Република Македонија
Универзитет „Св. Кирил и Методиј“ – Скопје
Филозофски факултет – Скопје

Студиска програма: Безбедност

Заканите на сајбер-тероризмот врз глобалната безбедност во XXI-от век
(*магистерска теза)*

Изработил:

Ненад Стевковски

Ментор:

Проф. д-р Митко Котовчевски

Скопје, февруари, 2015

СОДРЖИНА

Вовед 3
1. Формулација на истражувачкиот проблем 5
2.Определување на предметот на истражување 7
2.1.Теоретско определување на предметот на истражување 7
2.2 Појмовно-категоријален апарат 9
2.3.Операционално определување 11
3.Цели на истражувањето 13
3.1. Научна цел 13
3.2. Практична цел 13
4. Хипотетичка рамка 14
4.1. Варијабли 15
-Независна варијабла 15
-Зависна варијабла 15
5.Тероризам 16
5.1. Дефинирање на тероризмот 16
5.2. Правна легислатива за сузбивање на тероризмот во домашното законодавство 20
5.3. Одредување на тероризмот како асиметрично војување во глобалниот свет 23
5.4. Карактеристики на современиот тероризам 25
5.5. Современи форми на тероризам 26
6. Информационата технологија и нејзиниот развој 30
6.1.Историски осврт 30
6.2.Интернетот како глобална мрежа 31
6.3. Закани од интернