а со намера да изврши присилба или заплашување на актуелната власт или на државата, како би се постигнале политичките, верските, или идеолошките цели. Тероризмот преставува акт физичко насилство, чија цел е да предизвика силни психолошки реакции, во прв ред страв, со надеж дека тие ќе помогнат да се одржи или да се промени однесувањето кое е важно за постигнување на политичката цел, ако таквиот акт не е оправдан со општите интереси кои се определени независно од него и ако овој акт не е извршен по правилата кои вообичаено се применуваат при практикувањето на власта.[79] Терористите многу ретко се самоидентификуваат како „терористи„ поради негативната конотација на терминот, па затоа тие се почесто ги користат терминте со

---

[77] Bruce Hoffman, *Inside terrorism, revised and expanded edition*, June 2006, 21-23

Sheik Muhammed Hussein Fadlallah, верски водач на Либанската терористичка група одговорна за киднапирањето на познатиот американски новинар Terry Anderson ,во својата книга „Invisibal Armies„ ќе објасни: *„Ние не се гледаме себеси како терорити зошто не веруваме во тероризам. Не го гледаме отпорот спрема окупаторот како терористички акт.Ние сме Муџахедини (Свети војници) кои водат Света војна за лугето„*

[78] Арнаудовски.Љ.,``*Меѓуусловеност и меѓузависност на тероризмот и организираниот криминал*``во Годишник на Факултетот за безбедност, Скопје, 2002г.,стр.82

[79] Димитровић В.,``*Људска прва и демократија, Свет и Југославија*`` Пословна политика, Београд

кои ја истакнуваат својата идеолошка борба, како на пример „сепратисти„ „борци за слобода„ „ослободители„ „герилец„ „муџахедин„ или „фадаин„.[80]

Денес, кога цел свет заговара мир и демократија, се проприсутни се различните облици на терористички активности кои тероризмот го преставуваат како најбрутален облик на манифестација на насилство.Терористилките активности ги сочинуваат три основни чинители и тоа: извршител, жртва и цел што сака да се постигне, но кога станува збор за дефинирањето, овде сеуште не постои единствена и универзално прифатена дефиниција за тоа што преставува тероризмот.

Женевската конвенција за превенција и репресија на тероризмот од 1937 год. содржи неодредена дефиниција за овој поим според кој, акт на тероризам значи казнени дела насочени против државата, чија цел или природа е предизвикување терор кај определени лица, групи на лица или кај јавноста. Поблиска и појасна дефиниција не содржат ниту подоцнежните меѓународни конвенции, како Европската конвенција за спречување на тероризмот од 1977 год., Меѓународната конвенција на ООН за казнување на терористичкото подметнување на бомби од 1997 год. и други. [81]

Во Американската научна литература, постојат најразлични дефиниции кои при дефинирањето на овој комплексен поим тргнуваат од различни аспекти.

Така според Алекс Шмид[82], нејасната природа на тероризмот се должи на неговата неопиплива природа. Тероризмот не е физичко тело за да може да се измери и дефинира; тоа не е нешто кое постојана се менува. Тој станува поконкретен кога го дефинира тероризмот во кривичен кодекс, но проблемот е што тие кодекси не се применливи во секоја култура.

Волтер Лакуер[83], пак, вели дека дури и да се напишат цели томови за дефинирање на тероризмот тоа нема да придонесе многу во нашето разбирање за ваквата појава/поим, но иако тој дава неисцрпна дефиниција со корелација на десетици различни дефиниции, сепак неговите напори не го стават проблемот во фокусот. Комплексноста на дилемата околу дефинирањето се влошува кога се зборува за транснационалниот криминал.

Интересно е што од една страна постојат значајни аналитичари кои тероризмот го калсифицираат како криминална активност, сметајќи дека во која и да е криминална активност, постојат шанси да се вклучени терористи. Физичкото насилство, киднапирањето и убиството се на врвот на скалата, заедно со трговијата со дрога, перење пари и миграцискиот криминал кој спаѓа во друга област. Од друга страна, пак, има аналитичари кои одбиваат да го класифицираат тероризмот како криминална

---

[80] Латински збор „fidaiyin„ или „fedayeen„ што значи спомен на маченишство, термин наменет за арапските герилци кои оперираат против Израел

[81] Љ. Арнаудовски, *Криминологија*, Скопје 2007, стр 313

[82] Alex Peter Schmid – Political terrorism: A research guide to concepts, theories, data bases and literature, Amsterdam : North-Holland ; New Brunswick, U.S.A. : Distributors, Transaction Books, [1984], c1983.

[83] Walter Laqueur – The new terrorism: Fanaticism and the arms of mass destruction, Oxford University Press, 2000 - Political Science - 312 pages.

активност, па така Пол Вилкинсон[84] во своето дело „*Политички тероризам*„ расправа дека научниците, владите и новинарите мислат на политички тероризам кога станува збор за проблемот на тероризмот. Тој може да се разгледа како државна репресија, идеолошки револуционерни активности или националистички револуции.

Државата репресија се однесува на влади кои користат терор за да одржуваат ред меѓу граѓаните, додека идеолошкиот револуционерен тероризам се фокусира на користење на насилство за да се смени политичкиот систем. Националистичкиот тероризам ја става етичката структура на владата над идеологијата и државата, и националниот и револуционерниот тероризам можат да бидат спонзорирани од државите. Надоврзувајќи се неговиот колега Х.Х.А.Купер [85] вели дека терористите се вкучени во секаков вид на криминал, но сепак нивната крајна цел не е криминална, бидејќи цел на тероризмот е да го смени политичкото однесување. Па отука, и Вилкинсон и Купер ни сугерираат дека тероризмот е тема за политичка анализа, а не за криминологијата.

Според содржината на досега наведените дефиниции за тероризмот кои се разликуваат во одредени нијанси, може да се заклучи дека во нив во голема мера се препознаваат елементите кои го чинат ова дело општествено недозволиво и незаконско. Карактеристично за тероризмот е што терористите во ниту еден случај не може да биде невин пред законот, не постојат лица и објекти кои се имуни на ваквите терористички активности, а државите и нивните безбедносни структури кои даваат логистичка подршка на терористичките организации се одговорни за стореното. За изведување на своите акции каде што последица се голем број на човечки жртви и големите разурнувања кои траат неколку минути, терористите се подготвуваат со години. Тие секогаш се во предност во однос на безбедносните структури на државите, од причини што тие се подготвуваат онолку време колку им е потребно за изведување на терористичкиот удар и речиси секогаш го постигнуваат ефектот на изненадување. Своите активности терористите ги изведуваат плански и тие се плод на нивните внатрешни мотиви кои се комплементарни со политиката на терористичката организација, чии членови се самите терористи. Терористичката организација дејствува илегално, прво, со цел да се заштити таа и нејзините припадници од откривање и кривичен прогон, и преку изведувањето ненадејни акции, преку сеењето страв и преку создавањето чуство на несигурност, загрозеност и неизвесност, да постигне што е можно поголем ефект во државите. Современите терористички организации во својата структура имаат политички и терористички (воени) крила. Политичките крила обезбедуваат социјални услуги, едукација, водење на деловните активности како и учество на избори со свои преставници, додека воените (воооружените) крила учествуваат во изведувањето на атентати, бомбашки напади и слични акти на насилство.

---

[84] Paul Wilkinson-„*Political terrorism,* Macmillan, 1974 - Revolutions - 159 pages, достапно на https://books.google.mk/books?id=Tti7QgAACAAJ&source=gbs_book_other_versions

[85] H.H.A.Cooper–„Report on the Task Forces on Disorders and Terrorism„ достапно на http://handle.dtic.mil/100.2/ADA153506

Денес, терористите и терористичките организации, за разлика од минатото, применуваат современи методи, стратегија и тактика на дејствување. Тие користат средства кои порано не биле користени, како на пример, некои видови на нуклеарно, хемиско или биолошко оружје што преставува сериозна закана за безбедноста на државите. Ако во минатото познат метод на терористите било да се убие еден човек со цел да го заплашат останатото население, тие денес настојуваат да заплашат и да убијат што е можно поголем број на луѓе. За постигнување на посакуваната терористичка цел, терористите ги користат сите познати облици на насилство како диверзија, подметнување пожари, извршување атентати, киднапирање, закани со употреба на конвенционално или на нуклеарно оружје, масовни убиста на граѓани или туристи. Нападите најчесто ги насочуваат кон „меки цели„ каде безбедносните структури не можат веднаш и ефикасно да дејствуваат, како на пример: авиони, метроа, возови, прекуокеански бродови и сл., но неизбежна цел на терористите се и најосетливите државни институции, каде со помал напор и ризик за сторителите ќе се добие поголем ефект, преку изведување на што поголеми разорувања и човечки жртви, со крајна цел создавање состојба на страв и несигурност кај граѓаните.

Денес активностите на терористите ги препознаваме и преку современите форми на терористички активности познати како „екотероризам„ „биотероризам„ „наркотероризам„ или активности поврзани со нападите над современите комуникациски и информатички системи познати како „високо-технолошки тероризам„ познат и како „сајбер тероризам„.

3.2.3. Облици на современ тероризам

Современите форми на терористичките активности се само насилен облик на делување на тероризмот во современите држави. Некои автори сметаат дека човекот не се раѓа како терорист и според тоа тероризмот може да се дефинира, со помош на политичката и правната теорија, со чија цел може претходно да се увидат последиците кои можат да следат. Без оглед на тоа што сеуште во светот преовладува присуството на конвенционалниот тероризам, сепак и неконвенционалниот, еколошкиот и високо технолошкиот (сајбер тероризам) се сериозна закана и опасноста од нивното делување кој од ден на ден е предмет на длабока анализа за која современите држави превземаат стратегии за нивно спречување или во најмала рака намалување од таквиот вид закана.

Слика 1: Орвограм на современи облици на тероризам

Кога говориме на ***конвенционалниот тероризам***, тој се дели на убиствен терористички напад од далечина и самоубиствен тероризам.

Убиствениот терористички напад од далечина преставува облик на конвенционален тероризам кој се применува од почетокот на XX век. Тој сам по себе е облик на терористичка активност која од далечина, претходно обезбедна безбедно за терористите, испукуваат проектили, активираат експлозиви и други разнесувачки средства, само заради нанесување голема штета со човечки животи и материјално-технички средства на државата која е цел на терористите. Жртвите на ваквиот облик на тероризам се невини цивили, преку кој терористите сакаат да ги заплаша граѓаните, а со тоа да го свртат вниманието и на меѓународната политика за своите политички цели на кои тие се стремат и се спремни да ги направат.

Самоубиствениот тероризам е еден од најтрагичните облици на современиот тероризам, под кој подразбираме изведување терористичка акција која неможе да биде успешна без смрт на извршителот на акцијата, а он или она се за тоа свесни и претходно подготвени.[86] Иако денес кога говориме за самоубиствениот тероризам и терористичките организации, прва асоцијација е Ал Каеда, Хамас, Хезболах, сепак самоубиствениот тероризам не е својствен само за една религија, еден народ, држава, континент. Самоубиството во современиот свет го користат различни религиски групи, вклучувајќи ги и муслиманската (сунитски, шиитски), христијански и еврејски, како и многу други групи и организации во различни делови од светот.[87] Поради фактот што терористите можат да делуваат на било кој дел од светот, никој неможе потполно да биде сигурен дека нема да биде мета на терористичка активност. Цел на терористот самоубиец е саможртвувањето во текот на изведувањето на акцијата т.е во текот на разорнувањето на однапред одреден објект, се со цел да влијае на политичките процеси кои се и порака за таквиот превземен чекор кој може да биде проследен и со невини жртви од големи размери. Ваквите самоубиствени напади се одраз на крајна немоќ;

[86] Kurth Cronin, *CRS Report for Congress, Terrorists and Suicide Attacks*, 28 August, 2003.
[87] Pape, R. A. ***„Dying to Win„*** *The Strategic Logic of Suicide Terrorism,* Randon House, New York, 2005, p.28

слабост; очај кој се јавува од длабока неправда; или од аспирациите за постигнување повисоки цели, а проследени со отсуство на соодветни ресурси за исполнување на истите. Самоубиствените напади преставуваат насилни, политички мотивирани акции, но со претходна подготвеност на сигурна смрт, која е предуслов за успешен напад, па отука може да се каже и дека сомоубиствениот тероризам е „синтеза на војна и на театар„[88] Самоубиствениот тероризам е единствена и ефтина акција на која се спремни терористичките организации за реализација на зацртаните цели, бидејќи во ваквиот облик на тероризам нема потреба од мисија за спасување на извршителот; со него се зголемува веројатноста за поголем број на жртви и поголемо уништување на делокругот во кој делува терористот; бомбашот самоубица може прецизно да го одбере местото времето и да ги процени околностите за напад; нападот има големо влијание на јавното мислење и на медиумите.[89] Така, терористот-самоубица е целосно свесен дека тој/таа, сам/сама, ако не потегнат кон планираниот напад, истиот нема да биде реализиран, а нивната сопствена цел на која се подготвени е дека животот го даваат за идејата (религијата/организацијата) на која и припаѓаат на крај ги парви решителни на ваквиот чекор. Во изборот на луѓе за самоубиствен напад клучни се неколку карактеристики: религиозноста (националната посветеност), перцепцијата за нанесената неправда, сопственост да издржи силен психолошки притисок и способност да остане доверлив, а само што ќе се утврди дека кандидатот е соодветен, понатаму продолжува на психолошка обука која опфаќа две нивоа: религиозна и идеолошка (совладување на стравот од смрт) и втората е техничко оперативната.[90]

Неконвенционалниот тероризам го преставува тероризмот како политичко насилство, односно невооружено насилство, кое е доста сложено за препознавање како би можела државата и нејзините органи навремено да делуваат против вакват појава. Неконвенционалниот тероризам се врши преку комплементарни, односно различни - најсовремени методи и постапки без употреба на оружје. Ваквиот тероризам се врши преку психолошко-пропагандни активности, преку злоупотреба на информации со помош на примена на радио, телевизија, весници и сите информациски системи кои предизвикуваат страв со примена на терористичка закана, потикнување на бунт во државните институции со политички мотиви, потикнување и користење разни општествени кризи, организирање и подготвување државен удар од старна на политички мотивирани терористички групи и организации. Целта на овој вид на тероризам може да биде свртување на вниманието на меѓународната заедница на некои терористички организации кои сакаат да ја истакнат својата политичка цел, дека тие можат да ја добијат подршка од највлијателните и богати земји во светот. Оваа форма на тероризам е доста мистериозна и пред се тешка за откривање, па затоа е

---

[88] Cindy, C., Combs, Slann, M., Encyclopedia of Terorism, New York, Facts on File, Inc., 2002, p.20

[89] Sprinzak, E., Rational Fanatics, Foreing Policy, September-October 2000, p. 68

[90] *Религиозната обука е во суштина карактеристична за исламските терористички организации, јаизведуваат свештеници кои го проповедаат самоубиствениот чин како оправдан (светот после смрта во кој се оди треба да биде оправдан);*
Техничко оперативната обука опфаќа аспекти како што се: запознавање со средствата за активирање на експлозив, упатсво за сокривање на бомби, како да се дојде до целта, насоки кои се однесуваат за деталите на мисијата која му е зададена (вид на мета, начин на транспорт до целта, време на напад и.т.н)

веројатноста за негово сузбивање е сведена на најниско ниво. Иако тероризмот во суштина е јавен-отворен, но за неконвенционалниот тероризам може да се каже дека пред се тој преставува невооружан, подготвителен период за конвенционалните терористички акции кои следат, што во теоријата е добро познато дека и заканата и припремата како и самата акција е терористички акт.

Еколошкиот тероризам на почетокот на XXI век преставува најизразената опасност за човештвото. Овој облик на тероризам е карактеристичен по тоа што во својата активност како алатка и како мета за извршување на терористичките активности ги користи природните ресурси. Кога се во прашање ресурсите како алатка за терористички дејствија, еколошките ресурси се користат како преносител на деструктивните, опасни агенси на популацијата. Терористите кои пак сакаат да го користат ресурсот како мета можат да дигнат во воздух брани се со цел да поплават град или повеќе градови. Оваа врста на напад сега засега е доста несекојдневна кога станува збор за очекуваните напади или врсти на напади од страна на терористите, но сепак не е исклучена како можна следна активност. Еколошкиот тероризам како облик на тероризам во себе ги вклучува и нуклеарниот, хемискиот и биолошкиот тероризам.

Нуклеарниот тероризам преставува употреба или закана за употреба на радиоактивен материјал. Нуклеарното оружје на терористите може да им овозможи предност во процесот на остварување на нивните политички цели, а особено во предизвикување или насочување на внимание кај светските медиуми. Нуклеарниот тероризам преставува поим кој опфаќе повеќе можности кои не мораат неопходно да го вклучат и нуклеарното оружје. Според тоа најсоодветно е да се зборува за употребата на нуклеарен материјал за терористички цели што преставува најсоодветно објаснување за нуклеарнито тероризам. Во таа смисла може да се дефинираат три основни принципи на дејствување: преку употреба на нуклеарни експлозивни направи (нуклеарна експлозија), напад или саботажа на постоечки нуклеарни постројки, употреба на бомби (класична експлозија со чија помош радиоактивниот материјал ќе се рашири во околината). Проценката на ризикот е многу важна во објаснувањето на веќе наведените методи за терористичка акција. При проценка на ризикот за секоја метода е многу важно стручно да се предвиди ефикасното дејствие и последиците, како и веројатноста за нејзина употреба од страна на терористите. Бидејќи нуклеарниот тероризам е активност која се спроведува со помош на висока технологија, се сметало до пред крајот на XX век дека тоа преставува помалку веројтна активност, бидејќи радиоактивните материјали се добро чувани, тие се скапи и опасни така што некогаш било многу тешко да се набават, поседуваат, со нив стручно да се ракува и сето тоа да се држи во тајност. Меѓутоа на почетокот на XXI век ситуацијата во таа насока се менува. Нивото на техничкото знаење во светот се повеќе расте, начинот за изработка на такви направи јавно се објавува во разни стручни научни списанија, а пристапот до нуклеарнот материјал станува поедноставен.

Хемиски тероризам

Технолошките достигнувања во процесот на поизводство на хемиско оружје, како и средство за нивна употреба денес достигнаа на ниво на кое високи привилегии не уживаат само државните и воени институции туку и поединечни невладени субјекти, посебно оние кои своите терористички цели сакаат да ги изведат на ваков начин. Денес каде тероризмот е главна закана по современите држави се повеќе се стравува од заканата од хемиски тероризам, ако се земе во предвид дека предусловите за таквата закана се многу реални.

Употребата на хемиско оружје во терористичките акции може да има две форми во зависност од дирекните последици што сака да се предизвикаат: напади со цел масовно страдање и голема материјална штета.

Од гледна точка на ефикасноста на терористичките организации, употребата на хемиско оружје во терористичките организации има свои предности: лесна достапност на набавка на суровини кои се потребни за изведување на заканата, ниски цени, големи неконтролирани количини во насока за примена на истите бидејќи таквите состојки се користат во секојдневната работа на индустриите.

Хемискиот тероризам не бара голема финансиска основа, па така дури и сиромашните терористички организации може лесно да дојдат до хемиско оружје, а со тоа ваквиот тероризам крајно опасен.

Биолошкиот тероризам преставува употреба и ширење на разни опасни материи од биолошко потекло (различни видови микроби) во големите гратски центри и пошироко, со цел да се предизвика бројни опасни последици и да се поткопа моралот на нападнатата држава/нација.

За разлика од хемискиот тероризам, биолошкото оружје не е дизајнирано и не може вообичаено да биде користено за „отворени напади``. Биолошкото оружје во основа се користи за масовно уништување на цели нации/држави, а резултатите од ваквиот напад не се веднаш уочливи, бидејќи тие настануваат и го земаат својот голем данок во човечки животи неколку часа или денови подоцна, откако некои жртви веќе го напуштеле местото на нападот.[91]

Терминте ``биолошко оружје`` и ``биолошка војна``, првпат официјално се појавуваат по Втората светка војна, на Генералното собрание на ОН кое се одржува во 1947 година, каде заедно со хемиското, нуклеарното, и биолошкото оружје се одредува во групата на оружја за масовно уништување.

Биолошкото оружје како такво не се користи во меѓудржавен конфликт, но сепак постои голема опасност дека во иднина би можело да биде и една од можните закани на современите држави.

---

[91] М. Котовчевски., ``*Современ тероризам*``, Македонска цивилизација, Скопје, 2003, стр.195

Биолошкото оружје е ``одлично`` сретство за војна и тероризам, бидејќи ``економското производство``, според одредени пресметки е со ниска цена за разлика од хемиското и нуклеарното оружје. Дополнителна предност на ваквото оружје е фактот дека тоа е тешко да се заштити себеси (оној кој е директен учесник), бидејќи е невидлив, без мирис и вкус. Ризикот од биотерористички напад се заканува на сите земји, па за таа цел не би тербало да се занемари.

3.2.4. Тероризмот како асиметрично војување

Помеѓу многуте научници и аналитичари во XXI век се повеќе се споменува терминот сајбер тероризам, сајбер војна, сајбер шпионажа или информациска безбедност и информатилка војна, а во суштина сеуште не постои консензуалност околу дефинирањето на овие термини. Во контекст на ова виртуелниот простор се почесто преставува објект на заштита, иако не може да се опипа, ограничи и контролира неговиот развој.

Војната или војувањето како општествена појава го проширува своето онтолошко значење, така што денес овој термин не значи исклучиво меѓудржавен вооружен конфликт, туку води кон асиметричен конфликт каде еден од актерите може да биде не-државен актер/и и недржавен субјект како што се паравоените групи, терористичките организации и криминални банди, па така Клаузевицевото[92] традиционално поимање на војната како „продолжена рака на државната политика„ станува претесен за денешната комплексна реалност.

Префиксот „Сајбер„ преставува електромагнетни и компјутерски спектар на активности. „Сајбер„ е синоним за виртуелно неопипливо, а колоквијално најчесто се поврзува со глобалната мрежа на светот (интернетот), иако во него се вклучуваат и многу други делови. Оптички кабли, сателити, сите информациско-комуникациски технологии, дигитални мрежи, се категории кои може да се класифицираат под терминот, „сајбер простор„ па отука се поставува прашањето: дали за војувањето е потребно физичко насилство?

Според класичната дефиниција за војната, но ако ја прифатиме можноста дека војната може да се води и во сајбер просторот, јасно е дека на ова место неможе да се изврши чин на директно насилство, но сепак можно е ваквите активности во сајбер просторот да предизвикаат човечки жртви.

Денес, речиси сите аспекти на општествениот живот се директно или индиректно поврзани со информатичката и комуникациската технологија. Систем за делечински управување на шини за брзи возови, системи за ладење во нуклеарен реактор или

[92]http://www.odbrana.mod.gov.rs/odbrana-stari/vojni_casopisi/arhiva/VD_2011-prolece/17.%20Promenljivost%20fizionomije%20rata;%20Miloljub%20Sretenovic.pdf

компјутерско раководење со производна линија во петрохемиска фабрика денес е реалност, па клучот на манипулацијата во сајбер просторот е токму во тоа да може да се врши контрола во текот на целокупната инфраструктура. Операцијата во виртуелниот домен создава последица во физичкиот. Во тој контекст може да го прифатиме терминот сајбер војување како оправдан и можен. Сепак мора да се направи разлика помеѓу активностите кои се чести во сајбер просторот, а кои не преставуваат „војна„.

Тука се наведува и сајбер шпионажата, која е стара колку и сајбер просторот, субверзијата, саботажата, кражбата на податоци кои се составен дел од криминалните активности, а кои пак се составен дел од војувањето кога станува збор за воени дејствија на копно, воздух, море, но сепак не се задолжителни.

Актерите во овој простор не секогаш се политички мотивирани, па така војувањето не секогаш се одвива на релација држава на држава. Честопати дејствијата во овој простор се одигруваат на ниво на поединец-група, држава-организација, група институција, поединец- компанија и сл, па отука и од досегашните случаи, во праксата и жртвите во современиот свет сепак покажале дека војувањата можат да го водат и недржавни актери, што во научните кругови се дефинираат како асиметрично војување/конфликт.

Кога зборуваме за асиметријата во војувањето секогаш се поаѓа од неговите пет димензии : [93]

Знаењето – кое подразбира високо-квалитетна и од значење за мисијата информација која е достапна на една страна, но се држи во тајност да не ја дознаат противниците, со цел да се гарантира супериорност во поглед на квалитативното значење;

Сила/снага – квалитет и квантитет на сила во секоја димензија;

Време – се однесува на брзината, издржливоста, навременост, посветеност или комбинација од сите нив;

Простор – ги опфаќа областа, длабочината, сферата и општеството;

Генијалност – се однесува на поседувањето на лидерските квалитети, употребата на неконвенционалните активности и/или одбивање да се следат конвенциите;

Асиметричниот конфликт обично се води на еден променлив, асинхроничен и непредлидлив начин, а целта е да се нападне противникот и да се погоди неговиот гравитационен центар за да се постигне сопствената цел. Употребата на информациите за полесно извршување на посакуваното дејствие, а подоцна и ширењето на информацијата на ефектот кој е постигнат денес се постигнува со примената на мас-медиумите, особено на интернетот како една алатка од терористичката стратегија.

---

[93] Bockstette, C. Jihadist Terrorist Use of Strategic Communication Management Techniques, George C. Marshall European Center for Security Studies, Number 20, December, 2008, p.7.

Теоријата дека тероризмот е асиметрично војување т.е совршеното комбинирање на тероризмот со глобалните мас-медиуми кои во голема мера му овозможуваат истиот да достигне големи размери го прават тероризмот на XXI век уште потежок во карактеристиките за негово дефинирање и сузбивање.

Главниот застапник на оваа теорија се смета познатиот филозоф и публицист Алаин Де Беноист[94], а истата под влијание на глобалните општествени промени, тероризмот го прогласуваат како „воен акт„ при што станува збор за нов тип војување, за војна без терен и бојни полиња. Во судирите секогаш владее асиметријата: државите стојат наспроти наднационалните терористички организации; терористите ги знаат своите цели, додека државите не знаат каде да возвратат бидејќи наспроти огромниот државен безбедносен апарат вообичаено стои помала група на терористи.[95]

[94] http://files.alaindebenoist.com/alaindebenoist/pdf/terrorism_state_of_emergency.pdf

[95] М. Шикман, Самоубилачки тероризам-феноменолошки и виктимолошки аспекти, НБП Наука-безбедност-полиција, Часопис Криминалистичко-полициске академије, Београд, 2008, стр.182

Трета глава

1. Развој на комуникациската мрежа

Со крајот на XVIII век започнува и развојот на електричната револуција. Некои значани години кои го забележаа периодот на XIX век и почетокот на XX век се периоди на иновации кои сеуште и денес се едни од актуелните придонеси кои низ годините постојано се надоградуваат и преставуваат неопходен сегмент од човековото постоење.

1839 год: започнува периодот на испраќање на електрични сигнали преку жици, каде

1840 год: со појавата на електричниот телеграф, започнуваат и првите комерцијални телефонски услуги отврени во Лондон чии систем се надоградува и развива се до

1844 год: каде се појавува и првиот пренос на слика пратени на факс машина. Телефонските жици набрзо поврзуваат големи градови во многу земји, кои придобивката од ваквите иновации ги прават земјите подостапни за комуникација. Поради фктот што во овој период телеграфските и во поголем степен телефонските врски се главниот медиум за телекомуникација, во

1852 год: отпочнува со работа Националното типографско здружение чија основна дејност е да се грижи за трговијата со печатените весници и дригите медиуми. Нешто подоцна ова здружение се применува, па така во

1865 год: официјално е формирано и прогласено како Национална типографска унија (ITU)[96],

1869 год: поради своето проширување во Канада и релациите кои се воспоставуваат со тамошното население ова здружение се преименува во Меѓународна телеграфска унија (ITU), која и понатаму ја следи и контролира трговијата со печатените весници и другите медиуми.

1876 год: следен скок во оваа електронска револуција е периодот на патентирање на телефонската линија, а во

1885 год: Меѓународната телеграфска унија почнува да изготвува меѓународна легислатива за употреба на телефонијата.

1900 год: Откривањето на „бежичниот телефон (сега познат како „радио„) кон крајот на XX век ја зголеми мобилноста на официјалните и лични комуникации од точка до точка (пр.брод-обала), и точка до повеќе точки (пр.испраќање и соработка со полицијата), и воедно станува масовен медиум за информации, забава и трговија во повеќе земји.

[96] http://www.itu.int/en/about/Pages/default.aspx

1906 година. Оваа е годината се случува првиот светски пренос на глас и музика, а настанот е одржан во Берлин, проследен од Меѓународната телеграфка унија, која ја сочинуваа 29 земји членки, и на која се донесени неколку заклучоци, како следниве:

1907 година, заклучно со 1-ви Мај, Меѓународна телеграфка унија (ITU) ќе дејствува како централен администратор, кој пак истата година со почетокот на работата донесува и анекс кој ги содржи првите прописи од областа.

1908 година, е година каде САД се приклучува во составот на работата на Меѓународна телеграфка унија (ITU), а во -

1912 година, поткрепени со технолошкиот напредок каде телефонијата овозможила комуникација од брег до брег, а радиото прераснува во медиум за соживот, се појавува потребата од воспоставување на правни и регулативни режими во комуникациските мрежи.

1920 година, како и во текот на следните години употребата на радиото како медиум се зголемува, бидејќи се повеќе се емитуваат популарни емисии, па за да се подобри квалитетот на работата и ефикасноста на емитувањето во -

1927 година, на конференцијата која била одржана во Вашингтон се донесува акт, со кој се регулира работата на радиото, за што Министерството за трговија на САД, издава дозволи за користењето на радио фрекфенцијата, а со тоа се забранува и преносот на приватни радио пораки и откривање на нови содржини. Целата надлежност околу работата на телефонските и радио комуникациите преминуваат во надлежност на Меѓународна телеграфка унија (ITU).

1932 година, повторно се појавува потребата од одржување на конференција, на која земјите членки во Мадрид, договориле да се опфати целиот спектар на одговорности на Меѓународна телеграфка унија (ITU), и истата да биде преименувана во Меѓународна унија за телекомуникации, па така во -

1934 година, на 1-ви Јануари стапува на сила новото име на дотогаш Меѓународна телеграфка унија (ITU), сега преименувана во Меѓународна унија за телекомуникации (ITU).

Иновациите во електронските комуникации продолжуваат да напредуваат, па така во текот на -

1940 година, се појавила потребата за реализација на телевизиските сигнали за сите заедници во одалечените планински области, па со оглед на тоа се појавува и раниот развој на ``сателитската антена за телевизија`` - (CATV), како систем, која со донесувањето на кабел, а до неодамна и со оптички кабел, се до денес, се развива во модерна кабловска телевизија, која пак почнува да се натпреварува со телефонските компании за реализација на видео, глас, податоци и услуги за клиентите.

1947 година, на 15-ти Ноември, со договор меѓу Меѓународната унија за телекомуникации и тогаш ново создадените ОН, ``ITU`` е признаена како специјализирана агенција за телекомуникации, во чија надлежност се стават сите релации со телекомуникациите меѓу државите и нивна контрола.

1949 година, вака склучениот договор, официјално стапува на сила на 1-ви Јануари, а ``ITU`` продолжува да работи, но како специјализирана агенција.

1962 година е значајна по првиот експериментален комуникациски сателит лансиран во вселената, а со тоа сателитските комуникации стануваат подостапни не само за одредени влади, туку и за комерционалниот сектор и поединците ширум светот, па така во следниот период кој следи во -

1969 година, се појавува интернетот, тогаш познат како ``ARPAnet``, кога за првпат повеќе компјутери биле поврзани во една компјутерска мрежа, а пак овој настан го опфаќа пронаоѓањето на одговорот од заканите за потенцијален нуклеарен напад, чии проект е на американското Министерство за одбрана.[97]

За разлика од денес, кога милијарди луѓе имаат пристап до Интернет, во 70-те години од минатиот век, ``ARPAnet`` служел само за компјутерски професионалци, инжењери и научници, кои го познавале неговиот комплексен начин на функционирање, но иако неочекувано, сепак со голема брзина и во обем во кој беше надвор од сите очекувања и предвидувања, се создадоа нови компјутери на нови мали, средни и големи мрежи, кои меѓусебно се поврзале, создавајќи разновидни информатички инфраструктури – соединувања во една огромна мутант мрежа позната под името „Интернет„ Посебно е значајно да се укаже дека многу од компјутерските мрежи, а посебно оние кои ги покриваат националните сајбер простори и формираат национална информатичка инфраструктура, поради податоците кои ги имаат и функциите кои ги извршуваат, стануваат критични од аспект на националните интереси. Самиот термин национална информатичка инфраструктура се однесува на таков збир на компјутерски системи, база на податоци и телекомуникациски мрежи кои го покриваат целиот национален сајбер простор и кои ги чини електронските податоци и сервиси да се широко расположливи и достапни.

1971 година, со напреднувањето на комуникациите, се појавува и првата ``E-MAIL`` програма, која го подобрува комуникацискиот свет, а во -

1977 година, за првпат се појавува персоналниот компјутер-модем кој им овозможува на дигиталните компјутери да комуницираат еден со друг преку аналогните телефонски линии, а луѓето успеале да го прошират електронскиот нервен систем и со глобално опфаќање, надминувајќи ги границите на просторот и времето, успеале да ја покријат целата планета се до каде што се простираат нејзините физички граници.

---

[97] Pertovič R.S. „*Kompjuterski kriminal*„ Vojno izdavački zavod, Beograd 2004, III izdanje, str.66-73.

1980 година, се произведуваат првите популани компјутери за потрошувачкиот пазар, а оваа година се поврзува и со појавата на интернетот како глобално мрежа за јавноста, што и самиот визионер на комуникацијата Маршал Меклуан (Marshall McLuhan)[98] го нарекува ``глобално село``. [99]

1984 година, ``World Wide Web``- (www), се појавува како нова интернет апликација и услуга, која не е само во услуга на владите, туку својата намена ја има и кај пошироката јавност, а која се состои од многу видови на опрема и телекомуникациска инфраструктува, што само посебе кажува колку е во добра функција нејзината употреба.

1985 година, Меѓународната унија за телекомуникации ја одржува својата прва светска конференција во Аруша, Танзанија, на која земаат учество сите земји кои се во нејзин состав, а во -

1989 година, Меѓународната унија за телекомуникации на конференцијата одржана во Ница, донесува заклучок за неопходната помош на земјите во развој, да им се даде насоки за управување со целиот спектар на комуникации., а за таа цел Меѓународната унија за телекомуникации во -

1991 година, формира центар за развој на телекомуноикациите, кој подоцна како дел од ``ITU`` - Меѓународната унија за телекомуникации, во -

1992 година е преименувана како ``Биро за развоја на телекомунокациите``.

1994 година, се одржала конференција во Кјото, под називот „Светски форум на телекомуникациската политика„ на која земјите учеснички, со слободна размене на идеи и информации полемизираа за новите прашања на политиката што произлегуваат од промената на телекомуникациите, која на средина на конференцијата беше поткрената на високо ниво, во однос на можните закани кои можат да следат.

1998 година, се одржал повторно форум, но ваквиот тек на состанување и дискутирање на форумите се менува во -

2001 година, поради ``9/11`` терористичките случувања и дотогаш воспоставените стратегии го менуваат текот на менаџирање во телекомуникациискиот сектор, а со тоа во -

2002 година е потпишан акт со кој се менаџира домашната безбедност на проток на информациите на земјите членки на ``ITU``- Меѓународната унија за телекомуникации, поради позачестените упади во компјутерските системи.

2004 година, донесен е закон за разузнавачките реформи и тероризмот и како да се превенира од ваквите закани.

---

[98] Internet Growth Statistics – Global Village History, http://internetworldstats.com/emarketing.htm
[99] Marshall McLuhan Foresees The Global Village, http://livinginternet.com/i/ii_mcluhan.htm

2006 година, се прави нова ревизија на ITU- Меѓународната унија за телекомуникации- Уставна Конвенција,на која се донесува сет на нови мерки кои во

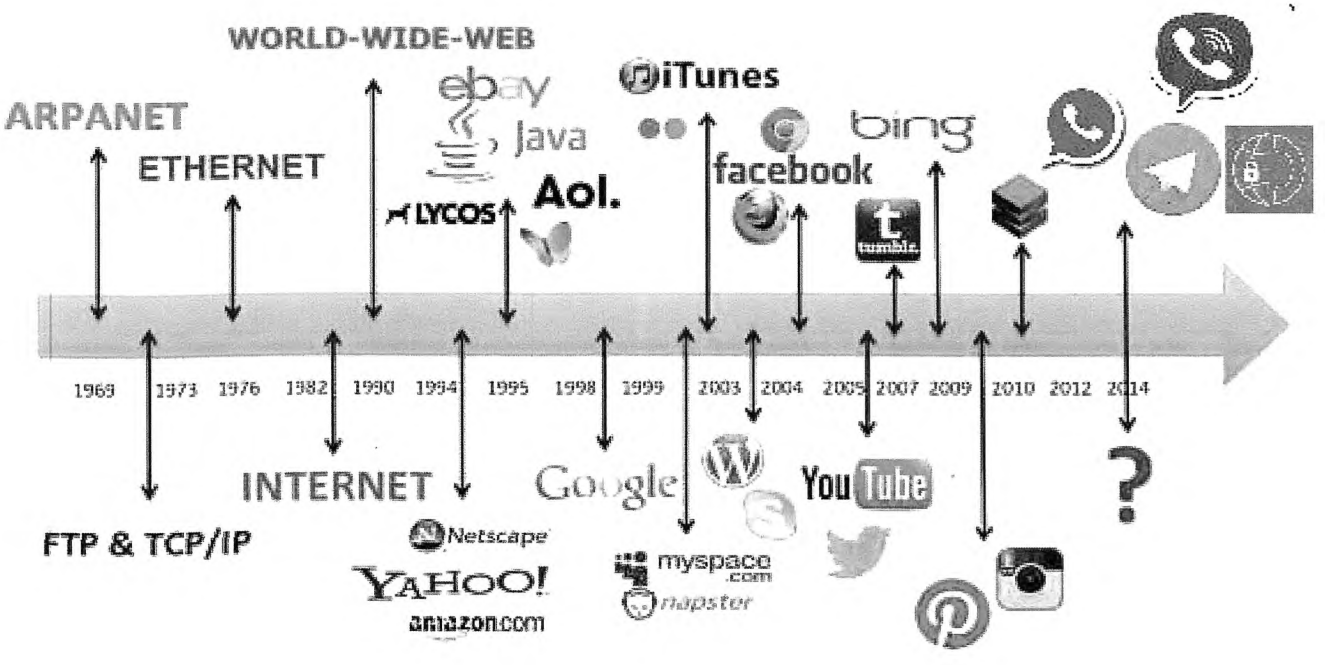
2007 година, овој акт на нови мерки е во насока за заштита на компјутерскиот систем и заштита од сајбер напади.

2008-2010 година, закани од компјутерски криминал

2011-2013 година, закани од сајбер војна

2014 ... год., закани од високо-технолошки тероризам

Во однос на развојот на комуникацијата која е достигната или нејзиниот еволутивен приказ може да се прикажат сите апликации, кои се појавуваат, а преку кои исто така се овозможува еден развој на телекомуникациите кој денес е доста актуелен, и кој својата примена ја има кај милиони корисници, на кои им се нудат многу можности и истата бележи раст.



Графички приказ на развој на комуникации

1.1. Интернетот како глобална мрежа

Во денешно време незамисливо е користење на компјутерите без истите да се поврзани во систем со друг компјутер. Изградбата на компјутерската мрежа, а со тоа настанокт и развојот на интернетот и неговите услуги кој ги пружа преку веб страните доведува до изразито значајно проширување на кругот на корисници на компјутери и промена на улогата на компјутерот во однос на она што тој уред беше некогаш.

Појавата на современите компјутерски мрежи доведе до револуција слична на онаа на појавата на првата парна машина која се појавува во XVIII век. Компјутерската мрежа е систем кој се состои од збир на хардверски уреди меѓусебно поврзани со комуникациска опрема, обезбедена со соодветен контролен софтвер кој овозможува функционирање на системот така што преносот на податоците се одвива помеѓу компјутерските уреди. Основната улога на компутерската мрежа е:

Комуникација- со користењето на компјутерите луѓето денес комуницираат по пат на електронска пошта, брзи пораки, видео комуникација итн.

Споделување информаци и податоци – во мрежното опкружување можно е да се пристапи до информациите кои се наоѓаат на друг компјутер со помош на мрежно поврзување, но преносот на информациите може да се врши и во рамки на локана мрежа, а тоа е случај во работењето во рамките на една компанија, но не е исклучок и во рамки на светската глобална мрежа.

Споделувањето на софтвер – корисниците поврзани во мрежа можат да користат многу услуги кои го пружа самиот софтвер кој работи во функција на самиот компјутерски уред во рамки на мрежна поврзаност. На пр: преку веб страните можат да се купат, резервираат карти за авионски, автобуски, возен и бротски превоз, да се испорача стока од производни фабрики или продажни места и сл.

Споделување хардверски ресурси – во мрежното опкружување, можно е заедничко користење на хардверот, на пр: штампач, скенер, од стана на многу корисници кои мрежно се поврзани со базниот компутерски уред. Компјутерските ресурси во мрежа можат да бидат расопредени на различни начини со што би можело да се обезбедат различни начини на извршни функции.

Денес најкористена и најпопуларна мрежа која е составен дел од секој компјутер е интернетот. Почетоците на интернетот како мрежа ги сретнуваме во доцните 50-ти години (1950 год.) кога Американското Министерство за одбрана (eng. Department of Defence-DoD) започнува проект за креирање на национална компјутерска мрежа која би продолжила да функционира и во можното пост-апокалиптично време, па дури и доколку нејзин голен дел биде уништен во нуклеарна војна или природни катастрофи. Во овој период основната воена комуникација се одвива преку телефонски мрежи што се смета дека се доста ранливи од можни закани, па за таа цел во 1960-те години DoD за сопствени цели ја ангажира RAND корпорацијата чии член Пол Баран

(eng.Pol Baran) како решение на овој проблен предлага да се користи дигитално пакетно комуницирање (Packet-Switching). Во октомври 1957 година, како одговор на Руското лансирање на сателитот „ спутник„ тогашниот претседател на САД Давид E.(eng. Dawight David Eisenhower)[100] ја основа ARPA (eng. Advanced Research Project Agency)[101] агенција чија основа задача е сумбвенционирање на истражувачки проекти на тоа поле. Во 1967 година тогашниот директор на ARPA одлучува да една од основните функции на ARPA биде инвестирање во коминкациите. Ваквиот проект дава големи резултати, па така Лари Робертс-програмски менаџер и директор (eng. Larry Roberts)[102] одлучува да изгради мрежа која денес е позната под името ARPAnet која всушност е првиот програмски безбеден комуникациски пакет-мрежа (store-and-for world- packet-switching)[103] која многу брзо расте и се развива, па така ARPAnet и понатаму продолжува да функционира и финансира на истражувачки проекти на поле на сателитската комуникација и радио мрежа.

Денес интернетот е најголемата и најзначајната мрежа која е составен дел на секој компјутер или комуникациски уред. Интернет мрежата поврзува голем број компјутерски мрежи и компјутери низ целата планета. Со оглед на тоа што сам посебе интернетот е доста комплексен поим тешко е да се дефинира во една единствена дефиниција. Во литературата во однос на опишување и дефинирање на поимот можат да се сретнат *два пристапи* и тоа *структурен и функционален пристап.*

Според *структурниот пристап* интернетот се дефинира преку хардверските, комуникационите и софтверски компоненти кои го сочинуваат, и според овој пристап интернетот е (WAN-Wide Area Network) компјутерска мрежа[104] која поврзува мноштво мали приватни и јавни мрежи, кои меѓусебно комуницираат. Комуникациските канали се изградени од голем број различни физички комуникациони технологии (различни врсти на кабли,безични врски,сателитски).

Според *функционалниот пристап* интернетот се дефинира преку услугите кои ги нуди на своите корисници, па отука интернетот е мрежна инфраструктура која овозможува работа со дистрибуирани апликации кои ги користат корисниците. Овие апликации го вклучуваат и WWW-(eng.World Wide Web)[105]кој им овозможува на корисниците целосен преглед на хипертекстуалните документи, електронска пошта-(eng.E-mail), пренос на податоци, испраќање брзи пораки итн. Сите овие апликации меѓусебно поврзани комуницираат преку своите специфични протоколи (пр: HTTP,SMTP,POP3…), а пак сите апликациони протоколки пак комуницираат преку два транспортни протоколи: TCP-кој е протокол за воспоставување на конекција кој гарантира дека податоците кои се испраќаат ќе бидат доставени исправно во целост и со редослед по кој се пратени, и UDP-кој е протокол без воспоставување конекција, и кој не дава никаква гаранција и сигурност за преносот на податоците. Како расте

[100] https://en.wikipedia.org/wiki/Dwight_D._Eisenhower
[101] http://searchnetworking.techtarget.com/definition/ARPA
[102] https://en.wikipedia.org/wiki/Lawrence_Roberts_(scientist)
[103] http://www.packet.cc/files/ev-packet-sw.html
[104] http://searchenterprisewan.techtarget.com/definition/WAN
[105] http://searchcrm.techtarget.com/definition/World-Wide-Web

бројот на компјутерски уреди поврзани со интернет мрежа, така расте и бројот на компании кои нудат он-лајн информации, а со тоа расте и бројот на корисници на веб страните, па така интернетот денес овозможува повеќекратни услуги:

Информација и тоа преку www-*world wide web* (споредливо со консултирање на дигитална библиотека), и *новински групи* (споредливо со списанија посветени на различни теми). Новинските групи кои се големи комуникациски системи преку кои луѓето со различни интереси разменуваат информации. *Блогот*[106] која денес преставува најсовремената апликација која својата популарност ја гради врз основа на лесната организација која не бара програмско знаење е еден вид он-лајн дневник со различни видови информации, вести и лични исповеди.

Комуникација преку праќање и примање писма; програма за разговарање (преку дирекна врска слична на телефонски разговор)[107]; електронска пошта (E-mail)[108]; конференции преку дирекна и истовремена врска помеѓу повеќе корисници во реално време;

Отука произлегува и едно од можните дефинирања на интернетот кој всушност може да се поима како глобална поврзна компјутерска мрежа, т.е децентрлизирана мрежа зад која не постои ниту една институција или држава која управува со нејзината работа. Интернетот како таков денес е само логистички подржан и финансиран од страна на компании кои имаат пристап до него, а неговата организација од гледна точка на техника е надгледувана од комисија наречена ICANN-Internet Corporation for Assigned Names and Numbers [109](Интернет корпорација за назначени имиња и броеви).

Интернетот нуди многубројни можности кои ги надминуваат границите на традиционалните медиуми. Интернетот е организирана алатка, алатка за групите во организирањето и координирањето на нивните активности, а со тоа значи и зголемен пренос на информациите, одошто дотогаш постоечките медиуми. Интернетот и се она што денес го овозможува информацискатa и информатичката технологија има импресивни економски и социјални ефекти во повеќе области кои се клучни за функционирање на општеството и тоа во делот на државната управа, научно истражувачката работа, здравствената заштита, националната безбедност и одбрана.

Со наглата експанзија на интернетот се потврдува и фактот дека технологијата може да биде и оперативна и опасна. Пропагандниот ефект на наглата интеграција на

---

[106] Македонската веб-блог услуга, http://blog.com.mk

[107] Оваа услуга овозможува комуникација во реално време преку впишување на пораки на тастатура. Виртуелната средина за дискусии е комуникациски „канал„ или „ соба за разговор„ што создава виртуелен простор за средба каде голем број корисници комуницираат истовремено (Yahoo Massenger, MSN Massenger …)

[108] Порака која се нарекува и-маил преставува пишан текст на кој корисникот може да прикачи слики, звуци, апликации и други видови документи.

[109] https://www.icann.org

интернетот во сите аспекти на човековото живеење е токму зголемената ранливост на современото општество.[110]

1.2. Сајбер простор

При самото дефинирање на поимот за „Сајбер простор„ може да се уочи дека станува збор за израз составен од два збора кои сами посебе преставуваат поединечни термини во процесот за нивно дефинирањето. За да може соодвето да се определи самото зачење најнапред мора да се тргне од дефинирање на поимот „сајбер„ и поимот „простор„.

Поимот „Сајбер„ честопати се поврзува со зборот „кибенетика„ па отука во секојдневната пракса доаѓа до недоразбирање околу терминот „сајбер„ и „кибер„.

Зборот „кибернетика„ потекнува од старогрчкиот збор „kibernao„ кој во превод би значело управување во општа смисла на зборот. Под кибернетика американскиот математичар Норберт Винер подразбира цела област на теории за управување и комуникации.[111]

Наспроти ова префиксот „сајбер„ укажува на исклучително сложена интеракција, неограниченост во просторот и неограничен број на услуги кои постојано се сретнуваат во нешто ново и неочекувано во светот на компјутерската мрежа.

Корените на поимот „сајбер„ прв пат во вовел Вилијам Гибсон[112] во 1984 година во својата позната невела „Neuromancer„. Во оваа новела В.Гибсон сајбер просторот го опишува како акумулирана можност на светот на компјутерскиот систем.

Сајбер просторот е теоретски простор во кој податоците можат да се складираат, пренесуваат и реконфигурираат.

Под сајбер простор се подразбира и врста на заедница составена од мрежно поврзани компјутери во кој елементите се класични друштва, изразени во облик на битови и бајтови, односно простор кој ја креиреаат компјутерската мрежа.

Сајбер просторот преставува термин кој го означува on-line светот на интернетот на компјутерската мрежа, но во дигиталниот свет/општество.

Сајбер просторот ги опфаќа сите облици на умрежување и дигитални активности. Во суштина сајбер просторот е вештачка творба настаната како резултат на друштвените потреби и технолошките иновации.

---

[110] Kurbalija, J., *Uvod u upravljanje internetom,* Drugo izdanje, Albatros Plus, Beograd, 2011, str.70

[111] http://www.livinginternet.com/i/ii_wiener.htm

[112] Gibson, William. *Neuromancer*. ACE, July 1984. p. 243-244

Сајбер просторот преставува нова форма на јавно место кое овозможува слободно движење на комуникацијата за разлика од физичкиот простор во кој има одредени димензии, граници, збиеност и други ограничувачки фактори.

Томас Ериксон смета дека сајбер просторот преставува „нешто„ квалитативно ново, налик на некоја врста бесконечен весник или некоја врста на голема библиотека.[113]

2. Интернетот и безбедноста

Загрозувањето на безбедноста на интернет, односно на одредени сервиси на интернет (веб сајтови, друштвени мрежи, форуми) во последно време зазама голем замав поради што се истакнува квалитативниот и квантитативниот аспек на оваа проблематика. Тоа е пред се нормативно и безбедносно, но и техничко-технолошко и глобално прашање, за кое сеуште не постои универзално усогласеност на субјекти кои на одреден начин ќе го полагаат правото на интернет.

Интернетот е замислен како средство кое ќе се користи во затворни кругови, првенствено помеѓу научни и експертски кругови кои не се оптоварени со проблемот за безбедност воопшто, а комуникацијата која се одвива помеѓу нив е отворена, а проблемите во однос на безбедност и интернетот се одвиваат на неформален начин.

Сајбер безбедноста својот почеток го има од моментот кога почнува наглата експанзија, а од тогаш се јавува и потребата за сериозно пристапување кон проблемот за безбедност на интернет.

2.1. Информациска безбедност

Различниот степен на општествено-економскиот развој и различниот степен на развој и примена на современите и инфомациски техологии, доведе до најизглед дијаметрално спротивни стојалишта во сфаќањето на поимот информациска безбедност.

Информациската безбедност се јавува не само како еден од облиците на безбедност на национално и глобално ниво, туку и како пресек на сите облици на безбедноста во кои инфоматичките техологии завземаат важно место. Доктрината за инфомациската безбеднос има широко значење, па оттука и самиот поим инфомациска безбедост во различни контексти има различно значење.

[113] http://personalpages.manchester.ac.uk/staff/m.dodge/atlas/atlas_chapter_5.pdf

Постојат *три фази* кои се клучни при техниката за следење и откривање на сајбер терористички активности, а кои се базирани на моделот на трагата.

Првата фаза се однесува на траги од класификација по претрага на клучен збор. Клучниот збор може да биде наведен и во самото URL –адресно пребарување каде системски се прикажува некакво значење - клучен збор на лице, група, организација, концепт, идеологија, критична инфраструктура, акција, работење и сл.

Ваквиот процес на систематизација може да доведат до следење на видовите на клучни зборови врз основа на значењето и така да се дојде до одредено сознание.

Втората фаза се однесува на траги од референци и поврзувања. Главната цел на овој процес во оваа фаза е добивање на целосни траги од активности од можен сајбер терористички напад.

Во однос на *третата фаза*, тука трагите се тесно поврзани со втората фаза каде можат да се проверат одредените референци и со истите да се направи првично поврзување како би се идентифукувал можниот сајбер терорист/тероризам или осомничен. Во понатамошната постапка при верификацијата се користи шемата на трага. Овој процес може да се престави и во равенство:[190]

Каде што:

a = атрибут

TK = видови на клучен збор

CcT = Сајбер тероризам

n = број

$$IF\ (an = TKn)\ THEN\ (TKn = CcTn)$$

[190] http://ijns.jalaxy.com.tw/contents/ijns-v18-n6/ijns-2016-v18-n6-p1034-1040.pdf

Шеста глава

1. Аспекти за одбрана од високо –технолошкиот тероризам

Како важени аспекти кои се истакнуваат во делот на одбраната од високо-технолошкиот тероризам е самата одбрана од сајбер напад во било кој облик кои е потенцијал за ваков вид на тероризам. Поради ваквата тенденциозна закана која е во пораст потребно е да се истакнат неколку важни насоки :

- Едукација и подготовка на професионален кадар за одбрана и детектирање на високо-технолошки тероризам. Во овој дел посебно се истакнува потребата од едукација и поткревање на јавното мислење кај населението поради подигање на јавната свест во делот на можните закани кои можат да произлезат во целокупниот сајбер простор, а кои пак ќе бидат потенцијал за извршување на високо-технолошки тероризам;
- Потеребата од обезбедување на финансиска подршка од државата за детектирање и спречување на високо-технолошки тероризам и истражувачка работа во делот на сајбер безбедноста, преставуваат битен аспект кој што поскоро треба и мора да се реализира во рамки на сите современи држави, а тука не се исклучува и Република Македонија, кога говориме за градење на безбедносни стратегии на национално ниво;
- Битен аспект е издвојување и зголемување на потребни ресурси и нивно правилно искористување и насочување во делот на сајбер форензиката, вклучувајки ја и дистрибуцијата на honeypost како компјутерска или сајбер замка, заради неопходност во понатамошната анализи;
- Анализа на ресурсите со кои располага државата и проценката на готовност во делот на целосна и навремена одбрана од високо-технолошки тероризам е од посебно значење не само на национално ниво, туку со заема кординација и соработка преминува и во рамки на регионално, и на глобално ниво;
- Неопходно е да се има „Тим за одговор на инциденти од високо-технолошки тероризам„ односно заедничко тело/орган кое би координрало одговорно на национално ниво. Националниот тим за одговор од сајбер терористички инциденти го сочинуваат група експерти за информациска безбедност, експерти од областа на тероризмот и безбедноста, кои ќе го проучуваат, анализираат, следат начинот на ранливост/закана, на компјутерскиот систем, и давање информации и обуки заради подобрување на националната безбедност;
- Размена на информации и соработка помеѓу приватниот и државниот сектор, поради поефикасно и навремено координирање како во делот на препораките, иницијативите, и законската регулатива кои би ги обезбедиле, би пружиле одредена мер на заштита на информациите и општо на целиот систем;
- Како битен аспект се наведува и тоа, да современите држави бидат на низок степен на целосна зависност од информатичката технологија, а тоа би се постигнало преку обуки, регулативи и слично, бидејќи таквата зависност само доведува до потенцијална закана како на индивидуално така и на национално ниво;

- Доста важно е имплементирање на високо структурна независна технолошка заштита или позната како Firewall – „огнен sид„ мрежен безбедносен систем, кој ги контролира дојдовните или појдовните податоци во мрежниот сообраќај врз основа на збир на правила, истиот софтвер се користи како филтер за ауторизирани корисници со помош на користење лозинка за идентификација за самиот корисник, енкрипција која спречува откривање и превзенање на податоци, бекапување и рикавери опција кои се значајни во случај да сите бариери се пробиени и уништени или самите податоци модифицирани;[191]

- Поставуавње на сензори- тоа произлегува од потребата да се контролира целокупниот сајбер сообраќај, бидејќи во него станува збор за големо количество на податоци, а кои преку сензорите снимени, во корелација, фузија и визуелизација можат да бидат корисни во лоцирање на самиот проблем. Сензорот, уред или програм кој реагира и снима одредени случувања, во случај на мрежниот сообраќај и компјутерската мрежа во целост сигнализира на одредени дејствија кои преку нивна анализа би дошле до одреден степен на детекција на проблемот, и доколку е можно негово навремено прекинување. Ваквиот сензор- уред или програм го има во повеќе видови кои имаат различни функции како што се снимање, филтрирање, прибирање и алармирање;[192]

- Перманенатно следење на сите новини и напреднувања на високата технологија, а со тоа и можните закани проследени со интернет пристапот како глобална мрежна подршка за сите превземени активности кои истат ги пружа.

Засега постојат неколку такви организации на интернет кои надгледуваат и обелоденуваат релевантни трендови и закани во доменот на компјутерската безбедност, како на пример се истакнува Computer Emergency Response Team- CERT [193] и Internet Storm Center[194]. Здружената асоцијација за анализа на податоци на интернет (Cooperative Association for Internet Data Analysis – CAIDA)[195] е исто така организација која обезбедува алатки, и обезбедува резултати врзани за надгледување на интернетот, во ова е вкучена и Европската Унија (ЕУ), која работи на проектот (Large-scale Monitoring of Broadband Internet Infrastuctures – project - Lobster 2007) за надгледување - следење на интернет инфрастуктурата.[196]

---

[191] Janczewski L., Colarik A., *Cyber Warfare and Cyber Terrorism*, IGI Global Hersey (USA), 2008, p. 250
[192] Idem., p.274-276.
[193] http://www.cert.org
[194] http://www.isc.sans.edu/
[195] http://www.**caida**.org/
[196] http://www.ist-lobster.org

2. Заштита од можните заканите во делот на критичната информацискатa инфраструктура

Во делот на критичната инфраструктура сите ресурси, системи, мрежи (физички и виртуелни), со чие уништување или онеспосување може да доведе до ослабување на националната безбедност, економската стабилност и на другите аспекти од нормативното функционирање на општеството.

Критична информациска инфраструктура подразбира услуги, компјутерски мрежи и други системи базирани на информатичка технологија значајни за секојдневното фунционирање на државите. Вака поставена и дефинирана таа преставува потесен поим од критичната инфраструктура т.е преставува негов составен дел, а може да биде и во државниот и во приватниот сектор.

Заштитата на критичната инфраструктура се дефинира како стратегија, политика и спремност на современите држави која е неопходна за да може во обратна насока да спречи или даде одговор во случај на напад на критичната инфраструктура.[197]

Мануел Сутера за заштита на критичната информациска инфрастуктура на национално ниво (Generic National Framework For Critical Information Infrastructure Protection)[198] наведува четири базни задачи:

- Превенција и рано предупедување;
- Откривање;
- Реакција;
- Управување со криза;

Со примена на ваквите базни задачи може со сигурност да се делува во насока на заштита на критичната инфраструктура на национално ниво во современите држави.

[197] Lewis G., Critical Infrastructure Protection in Homeland Security – Defending a Network Nation, John Wiley & Sons Inc. Hoboken, New Jersey (USA), 2006. p.4

[198] Suter M., A Generic National Framework For Critical Information Infrastructure Protection, Center for Security Studies, ETH Zurich, 2007.

2.1. Меѓународни организации и форуми

Со глобалната, меѓусебно поврзана компјутерска мрежа, се наметнува и потребата од глобана поврзаност и во делот на решавање на проблемите од заштита на критичната информациска инфраструктура како во делот на високо-технолошкиот тероризам, сајбер војувањето, високо-технолошкиот криминал и сите други закани кои дирекни или индирекно можат да влијаат како закана на национално ниво на современите држави. Во овој дел, многу меѓународни организации и форуми, превземаат рани активности, низ разни иницијативи, директиви, упатства, и препораки а со помош на национални организации и органи, за да можат навремено да превенираат, предупредат, откријат, или во случај на веќе нанесена закана да реагираат или пак да управуваат со оваа криза. На меѓународен план се превземаат бројни активности, во делот на заштита на критичната информациска инфрастуктура, првенствено од стана на Европската Унија, Обединетите нации, Група 8, Организацијата за економска соработка и развој, Форум за одговор на инциденти и безбедносни тимови и други меѓународни организации и форуми кои во основа им е ваквиот домен на работа, или пак заштитат на критичната информациска инфрастуктура им е само дел од мерките, стартегиите кои ги превземаат во нивна надлежност за решавање.

2.1.1. Европска унија (European Union)

Од страна на Европската Унија се превземени голем број на активности во делот на заштитата на критичната информациска структура се со цел да се зголеми нивото на нивната безбедност.

Акцискиот план, усвоен на 30.03.2009 година од страна на Европската Комисија е базирана на пет столба:

- ✓ Спремност и превенција;
- ✓ Детекција и одговор;
- ✓ Ублажување на последиците и одговор од нив;
- ✓ Меѓународна соработка;
- ✓ Критериуми за европската критична инфраструктура во областа на информациско-комуникацискатa технологија;

Планираните активности во акциониот план се само дополнувања на „ Европската програма за заштита на критичната инфраструктура„- (European Programme for Critical Infrastructure Protection - EPCIP). Како клучен елемент во Европската програма за заштита на критичната инфраструктура е „Директивата од советот за идентификација и означување на европската критична инфраструктура„ (Council Directive on the identification and designation of European Crtitical Infrastructures) кој експлицитно

нагласува дека информатичко комуникацискатa технологија како сектор е дел од критичната инфраструктува воопшто на која треба да се посвети поголемо внимание за да може навреме да се заштити.

Сите предложени активности во овој дел се усогласени и со работата на полицијата и правосудните органи во откривањето, спречувањето и процесуирањето на криминалните и терористичките активности кои имаат за цел да нанесат штета или целосно да ја онеоспособат критичната инфраструктура.

Европската Комисија на 31.03.2011 година, го усвои соопштението за „Достигнувањата и следните чекори: кон глобалната сајбер (компјутерска,кибер...) безбедност (Achievements and next steps: towards global cyber-security–COM(2011) 163). Во соопштението се опишани понатамошните чекори кои ќе бидат превземени во секоја акција на Европски и меѓународен план. Во глобални рамки фокусот е ставен на меѓусебната соработка на државите членки на Европската Унија и на приватниот сектор на национален, европски и меѓународен план.[199]

Во периодот од 27-ми до 28-ми Април 2009 година, во Талин-Естонија одржана е Министерска конференција на ЕУ на која беа дадени некои препораки и директиви околку заштитат на критичната инфраструктура. Фокусот на оваа конференција е ставен во меѓусебната соработка и напредок на Европската Унија и земјите членки на ЕУ да во заедничка кординација го поткренат нивото на безбедност, спремност и еластичност на критичната информациска инфраструктура. Констатирано е дека пред се работи и на подобрување и зголемување на координацијата и соработката со подршка на „ Агенцијата за европска мрежа и информациска безбедност",(European Network and Information Security Agency – ENISA),[200] која е формирана се со цел да обезбеди висок степен на мрежна и информациска безбедност на ниво на Европската Унија. Покрај мрежата ENISA, значајна улога во заштитата на критичната информациска инфраструктура на ниво на Европската Унија има и „Информационата мрежа за предупредување на критичната инфраструктура" (Critical Infratructure Warning Information Network – CIWIN)[201], која им помага на земјите членки на ЕУ, институциите на Европската Унија, корисниците и операторите за заштита на критичната инфраструктура, да разменуваат информации за можните закани, ранливоста се со цел да можат да превземените мерки и стратегии за намалување на ризикот и целосна заштита на критичната инфраструктура.

Стратегијата за сајбер безбедноста на Европската комисија од 2013 година е сеопфатен документ за политиката на Европската унија во оваа област. Во својот составен дел стратегијата ги опфаќа вантрешниот пазар, правдата, внетрешните работи

---

[199] Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - ``Achievements and next steps to wards global cyber – security`` - COM (2011) 163;
http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

[200] European Union, Ministerial Conference on Critical Information Infrastructure Protection, Tallinn, 27-28 April, 2009, https://www.enisa.europa.eu/about-enisa

[201] https://**ciwin**.europa.eu/

и сајбер просторот од димензија на надворешната политика. Стратегијата е проследена со законодавниот предлог се со цел да се зајакне безбедноста на информатичките системи на ЕУ. Сето ова вако поставено води кон потикнување на земјите во насока на зголемен економски раст во однос на растот на довербата во он-лајн купувањето и користењето на интернетот како механизам за олеснување на секојдневното делување.

Стратегијата јасно ги наведува приоритетите на меѓународната политика за сајбер простор на ЕУ и тоа:

- слободата и отвореноста,
- ЕУ-законите, нормите и основните вредности кои се применуваат како во сајбер просторот така и во физичкиот свет;
- развојот во градењето на сајбер бебедносносните капацитети и
- потикнување на меѓународната соработка во сајбер просторот.

Во Стратегијата за сајбер безбедноста на ЕУ[202] јасно е зацртана визијата на Европската унија да обебеди силна и ефективна заштита и промоција на правата на гараѓаните за да ја направи он-лајн средината на ЕУ најбезбеден свет во кои би цилкулирале сите општествени потреби.

За исполнување на оваа стратегија во својата политика Европската унија[203] обврзува задолжителни пет стратегиски приоритети кои се клучни во исполнуавњето на државите членки и тоа:[204]

1. Постигнување на сајбер отпорност- со зголемување на способностите, соработката, размената на информации, подготвеност и подигање на свеста во областа на мрежната и информацискатa безбедност за јавниот и приватниот сектор и на национално ниво и на ниво на ЕУ;
2. Драстично намалување на сајбер криминалот- преку зајакнување на стручноста на оние кои се задолжени за истражување и гонење на овие казнени дела, со донесување на поокординиран пристап помеѓу спроведувањето на законот во рамки на ЕУ, како и преку подобрување на соработката со другите актери.
3. Развој на сајбер безбедносната политика и способностите поврзани со заедничката безбедност о одбранбената политика на државите.
4. Развој на индустриските и технолошките ресурси за сајбер безбедност за да имаат корист од дигиталниот пазар, кое ќе помогне да се стимулира појавата на европската индустрија на пазарот за обезбедување на информатичко-комуникацискатa технологија, а тоа ќе придонесе за раст на конкурентноста на економијата на ЕУ.
5. Воспоставување кохерентна меѓународна политика на сајбер просторот на ЕУ и промовирање на основните вредности на ЕУ-дефинирање на нормите за

[202] http://ec.europa.eu/digital-single-market/en/cubersecurity
[203] http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf
[204] http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf

одговорно однесување, заложби за примена на меѓународното право во сајбер просторот и да им се помогне на земјите надвор од ЕУ во градењето на сајбер безбедносните капацитети.

За да се одговори на сајбе напдите улогата и одговорноста имаат три клучни столба во ЕУ:

- ✓ Мрежата и информацискатa сигурност;
- ✓ Органите кои го спроведуваат законот;
- ✓ Одбранбените агенции.

За таа цел градењето на капацитети во трети земји се приоритети за кои ЕУ во наредните години ќе настојува за силна врска на одржлив развоја преку IPA (Instrument for Pre-Accession Assistance)[205] како инструмент за претпристапни помош на земјите кандидати и потенцијалните кандидати за членство во ЕУ.

2.1.2. Обединети нации (United Nations)

Од самото формирање до денес основна цел и структура на ООН е да го одржи светскиот мир, и за таа цел тие служат како симбол за меѓународниот поредок и глобалниот идентитет, унапредувајќи и кординирајќи ги економиите и општествениот поредок на земјите во развој.

Генералното собрание и Советот за безбедност во чии состав се на ООН, при одржување на годишните седници ја истакнува зголемената зависност на владите, компаниите и др. Организации и индивидуални корисници на информатичката технолоција и за таа цел на 31 Јануари 2003 година донесоја резолуција (57/239)[206] за создавање на глобална култура на сајбер безбедност.

Истакнувајки ја работата на релевантните меѓународни и регионални организации во насока на подобрување на сајбер безбедноста и сигурноста на информациските технологии земјите членки ја признаа потребата за зголемување на сајбер безбедноста.

Земајќи ги предвид елементите приложени во оваа резолуција, се со ел да се создаде глобална култура на сајбер безбедност од сите учесници се бара да се водат од следниве девет комплементарни елементи:

- ✓ Свеста- учесниците се одговорни за безбедност на информациските системи и мрежи на начин на кој одговара на нивните индивидуални улоги во цел тој процес, со цел за изнаоѓање на механизми за поголема безбедност.
- ✓ Одговорност- учесниците треба да ги разгледуваат сите политики, практики, мерки и постапки секојдневно за да се оцени дали тие се ссоодветни за нивната животна средина

[205] https://sr.wikipedia.org/wiki/IPA_fond
[206] https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf

- ✓ Одговор- учесниците е потребно да ја споделат информацијата за закани и слабости како што е соодветно и брзо спроведување на постапки за ефикасна соработка за спречување и откривање како одговор од безбедносни инциденти. Ова може да вклучи и регионална и меѓународна размена на информации.
- ✓ Етика- учесниците треба да ги почитуваат легитимните интерси на другите учесници, превземајќи или признавајќи дека нивното дејство или неактивност може да наштети на другите.
- ✓ Демократија- За безбедноста треба да се спроведе и начин на согласност со вредности прифатени од демократските општества, вклучувајќи ја и слободата на информации, мисли и идеи, преку соодветна заштоита на личните податоци, отвореност и транспарентбост.
- ✓ Проценка и ризик- сите учесници треба да вршат периодичен ризик-проена кои се идентификуваат и како закана или слабост;
- ✓ Безбедносен дизајн и имплементација- учесникот треба да ја вклучи безбедноста како суштински елемент во палнирање на дизајн, функционирање и користење на информациски системи и мрежи.
- ✓ Управување со безбедноста- учесникот треба да усвои сеопфатен пристап за управување со безбедноста врз основа на проценка на ризикот кој е динамичен и ги опфаќа сите нивоа на активности на учесниците и на сите аспекти во нивното работење.

Значајна улога во рамките на Организацијата на Обединетите Нации имаат „Оперативните сили за информациско-комуникациска технологија„ (United Nations Information and Communication Technologies Task Forces – UN IGT TF)[207], кои се формирани Ноември 2011 година, а основна намена им е на владите на современите држави и на меѓународните организации им обезбеднат соодветна политика за надминување на „дигитален јаз„ на глобално ниво.

Меѓународната унија за телекоминукации (International Telecommunication Union – ITU)[208], со седиште во Женева и во која членуваат преку 190 земји, е специјализирана агенција на Обединетите Нации, одговорна за информациско-кумуникациската технологија.

Меѓународната унија за телекомуникации во свој домен превзема бројни активности се со цел да ја подобри комуникациската инфраструктура, развојот на меѓународните стандарди, размената на идеи, знаење и технологија.

[207] http://www.un.org/en/ecosoc/docs/report.asp?id=1132
[208] http://www.itu.int/en/Pages/default.aspx

2.1.3. Група 8 (G-8)

Во однос на заштитата на критичната информациска инфраструктура значаен документ прставуваат „Принципите за заштита на критичната информациска инфраструктура„ (G8 Principles for Protecting Critical Information Infrastructures),[209] преку кој се препорачува да:

- Државите треба да имаат мрежи за алармирање/предупредување во врска со сајбер слабостите, заканите и инцидентите;
- Државата треба да работи на поткревање на свеста на корисниците но за да се олесни разбирањето на природата и степенот на загрозеност на нивната критична информациска инфраструктура, како и улогата на кој начин истите би биле во функција на заштита на истата;
- Државите треба да ја проверат нивната инфраструктура и да се идентификува меѓузависноста меѓу нив со другите, а со тоа би се постигнало подобрување и заштита на инфраструктури;
- Државите треба да промовираат партнерство помеѓу засегнатите страни, како јавни така и приватни, да се споделат и да се анализираат критичните информации за инфраструктурата се со цел да се спречи, да се истражи и да се одговори на оштетувањата или на нападите на таквите инфраструкти;
- Државите треба да создаваат и одржуваат криза во комуникациската мрежа, да ја тестираат дали истата би останала стабилна и безбедна во итни ситуации;
- Државите треба да превземат мерки дека, актуелните политики и другите мерки кои се применуваат за заштита на критичната информациска инфраструктура се применуваат;
- Државата треба да помогне во следењето на нападите врз критичната информации, и каде што е неопходно да помогне на другите држави;
- Државата треба да спроведе обуки и вежби за подобрување на способностите за одговор, да спроведува тестирања за функционирање на плановите во континуитет за непредвидливите ситуации во случај на информациско инфраструктурен напад и да ги потикнува сите засегнати страни да се вклучат во слични активности;
- Државата треба да обезбеди соодветни материјали и закони, како што се оние кои се истакнати во Советот на Европа за компјутерскиот криминал од 23 ноември 2001 година, и да обучи кадар за да се овозможи истиот да ги испита и да ги осуди нападите на критичната информациска инфраструктура, и да се кординира во делот на испитување на нападите каде што е потребно со другите земји;
- Државата треба да се вклучи во меѓународната соработка, кога е неопходно, да се обезбеди критичната информациска инфраструктута, вклучувајќи го тука и развојот

[209]Принципите се усвоени 5 Мај 2003 година од страна на министрите за правда и внатрешни работи на земјите членки на Г-8;
http://www.justice.gov/sites/default/files/ag/legacy/2004/06/03/G8_CIIP_Principles.pdf
www.usdoj.gov/ag/events/g82004/G8_CIIP_Principles.pdf

и координирањето на системите за итни случаеви, споделување и анализа на информации во врска со слабостите, предупредување од можни закани, како и координирање за испитување на нападите во согласност со домашното законодавство;

- Државите треба да промовираат национални и меѓународни научно - истражувачки проекти, за развојот и потикнување на примената за безбедносните технологии кои се сертифицирани во согласност со меѓународните стандарди;

2.1.4. Организација за економска соработка и развој (Organization for Econoimic Cooperation and Development-OECD)[210]

При процесот на промовирање на културата на безбедноста на информациите и системите, во 2002 година од страна на секретаријатот на одговорните 18 –земји членки на Организација за економска соработка и развој (Organization for Econoimic Cooperation and Development-OECD) беше изготвен и усвоен извештајот за ``Насоки за безбедност на информациските системи и мрежи: кон културата на безбеднсота``. Во 2005 година во период од 19-20 мај на одржувањето на 18-от состанок на работната група за безбедност на информациите и приватноста (WPISP)[211] го изготви првиот извештај и се согласи да го финализира со писмена постапка на Комитетот за информации, компјутерска и комуникациска политика (ICCP)[212] . Во самиот извештај е даден детален опис на иницијативата за спроведување на насоките во насока на културата на безбедноста на 18-те земји членки (Австралија, Австрија, Канада, Данска, Финска, Франција, Германија, Јапонија, Кореја, Холандија, Норвешка, Португалија, Словачка,Чешка, Шпанија, Шведска, Велика Британија и САД) на Организација за економска соработка и развој, а кој е наменет во насока на поттикнување на спроведување и ширење на практични информации и најдобри практики понеѓу ОЕЦД и со економиите на земјите кои не се членки, и целосно мониторирање на националниот пристап на безбедноста на информациите;

Развојната политика за заштита на критичната информациска инфраструктура (Development of Policies for Protecting of Critical Information Infrastructure), публикувана на 18 декември 2007 година, ја прикажува компаративната анализа на политиката за заштита на критичната информациска инфраструктура во Австралија, Канада, Кореја, Јапонија, Холандија, Велика Британија и Соединетите Американски Држави.[213]

Препораките на „Комисијата за информациска, компјутерска и комуникациска политика (Committe for Information, Computer and Communication Policy – ICCP

---

[210] http://www.oecd.org/internet/ieconomy/35884541.pdf

[211] http://www.oecd.org/sti/whatistheoecdworkingpartyoninformationsecurityandprivacywpisp.htm

[212] https://www.corrosion.nl/iccp-cathodic-protection

[213] Development of Policies for Protecting of Critical Information Infrastructure, www.oecd.org/dataoecd/25/10/40761118.pdf

Committe)[214], кои беа упатени на Организацијата за економски соработка и развоја, усвоени на 30 април 2008 година, предлагаат низа мерки за заштита на критичната информациска инфраструктура на национално и на меѓународно ниво.

2.1.5. Форум за одговор на инциденти и безбедносни тимови (Forum for Incident Response and Security Teams – FIRST)

Форумот за одговор на инциденти и безбедносни тимови[215] е широко позната организација како глобален лидер во одговорите за инциденти и обединување на различни тимови за одговор на инциденти (Computer Security Incident Response Teams – CSIRTs)[216] во рамки на владите, претпријатијата и екомонските организации. Форумот за одговор на инциденти и безбедносни тимови FIRST – (Forum for Incident Response and Security Teams), е наменет да воспостави соработка и координација во превенција на инцидентите, брза реакција во случај на инциденти и промовира размена на информации помеѓу членовите и низ поширокаата заедница.

2.2. Национални организации

Направените анализи во делот на заштитата на инфраструктурата и критичната информациска инфраструктура, во многу земји евидентно покажуваат дека не постои јасна дистинкција околу овие два аспекта на заштита, а тоа се гледа и во делот на тоа дека не постојат официјални листи за критичната информациска инфраструктура на современите држави. Општествено политичките, историските, географските и другите фактори во голема мера влијаат на тоа да некои сектори на општественото делување бидат критични или не. Само некои држави како на пример САД, Русија, Франција, Германија, Велика Британија, Италија, Норвешка ..., имаат централизирани владини организации за заштита на критичната информациска инфраструктура. Во остатокот од земји, ваквата одговорност е во повеќето големи авторитети и организации во високите владини институции.

Ваквиот тренд на прашањето за раното предупредување во случај на загрозување на критичната информациска инфраструктура е во тоа да се формираат централни точки за безбедносно информациски системи и мрежи, а тоа се најчесто разни тимови за одговор на инциденти кои пред се ќе разменуваат информации во рамки и кординација со FIRST – (Forum for Incident Response and Security Teams).

---

[214] OECD Recommendation of the Council on the Protection of Critical Information Infrastructures, www.oecd.org/dataoecd/1/13/40825404.pdf

[215] Forum for Incident Response and Security Teams – FIRST www.first.org

[216] https://www.csirt.org

2.2.1. Соединетите Американски Држави

Кординативното тело за заштита на критичната инфраструктура (критична информациска инфраструктура), на Соединетите Американски Држави, е Министерството за внатрешна безбедност (Department of Homeland Security – DHS), кое е формирано во 2002 година, а се формирани врз основа на Националната стратегија за внатрешна безбедност (National Strategy for Homeland Security)[217], и Актот за внатрешна безбедност (Homeland Security Act)[218].

„Претседателската директива за внатрешна безбедност„(Homeland Security Presidential Directive – HSPD-7) [219] идентификува 17 критични инфраструктурни сектори, но поради постоење на одредени празнини во директивите, во март 2008 година формира, нов 18-ти сектор за критично производство (Critical Manufacturing Sector). За секој од осумнаесетите сектори се формирани посебни агенции (Sector-Specific Agencies) кој изготвува специфицни планови за примена на националниот план за заштита на инфраструктурата за секој сектор. Секторите на критична инфраструктура се: земјоделство и храна, комерцијални објекти, брани, енергија, информатичка технологија, поштенски и шпедитерски сектор, банкарство и финансии, комуникации, објекти за воена индустрија, владини објекти, национални споменици и обележја, транспортни системи, хемикалии, критично производство, енергетски услуги, здравствена заштита, нуклеарни реактори материјали и отпад, и вода.

Во рамки на Министерството за внатрешна безбедност постои „ Директорат за анализа на информации и заштита на инфраструктурата„ (Directorate for Information Analysis and Infrastructure Protection – IAIP), во чии состав е „ Одделението за сајбер безбедност„ наменет да идентификува, анализира и да ги намали сајбер заканите и ранливоста на целиот систем, праќа пораки за предупредување и координира во случај на инциденти, изготвува планови за безбедно функционирање на целата мрежа. Оперативното тело „ Оделението за национална сајбер безбедност„ е„Тимот за одговор на инциденти„ (US Computer Emergency Readiness Team – US CERT).

Покрај Министерството за внатрешна безбедност, значајна улога во заштитата на критичната информациска инфраструктура имаат и други федерални органи, како, Националниот институт за стандардизација и технологија, Министерството за правда, Министерството за одбрана и сл.

Во состав на Министерството за правда постои Национален центар за заштита на инфраструктурата и Федерално истражно биро кои се во постојано следење и

---

[217] National Strategy for Homeland Security, www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf

[218] Homeland Security Act, www.Dhs.gov/xlibrary/assets/hr_5005_enr.pdf

[219] Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection; http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm

кординираат по можните закани. Во рамки на Министерството за одбрана значајна улога има Агенцијата за развој на напредните истражувања од областа на безбедноста, Тим за одговор на инциденти на копнената војска, Тим за одговор на инциденти на воздухопловната снага, кој постојано се во процес на обучување, анализа и навремено координирање со другите органи на национално ниво.

Денес, со сигурност може да се каже дека свеста и напорите кои САД ги прави во насока на одбрана од високотенолошките закани е на високо ниво и цели кон нејзин напредок со самиот чин на следење на иновациите на информатичката и информацискатa безбедност.

2.2.2. Русија

„Концептот за информатичката безбедност на Руската Федреација„ е усвоен на 9 септември 2000 година, и преставува проширување на „Националниот концепт за безбедност„ на Русија, кој пак е усвоен на 10 јануари 2000 година, а кој има за цел да ја зајакне државната политика по прашањето за информацискатa безбедност на државата.

Главни организации за одговор за информацискатa безбедност во Русија се Советот за безбедност на Руската Федерација, Федералната служба за безбедност при Руската Федерација, Федералната гарда на Руската Федерација, Федералната техничка и службата за контрола на извоз на услуги, и Министертвото за информациска технологија и комуникации. За соработката на државното-приватно партнерство во Руската Федерација, надлежна е Руската асоцијација за мрежи и услуги (Russian Association of Networks and Services – RANS)[220] и Рускoто електронско партнерство за развој (Russian e-Development Partnership – PRIOR).[221] На национално ниво во Руската Федерација постои Тим за одговор на инцидент (Computer Security Incident Response Team – RU CERT).

Од сето ова, може да се констатира дека Русија е една од земјите во висок степен на развиена свест за можните закани од сајбер тероризмот. За таа цел постојаните следена на новитететитте кои сосебе ги носи информатичата доба, а и самиот факт на обучување на кадри ги носи на нивото на се повеќе спремна да одговори во иднина на овие предизвици.

[220] https://www.icann.org/en/system/files/files/rans-mou-25jun08-en.pdf
[221] http://www.iis.ru/en/directorate

2.2.3. Франција

Во Франција, Генералниот секретар за национална одбрана (Secretary-General of National Defense – SGDN), кој е во склоп на кабинетот на премиерот, има целосна одговорност за заштита на критичната инфраструктура. Во рамки на Министерството за одбрана, главни организации за одговор за заштита на критичната (информациска) инфраструктура се Централниот директорат за безбедност на информациски системи (Central Directorate for Information Systems Security – DCSSI) и советодавната канцеларија, додека централната служба за високо-технолошкиот криминал (Central Office for the Fight Against Hi-tech Crime) има главна улога во рамки на Министерството за внатрешни работи.За реализација на соработката помеѓу државниот и приватниот сектор одговорен е Стратегискиот советодавен одбор за информациска технологија (Strategic advisory Board on Information Technologies – CSTI).[222]

Франција ги користи насоките на Организација за економска соработка и развој (Organization for Econoimic Cooperation and Development-OECD)[223] како принципи за подигање на свеста кај населението и во рамки на таквата иницијативност на владата се стреми да обезбеди насоки за безбедност на информациите. Централната управа за Информатички системи за безбедност во оваа насока издаде и водич за развој на политиките за безбедност на информациите и метологии за управување со ризикот. Основната цел е насочена кон базичните три нивоа на уравување со ризикот и обезбедување на сигурност со помош на неколу безбедносни функции и тоа електронски потпис, доверливост и временски печат.

Добрата кординација и постоењето на институционална свест, Франција е на чекор на превземање на нови политики за поткревње на јавната свест на граѓаните за информацискатa бебедност како би дошло до адекватно одвраќање од секоја современа закана која може да наштети на нејзината национална безбедност.

2.2.4. Германија

Целосната заштита на критичната (информациска) инфраструктура е на Министерсвото за внатрешни работи на Германија, заедно со неколку свои потчинети агенции, како што е Федералната служба за информациска безбедност (BSI), Федералната служба за заштита на цивили и помош во несреќи (BBK), Федералната агенција на криминалистичката полиција (BKA), и Федералната полиција (BPOL). За кординација помеѓу овие агенции во 2002 година Министерството за внатрешни работи формира „Посебна единица за заштита на критичната инфраструктура„ (AG KRITIS), која е во постојана корелација со сите нив. За развојните стратегии на

[222] http://www.csti.pm.gouv.fr/uk/home-uk.html
[223] http://www.oecd.org/internet/ieconomy/35884541.pdf

државно ниво и другите активности кои се превзенаат за заштита на критичната (информациска) инфраструктура Министерството за внатрешни работи се кординираат и со другите федерални министерства како што е Федералното министерсвто за одбрана, Федералното министерство за правда, Федералното министерство за надворешни работи, Федералното министерство за економија и технологија и други релевантни министерства и агенции.

Во националната стратегија за заштита на критичната инфраструктура на Германија е наведено дека критичната инфраструктура ја сочинуваат организациони и физички структури и средства од витално значење за државата и економијата, така што во случај на прекин и деградација може да настане недостаток на напојување, значајни поместувања и последици кои директно ќе влијаат на човековата безбедност или пак би настанале други потешки последици.[224]

- Критичната инфраструктура може да биде изложена на многу закани кои можат, условна да се групираат како: Елементарни непогоди (пожари, замјотреси, епидемија, пандемија и сл.)
- Технички пропусти/ човечки грешки (системски пропусти, невнимание, опганизациски пропусти и сл.)
- Тероризам, криминал, војна и.т.н

2.2.5. Велика Британија

Во Велика Британија, како главна одговорност за заштитата на критичната информациска инфраструктура му е дадена на Секретарот за внатрешни работи, но и многу други органи имаат улога во заштитата на различни сектори. Нивната координација се врши од страна на Центарот за заштита на националната инфраструктура.[225]. Центарот за заштита на националната инфраструктура е формиран на 1 февруари 2007 година, а него го чинат двата центри, Центарот за координација за безбедност на националната инфраструктура и Центарот за советување по прашањето на националната безбедност.

Политиката за заштита на критичната информациска инфраструктура е донесена и спроведена од страна на високите владини органи и тела, вклучувајќи го и Центарот за координација за безбедност на националната инфраструктура (Centre for the Protection of the National Infrastructure – CPNI)[226], Центарот за подршка на информациско обезбедување (Central Sponsor for Information Assurance – CSIA), Кабинетот за безбедносна политика на владата на Велика Британија (Cabinet Office Security Policy

[224] National Strategy for Critical Infrastructure Protection (CIP Strategy), Federal Ministry of Interior, Federal Republic Germany, Berlin, 17 June,2009,p.4
[225] Centre for the Protection of the National Infrastructure, www.cnpi.gov.uk
[226] https://www.cpni.gov.uk

Division), Канцеларијата за внатрешна политика (Home Office), и Владиниот штаб за комуникации (Government Communications Headquarters – GCHQ).

2.2.6. Италија

Главно владино тело во Италија одговор за заштита на информацискатa инфраструктура е Министерството за внатрешни работи и Министерeството за иновации и технологија. Министерството за комуникација е исто така вклучено во различните активности кои е превземаат се со цел да се подобри информацискатa и комуникацискатa мрежа. Во остварувањето на соработката помеѓу државниот и приватниот сектор кога станува збор за заштитат на информацискатa инфраструктура и за заштитат на инфраструктурата воопшто, главна улога има Здружението на италијански експерти за критична инфраструктура (Associazione Italiana Esperti in Infrastructure Critiche)[227], т.е. тоа е експертска група на практичари во таа област од приватниот и државниот сектор.

2.3. Република Македонија против високо-технолошкиот тероризам

Република Македонија како парламентарно-демократска држава направи крупен чекор во дефинирање на основните витални вредности и изградба на сопствен автономен безбедносен систем во функција на заштита на истите. Безбедносниот систем фукционира како подсистем на вкупниот општествен систем.

Новите предизвици кои се закануваат на глобалната безбедност во поширокатa општествена заедница и по безбедноста во Република Македонија бараат единствен и моќен професионален систем кој може да одговори на истите. Од друга страна градење на еден таков систем во услови на недоволна изградена безбедносна и политичка култура преставува сериозна опасност заради концентрирање на голема моќ во рацете на мал број на луѓе или групи која може да биде злоупотребена за остварување на тесно партиско или криминални интереси.

За да зборуваме за модел на безбедносен систем кој би бил најсоодветен да одговори на новите облици на загрозување најпрво треба да се познава етиологијата на загрозувањата на овие простори како и развојот на безбедносниот систем низ историјата прилагодувајќи се на соодветните опасноси.

Безбедносниот систем во Република Македонија по осамостојувањето се конституира како систем на заштита на основните вредности, систем во функција на

[227] http://www.infrastrutturecritiche.it/aiic/

заштита на државата во интерес на заштита на правата и слободите на граѓаните на Република Македонија.

Со оглед на фактот што Република Македонија се определи за зачленување во евро-атланските интеграции потребно е прилагодување на сопствениот безбедносен систем и кон глобалниот европски безбедносен систем на кој начин и безбедносниот систем ќе биде еден од подсистемите на глобаниот систем на кој начин ќе биде способен да реагира и одговори на новите предизвици и закани. Реформите и изградбата на безбедносниот систем се одвиваат во континуитет од осамостојувањето до денес така што може да кажеме дека станува збор за еден динамичен процес кој мора да кореспондира со реалните промени во опкружувањето и сопствените потреби и можности. Имено при изградбата и реформите во безбедносниот систем треба да се има предвид неколку критериуми:

- Безбедносни потреби - реални ризици и закани
- Економско социјални можности на државата во зависност од развојот и можноста за издигнување на безбедноста
- Безбедносниот систем да биде во функција на заштита на основните вредности согласно уставот
- Прилагодување на безбедносниот систем во насока со надворешната политика и сл.

Еден од главните ризици и закани од кој стравува секоја современа држава и која всушност преставува глобален проблем е тероризмот во сите свои облици.

Кога говориме за високотехнолошкиот или сајбер тероризам како облик на закана, во Република Македонија се прават големи напори да биде адекватно анализиран и разработен со цел изнаоѓање на конкретно дефинирани аспекти кои се најчесто од правна и практична природа. Тоа значи дека правните нормативи и заклучоци со кои се осудува секој вид на терориам како непожелна општествена појава предвидуваат и конкретни мерки за дејствување против него и последиците од него.

Но сепак во Република Македонија не постои сеуште одредена законска рамка за борба против сајбер тероризмот, бидејќи многу луѓе и институции немаат одредена знаење за тоа што всушност преставува поимот сајбер тероризам и каков сериозен проблем би преставувал овој вид на тероризам.

Република Македонија ја иницираше борбата против тероризмот со учество на разни семинари и конференции кои се поврзани на темата сајбер или високотехнолошки тероризам.[228] Во изминатиот период Македонија има ратификувано и голем број на меѓународни конвенции кои се однесуваат на сајбер криминалот а кои даваат и мерки кои се тесно поврзани со високотехнолошкиот тероризам бидејќи како појава сајбер криминалот и сајбер тероризмот се тесно поврзани.

---

[228]Активности за превенција и спречување со последици ос сајбер тероризам. Министерство за информатичко општество http://www.mio.gov.mk/?q=node/1911

Во 2004 година Македонија ја ратификуваше и Конвенцијата за компјутерски криминал донесена во 2001 година од страна на Советот на Европа, како и дополнителните протоколи за криминални акти од расистичка и ксенофобична природа преку компјутерските системи, што значи дека овие меѓународни правни акти се инкорпорирани во домашното законодавство.[229]

Почетоците на ваквата закана од сајбер тероризам во Република Македонија можат да се забележат во 2008 година каде беше нападната официјалната веб страна на поранешниот Претседател Бранко Црвенковски од страна на група хакери од Косово, Албанија и Грција[230], но забележана појава од вакви напди се детектирани и од хакирани сајтови од страна на Грчки групи кон планинарски и граѓански здруженија, но и од страна на бугарски хакери кои ги напаѓаа македонските сајтови каде се дебатираше за македонскиот идентитет.

Ваквите закани ги направија Македонските државни власти посвесни за фактот дека официјалните веб страни на државните институции се ранливи на сајбер напади а поради слабата заштита тие се лесна цел. За таа цел одредени експерти од информатичката технологија пристапија кон изнаогање на соодветни решенија или контратерористички мерки и протоколи кои можат да ја одбранат или во најмала рака превентивно да делуваат на следните предизвици кои ги носи новото време

Сепак Република Македонија е помалку ранлива на овие напади за разлика од државите каде информатичката технологија е на многу високо ниво. Досегашното ниво кога станува збор за Република Македонија е на ниско ниво како и другите земји од југоисточна европа, но тоа незначи дека идните активности на влади која во своите цели го има наведено дека ќе пристапи кон дигитализација на општеството за 40-60 проценти нема да го донесе и новиот облик на закана.

Потребата и од измени во Кривичниот закон на Р.М со посебни одредби кои ќе ја регилираат терминот сајбер или високотехнолошки тероризам без двоумење и без никакво одложување е нешто што треба да се направи за Македонија да може да продолжу во насока на безбедна и демократска држава.

Во целиот овој процес на заштита од високотехнолошки тероризам, немањето на посебни институции во Република Македонија кои се занимаваат со сајбер тероризам и кои легално го истражуваат ги прави сите обиди нецелосни како и самиот поим при легалното дефинирање на сајбер тероризмот. Но сепак постојат државни институции одговорни за одредени аспекти на сајбер тероризам како на пример заштита на информатичката технологија и безбедноста во целина.

---

[229] http://www.mio.gov.mk/?q=node/191 ,и http://www.mvr.gov.mk

[230] http://www.vest.mk/default.asp?ItemID=E0813EB97B954947A3B8425ED802B375

2.3.1. Институции за борба против високо-технолошкиот тероризам во Република Македонија

Континуираната дигитализација на државните институции несомнено го подигна нивото на ранливост од високотехнолошки тероризам. Самиот сајбер простор е ``отворено море`` каде што одредени организации го користат интернетот и дигиталната сфера за терористички активности.

Бидејќи сајбер тероризмот е облик на тероризам, предвиден во Уставот на Република Македонија во кој како највисок правен акт се наведени мерки и активности за борба против сите извори на загрозување не само на суверенитетот и независнота на Република Македонија, туку и против сите извори на загрозување кои можат да им наштетат на гарѓаните во нивната стабилност и безбедност, вклучувајќи го тука и тероризмот, постојат институции кои се одговорни за одредени аспекти во оваа област.

Такви институции кои ја носат одговорноста на заштита на информатичката технологија и безбедноста во целина ги сочинуваат :

- Министерството за информатичко општество и администрација
- Министерството за Внатрешни работи во чии состав влегуваат:
  - ✓ Бирото за јавна безбедност
  - ✓ Управата за безбедност и контраразузнавање
  - ✓ Криминалистича полиција
- Министерество за одбрана, во чии рамки функционира
  - ✓ Секторот за безбедност и разузнавање
- Агенцијата за разузнавање на Република Македонија
- Советот за национална безбедност на Претседателот на Р.Македонија
- Центарот за управување со кризи, и
- Агенцијата за електронски комуникации.

Овие институции во процесот за изнаоѓање и градење стратегија за национална безбедност се согласни во кординативните активности, а со тоа е направен обиди за градење определена оперативно институционална основа при градење норми и интензивни меѓународни договори за соработка во борбата против сајбер тероризмот.

Земајќи го во предвид ова, важно е да се потенцира дека за да се започне да се применува еден функционален систем или кога би се оредила институција за борба против високотехнолошкиот тероризам потребна е голама проактивна ангажираност и соработка и со другите државни институции кои го сочинуваат системот на целокупното општествено функционирање, како и приватниот сектор во целост.

2.3.2. Кривично-правна регулатива на сајбер просторот во Република Македонија

Успешното спротиставување на современите форми на тероризам е детерминирано од јасно и прецизно дефинирање на инкриминираната појава односно нејзина апликација во меѓународното и националното законодавство.[231]

Постојната правна рамка за електронски комуникации преку која Република Македонија се обврза на апроксимација кон регулаторната рамка на Европската Унија во областа на електронските комуникации е донесена во 2005 година под називот Закон за електонските комуникации, кој е во целост усогласен со регулаторниот пакет на ЕУ за елекртонски комуникации од 2002 година и претставува правна рамка за целосна либерализација на пазарот за електронски комуникации. Во дополнение на законот за електронски комуникации донесени се преку 45 подзаконски акти кои ја дополнуваат и во целот регулираат оваа област.

Со Законот за електронски комуникации се обезбедија услови за интерконекција и пристап со примена на принципот за транспарентност и недискриминација, избор на даватели на услуги, водење постапка за нотификација на правните и физичките лица пред да започне со изградба на јавни електронски комуникациски мрежи и обезбедување на комуникациските услуги, определување на оператори со значителна пазарна моќ, овозможување на пристап до услугите на друг оператор по избор на претплатникот и сл. Исто така се утврдуваат и правилата под кои ќе се распределуваат ограничените ресурси на пример радиофрекфенцискиот спектар, нумеричкиот простор и сл.

Надлежни институции за имплементација на правилата од областа на електронските комуникации согласно постојниот закон за електронски комуникации се Министерството за транспорт и врски и Агенцијата за елекронски комуникации во својство на регулаторно тело за електронски комуникации.

Во рамки на надлежностите на Министерството за транспорт и врски е реализирање на политиката на Владата на Република Македонија во областа на електронските комуникации, подготвување на законска регулатива во област во соработка со Агенцијата, вршење на работи во враска со развојот на електронските комуникации и информатичките технологии, промовирање конкуренција во област на електронските комуникации и зголемување на пристапот и користење на електронските, комуникациски и информатички технологии.

Една од насоките во вид на законско решене кои го превзема Република Македонија за заштита од сајбер напади е донесувањето на Правилникот за стандардите и правилата за безбедност на информациските системи кои се користи во органите за комуникација по електронски пат во 2010 година, од страна на

[231] М. Николовски, Кривичното законодавство во справување со современите форми на тероризам, Годишник на Факултетот за безбедност, Скопје,2009,стр.43

Министерството за информатичко општество, а е во согласнот со Законот за електоско управување.[232]

Во 2011 година беа донесени и насоки за следење и управување на инциденти поврзани со информациската безбедност, под кои се подразбира:

Организирање и воспоставување на центар за управување со инциденти поврзани со информациската безбедност и развивање формални процедури за следење и управување со безбедносни инциденти. Безбедносен инцидент преставува настан кој предизвикува или може да предизвика нарушување на интегритетот, достапноста и доверливоста на информациските ресурси. Целта на процесот за управување со безбеносни инциденти е ефикасно и рентабилно обновување на нормалните операции што може побрзо со најмалку можно негативно влијание врз деловниот процес и целите на индустријата. Критичен елемент од управувањето со безбедносниот инцедент е обновување на функциите на системот.

Процесот на управување со информатичко безбедносите инциденти ги вклучува следниве елементи:

- Откривање и инцидентот
- Единствена точка на пријавување
- Евидентирање
- Доделување на приоритет на инцидентот
- Класификација на инцидентот
- Процена на настанот и одлука за начин засправување
- Дефинирање на прво ниво за решавање и услови за пренасочување на повисоко ниво
- Обновување
- Верификација и затварање на инцидентот
- Идентификација на потребни подобрувања на процедурите за спречување на безбедносни инциденти
- Следење на инцидентите
- Управување со животниот циклус на инцидентите

Насоки за дејствија по оценка и управување на ризикот кои органите се должни да си спроведат се проценката и оценката на ризикот по однос на безбедноста на информацискиот систем. Ваквата проценка треба да има стандардизиран и структуиран пристап во управување со ризиците, при што упрвувањето треба да се извршува преку постојната примена на два типа циклични повторувачки дејствија оценка(проценка) на ризикот и избор на ефективни и економски мерки за негова неутрализација. Проценатa за управување со ризиците треба да ги вклучи и фазите на избор на објектите кои ќе бидат предмет на анализа, избор на метологија за оценка на ризикот,идентификација и

[232] Службен весник на Република Македонија бр 105/09 и бр.45/2011, член 32 став(3) и член 33став(2) од 2010 година.
http://www.pravo.org.mk/documentDetail.php?id=4943

информациски сретства, анализа на заканите избор за заштитни мерки и проценка на преостанатиот ризик за следни несакани појави.

За таа цел повеќе од неопходно е да се цели кон формирање на специјалицирана институција со специјализирани кадри за рана превенција и борна против високотехнолошкиот тероризам, и донесување на правна регилатива со кај би се осудиле сите закани и сторители кои во иднина можат да ја загрозат индивидуалната и националната безбедност на Република Македонија со новите достигнувања во информатичкото општество.

Заклучок

Основната цел на овој магистерскиот труд беше добивање на научна дискрипција за суштината и опасноста од дејствувањето на високо-технолошкиот тероризам врз националната безбедност на современите држави, како и начинот и методите за нивен одговор, се со цел обезбедување на мир, безбедност и благосостојба, а на тој начин и заштитат сите витални вредности.

Конкретно, овој магистерски труд има за цел да даде придонес во објаснувањето на едно од сериозните безбедносни закани на современите држави, како и на меѓународната соработка на државите во спречување на овој вид на закана.

При самата научна дискрипција која е наведена може да се увиди дека она што ја прави една земја силна, секако не е нејзиниот народ, нејзината војска, туку тоа се хардверот, софтверот и финансиската инфраструктура која го поддржува нејзиниот економски развој и благосостојба. Основната цел на современите терористички организации е токму оштетување на економијата и економската стабилност на земјата, а со тоа и поткопување на довербата и подршката што граѓаните ја положиле во институциите и секако нивниот начин на живот.

Секоја држава гради свој автентичен систем за безбедност и одбрана. Во рамки на тој систем секоја држава знае дека мора да концепира своја сопствена национална-безбедносна политика. Во рамки на таа политика државата мора да ги донесе сите неопходни документи, закони и правила, врз основа на кои ќе се темели одбраната и безбедноста на државата, и да формира институции кои ќе ја спроведуваат одбранбено-безбедносната политика и стратегија на државата.

Новиот милениум е време на промени во дефинирањето на општо безбедносните закани и ризици, па на тој начин и на глобално и на национално ниво на одделните современи држави, се повеќе е присутна заканата за разнишување на безбедноста и стабилноста и внесување немири и постојан страв од заканите со асиметрично потекло. Ваквите закани секако дека приматот го имаат терористичките напади, кои станаа безбедносна закана број еден и кои покажуваат дека флуидноста на овој непријател, ненадејноста и разорувачкиот ефект од неговите дејства, навистина темелно го поткопуваат сонот за глобален мир и спокој на новиот милениум.

За разлика од конвенционалните напади, високо технолошките напади, денес се доста поприсутни, што укажува на фактот дека можат да бидат изведени по пат на далечинско управување, така што иднината на тероризмот вели дека терористите нема да бидат волни да го жртвуваат својот живот за целите на организацијата, па на тој начин овој вид на закана може да се каже дека преставува сериозен предизвик за нејзино одвраќење на секоја современа држава.

Од претходно изнесеното може да се констатира дека сајбер тероризмот е современ облик на тероризам кој се користи од страна на терористичките организации

во светот заради постигнување на терористички цел по пат на упади во информациско компјутерските системи и искористување на недоволната правна регулатива на полето на информацискаата безбедност и генерално искористување на недостатоците во законите кој ја уредуваат националната безбедност на современите држави.

Врз основа на проучувањето на поврзаноста помеѓу терористите и интернетот увидовме дека терористите го искористуваат интернетот за остварување на своите цели преку ширење на своја пропаганда за регрутирање за обезбедување на материјални сретства за комуникација и кординација на своите активности и сл.
Терористите се стратешки актери кои промислено ги одбираат своите цели и таквиот нивен избор се заснова на слабостите и пукнатините што ќе ги воочат на нашите одбрамбени системи и нашата подготвеност.

Врз основа на криминалистичките карактеристики на сајбер тероризмот и проучувањето на личноста на сторителот добиваме сознание за тоа што точно преставува сајбет тероризмот, за каков терористички метод се работи, но и какви се заканите по безбедноста на современите држави кој сосебе ги носи.
Преку разгледување на карактеристиките на современите терористички групи и нивното користење на високата технологија, увидовме дека многу од нив минале преку една трансформација од стрикно хиерархиска организација со назначен лидер во мрежно поврзување преку што им е овозможена меѓусебна комуникација која е тешко достапна за следење и разбивање.

Во однос на дејствувањето и сузбивањето на сајбер тероризмот преку широката дискрипција дојдовме до согледување на недосатоците кои значат предизвик и загриженост.
Едно од нив е и недостатокот од свесност за културата на сајбер безбедност на граѓаните на современите држави, како и недостсток во однос на разбирање и иплементација на институционално ниво.
Недостаток во правната регулатива кои ги уредуваат овие и слични закани, недостаток за обучен и квалитетен кадар кои ќе изнајдат мерки за безбедност.
На ова бојно поле и против ваков вид на оружје, терористите се чекор напред и настојуваат да ја одржат таквата предност.

Градењето и созадавањето на еден тим за борба против сајбер тероризмот бара *димамичност, современост и точност од едноставна причина што, оружјето против кое* се бори секоја современа држава за зачувување на националната безбедност се повеќе се усовршува и менува, и за разлика од обичните терористи, доколку сајбер терористот не успее денес, тој не умира, туку напротив учи каде згрешил и што во неговиот план недостасува, така што секоја нареден напад тој ја искористува.
Отука, може да констатираме дека, за разлика од другите терористички методи, сајбер тероризмот е безбеден и профитабилен и секако потежок за сузбивање, без потребна експетиза, знаење и што е најважно разбирање на умот на сајбер терористите.
Сепак, многу од прашањата поврзани за сајбер тероризмот останууваат неодговорени поради неговата природа, но тоа не треба да не спечи во градење на темелите на програмата за борба против ваквиот вид на тероризам во која програмна би требало да бидат опфатени следниве елементи:

- Целосна подршка за организациите кои се задолжени да се справуваат со сајбер тероризмот;
- Заеднички напори од сите владини агенции за обезбедување и обука на квалитетни персонални решенија и имплементација на мерки за безбедност;
- Поголема финансиска подршка на инвестициите во полето на сајбер тероризмот;
- Усвојување и практикување на новите законски решенија, новите техничко технолошки достигнувања и целосна инклузија на нови и стручно оспособени кадри при процесот на сите нивоа;
- Взаемна соработка и размена на информации помеѓу државите како на регионално, така и на национално ниво;
- Изградба на платформа за постојана едукација и подигање на свеста кај граѓаните за заканите од високотехнолошкит тероризам;
- Формирање на специјализиран ценатар за пријава и рана превенција од можни напади на високотехнолошкиот тероризам;
- Соодветна кординација со приватниот сектор и нивна едукација за можни сајбер терористички напади;

Генералното согледување во однос на можните закани од овој вид кажуваат дека спречувањето на сајбер терористичките напади е скапа работа и секако дека одзема многу реме и бара многу напори.Многу големи компании, кои се лесни мети на сајбер терористи не само што не се свесни за импликациите од таквите напади, туку истите неможат да си дозволат таква соодветна заштита.
Значи постои асиметрија и во однос на можностите за спроведување на сајбертерористички напад и можностите за заштита од истиот. Тоа значи дека многу поефтино е спроведување на таков напад брз критичната инфраструктура како на пример SCADA-системите, а многу е поскапа заштитата на таквите системи.Иако превенцијата се чини скапа и несоодветна, всушност на долг рок таа може да биде многу економична и без фатални последици на секое ниво од секојдневното делување.

Кога станува збор за Република Македонија, несомнено и покрај сите напори и заложби во градењето на национална стратегија за безбедност, сеуште неможе сама да одговори на сите видови современи безбедносни закани кои најчесто се со транснационален карактер. Од таа причина, развојот на национален безбедносен систем интегриран во колективна безбедносна структура е стратегиска инвестиција за Република Македонија и важен придонес кога станува збор за евроатланскиот безбедносен регион.

За таа цел повеќе од неопходно е да се цели кон формирање на специјалицирана институција со специјализирани кадри за рана превенција и борна против високотехнолошкиот тероризам, и донесување на правна регилатива со кај би се осудиле сите закани и сторители кои во иднина можат да ја загрозат индивидуалната и националната безбедност на Република Македонија со новите достигнувања во информатичкото општество.

Библиографија

Книги

Арнаудовски, Љупчо, Меѓусловеност и меѓузависност на тероризмот и организираниот криминал во Годишник на Факултетот за безбедност, Скопје, 2002г.

Ангелески, М. Криминалистика, НИО Студенски збор, Скопје 1993.

Арнаудовски, проф. Д-р Љупчо, Криминологија, Скопје 2007,

Бакрески О.*"Контрола на безбедносниот сектор"*,Филозофски Факултет ,Скопје, 2008

Гоцевски Т., Бакрески О., Славески С., Георгиева Л.- „*Интересите на Република Македонија во градењето на европската безбедност*", МАНУ – Центар за стратегиски истражувања, Филозофски факултет, Скопје, 2008.

Гоцевски Т. - „*Основи на системот на национална одбрана*", Филозофски факултет – Скопје, "Киро Дандаро", Битола, Скопје, 2005.

Георгиева Л.- „*Менаџирање на ризици*",Филозофски факултет -Скопје, - „Југореклам„- Скопје, 2006.

Горгиева Л.,-„Творење на мирот„ Студио АДА, Скопје,1999.

Камбовски, В., „КАЗНЕНО ПРАВО-посебен дел„Скопје, 2003,

Котовчевски М.- *"Националана безбедност",* Филозофски факултет, Скопје, 2011.

Котовчевски М., ``Современ тероризам``,Македонска цивилизација, Скопје,2003,

Котевчевски М. – "*Национална безбедност на Република Македонија*„ (прв дел), Македонска цивилизација, Скопје, 2000

Нацев З. Начевски Р. - „Безбедноста и националната одбрана, ,- Македонска ризница, Куманово, 2001.

Шалијан, Жерар и Блин, Арно, Историјата на Тероризмот, Скопје, Табернакул,2009,

Vodinekič, V., Savremena administracija, Beograd, 1985,

Димитровић В.,``*Људска права и демократија, Свет и Југославија*`` Пословна политика, Београд

D.Simeunovič, Definisanje terorizma kao naučni izazov, u Zborniku: Stanje kriminaliteta u Srbiji i pravna sredstva reagovanje, III deo, Beograd,2009

Tatalović S. Bilandiž M. – "*Osnove nacionalne sigurnosti",* MUP R., Hrvatske, Zagrb, 2005.

Jaganjac J. –" *Sigurnost u sistemu znatnosti",*Odjek, Sarajevo, 2009.

Kurbalija, J., *Uvod u upravljanje internetom,* Drugo iydanje, Albatros Plus, Beograd, 2011,

Milosavljevič, M., Grubor, G.,Istraga kompjuterski kriminala, Univeryitet SINGIDUNUM, Beograd, 2009 g

Masleš R. – " *Teorije i sistemi sigurnosti",* Magistrat, Sarajevo, 2001

Pertovič R.S. „*Kompjuterski kriminal,,* Vojnoiydavački zavod, Beograd 2004, III izdanje,

Стајић Љ. Гилановић Ч.-*"Основи безбедности"*, Полициска академија у Београду, Београд 1994.

Saćić Ž.,- " *Organizovani kriminal - metode suzbijana* " – Informator, Zagreb, 2001.

A. Clark, Cyber Terrorism: Political and Economic Implications, London, 2006.

Alex Peter Schmidt – Political terrorism: A research guide to concepts, theories, data bases and literature.

Ashley, B.,K., Anatomy of Cyber terrorism. Is America vulnerable? Air war College, Maxwell AFB, AL.2003,

Baldwin D. - „ *The Concept of Security", Review of International Studies,* 1997.

Buzan B.-"Peoples, States and Fear: An Agenda for International Security Studies in the Post Cold War Era" London, 1991.

Bottler, J., Threats posed by Cyber Terror and Possible Responses of the United Nations Delegation of Canada, First Committee on Disarmament and International Security UNISCA, 12 December 2002,

Bockstette, C. Jihadist Terrorist Use of Strategic Communication Management Techniques, George C. Marshall European Center for Security Studies, 2008,

Buzan B., Weaver O., and de Wilde J., (1998), Security: A new Framework for Analysis, London: Lynne Rienner Publishers.

Collin, C., B., The Future of Cyber – Terrorism: Where the Physical and Virtual Worlds Converge, 11th Annual international Symposium of Criminal Justice Issues, Institute for Security and Intelligence,

C. Walker, Cyber-Terrorism: Legal Principle and Low in the United Kingdom, Pennsylvania State Law Review 2006.

Denning, E., D., ``Cyber terrorism``, Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services, US House of Representatives,

Denning, E., D., *Hacker Warriors: Rebels, Freedom Fighters, and Terrorists Turn to Cyberspace*, Harvard International Review, 2001

Janczewski, A. Colrik Managerial Guide for Handling Cyber-Terrorism and Information Warfare, London, 2005

Janczewski L, Colarik A, Cyber Warfare and Cyber Terrorism, IGI Global Hersey, 2008.

King G. and Murray C. – *"Rethinking Human Security"*, Political Science Quarterly, 2001.

K.Gable, Cyber-Apocalypse Now> Securing the Internet against Cyber terrorism and Using Universal Jurisdiction as a Deterrent, Vanderbilt Journal of Transnational Low 2004.

Lewis G., Critical Infrastructure Protection in Homeland Security – Defending a Network Nation, John Wiley & Sons Inc. Hoboken, New Jersey (USA), 2006.

M.Iqbal, Defining Cyber terrorism, Journal of Computer & International Low, 2004,

National Strategy for Critical Infrastructure Protection (CIP Strategy), Federal Ministry of Interior, Federal Republic Germany, Berlin, 17 June, 2009.

Paler P. - „*National Security - imperatives and Challenges"*, Tata McGraw – Hill Publishing Co Ltd, New Delhi, 2008 No 125-132.

Prichard, J., J., MacDonald, E., L., Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks, Journal of Information Technology Education, Volume 3, 2004.

Paper, R. A., Dying to Win, the Strategic Logic of Suicide Terrorism, Radom House, New York, 2005.

R. Abeyant, Cyber terrorism and aviation-national and international responses, book of Transportation Security, 2011,

S.Berner, Cyber-terrorism: reality or paranoia?, South African Journal of Information Management, vol.5, 2003.

Sutter M., A Generic National Framework for Critical Information Infrastructure Protection, Center for Security Studies, ETH Zurich, 2007.

Venter,H.S., & Eloff,J.H.P.2003,,A tahonomy for information security technologies,, Computers & Security, 22(4), 299-307.doi:10.1016/so167-4048(03)00406-1.

Walter Laqueur – The new terrorism: Fanaticism and the arms of mass destruction.

Зборници и часописи

М. Николовски, Кривичното законодавство во справување со современите форми на тероризам, Годишник на Факултетот за безбедност, Скопје,2009,

Службен весник на Република Македонија бр 105/09 и бр.45/2011

Шикман, М., Самоубилачки тероризам-феноменолошки и виктимолошки аспекти, НБП Наука-безбедност-полиција, Часопис Криминалистичко-полициске академије, Београд, 2008.

CRS Report for Congress, Terrorists and Suicide Attacks, Kurth Cronin, August 28, 2003.

S. Jadhao, Computer Crime, Indian Streams Research Journal, 2013.

Cindy, C., Combs, Slann, M., *Encyclopedia of Terorism*, New York, Facts on File, 2002.

Sprinzak, E., Rational Fanatics, Foreing Policy, September-October 2000,

S.Saint-Claire, Overview and Analysis on Cyber Terrorism, School of Doctoral Studies European Union Journal, 2011.

B.Dobovsek, M.Dimc, Cyber Terrorism: Transference of virtual World Threats to the Physical World I Zborniku: Terorizam kako globalna pretnja.

Речници и енциклопедии

Department of Defense Dictionnary, http://www.dtic.mil/doctrine/doddict/c/01168.html

The New Dictionary of English, Oxford English Dictionary, http://www.oed.com

Исламски речник достапно на http://www.islamic-dictionary.com/index.php?word=ummah

Министерство за информатичко општество и администрација на Република Македонија

Правни акти и правилници

Законот за електоско управувањена Република Македонија, 2010 година

Закон за слободен пристап до јавни информации,Службен весник бр.13/06

Устав на Република Македонија, 1991година

Павилник за транснационален кринимал и правда –Филип Рајкел``Датапонс``2009 година

Конвенција за Компјутерски криминал ма Советот на Европа,2001 година.

Интернет извори

http://www.odbrana.mod.gov.rs/odbrana-stari/vojni_casopisi/arhiva/VD_2011-prolece/17.%20Promenljivost%20fizionomije%20rata;%20Miloljub%20Sretenovic.pdf

http://files.alaindebenoist.com/alaindebenoist/pdf/terrorism_state_of_emergency.pdf

http://www.itu.int/en/about/Pages/default.aspx

http://internetworldstats.com/emarketing.htm

http://livinginternet.com/i/ii_mcluhan.htm

https://en.wikipedia.org/wiki/Dwight_D._Eisenhower

http://searchnetworking.techtarget.com/definition/ARPA

https://en.wikipedia.org/wiki/Lawrence_Roberts_(scientist)

http://www.packet.cc/files/ev-packet-sw.html

http://searchenterprisewan.techtarget.com/definition/WAN

http://searchcrm.techtarget.com/definition/World-Wide-Web

http://blog.com.mk

https://www.icann.org

http://www.livinginternet.com/i/ii_wiener.htm

http://personalpages.manchester.ac.uk/staff/m.dodge/atlas/atlas_chapter_5.pdf

http://pravo.gov.ru/proxy/ips/?docbody=&nd=102034341&rdk=&backlink=1

http://primorsky.ru/authorities/executive-agencies/departments/information-security/Documents

https://www.cnss.go/

http://www.efos.unios.hr/arhiva/dokumenti/UIR2_Vrijednost%20informacije_IS_sigurnost%20pdf.pdf

http://www.start.umd.edu/start/data_collections/tops/terrorist_organization_profile.asp?id=4062

http://www.cs.georgetown.edu/-denning/infosec/cyberter ror.html

http://afgen.com.terrorism1.html

http://www.usip.org/sites/default/files/sr119.pdf

https://www.researchgate.net/publication/222194085_Terrorism_and_Cyberspace

http://s3.amazonaws.com/academia.edu.documents/30719627/165.pdf

http://www.igi-global.com/affiliate/matthew-warren/1514

https://repository.library.georgetown.edu/bitstream/handle/10822/553509/hayneSpencer.pdf?sequence=1

https://www.youtube.com/watch?v=SWP_95eSLBI

https://en.wikipedia.org/wiki/National_Organization_of_Kurdish_Youth

https://www.youtube.com/watch?v=pf_SuKN23m4

http://ichef-1.bbci.co.uk/news/560/media/images/75765000/jpg/_75765420_isisisil2.jpg

http://wemeantwell.com/blog/wp-content/uploads/2015/02/japan_isis4.jpg

www.odbrana.mod.gov.rs/grab_file.php?...%20

https://mk.wikipedia.org/wiki/**Клод**_Шанон

https://en.wikipedia.org/wiki/**Chat_room**

http://www.hum.au.dk/ckulturf/pages/publications/mt/parameters_islamic_terror.pdf

http://linktionary.com/o/opsec.html

https://en.wikipedia.org/wiki/**Data_mining**

http://www.loyalistcollege.com/current-students/technology-services/

http://www.globalsecurity.org/military/world/para/lvf.htm

https://www.paypal.com/us/selfhelp/contact/call

http://www.un.org/en/terrorism/ctitf/pdfs/ctitf_financing_eng_final.pdf

https://www.geo.tv/shows/**meray**-mutabiq?vid=127427

https://www.trackingterrorism.org/group/al-wafa-al-igatha-al-islamia

https://en.wikipedia.org/wiki/Rabita_Trust

www.satp.org/satporgtp/countries/pakistan/terroristoutfits/**Al-Rashid_Trust**.htm

https://en.wikipedia.org/wiki/**Global_Relief**_Foundation

http://www.globalreliefeffort.com/

http://www.hir.harvard.edu/archive/articles/pdf/denning.html

http://www.makdenes.org/content/article/24390898.html

http://www.iso.org/iso/catalogue_detail?csnumber=39883

http://embeddedsw.net/doc/Openpuff_thesis_Digital_forensic_in_security_of_information_system_based_on_linux_and_windows_platforms.pdf

http://www.cert.org

http://www.isc.sans.edu/

http://www.**caida**.org/

http://www.ist-lobster.org

http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

https://www.enisa.europa.eu/about-enisa

https://**ciwin**.europa.eu/

http://www.un.org/en/ecosoc/docs/report.asp?id=1132

http://www.itu.int/en/Pages/default.aspx

http://www.justice.gov/sites/default/files/ag/legacy/2004/06/03/G8_CIIP_Principles.pdf
www.usdoj.gov/ag/events/g82004/G8_CIIP_Principles.pdf

www.oecd.org/dataoecd/25/10/40761118.pdf

www.oecd.org/dataoecd/1/13/40825404.pdf

www.first.org

https://www.csirt.org

www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf

www.Dhs.gov/xlibrary/assets/hr_5005_enr.pdf

http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm

www.cnpi.gov.uk

http://www.mio.gov.mk/?q=node/1911

http://www.mio.gov.mk/?q=node/191 ,и http://www.mvr.gov.mk

http://www.vest.mk/default.asp?ItemID=E0813EB97B954947A3B8425ED802B375

http://www.pravo.org.mk/documentDetail.php?id=4943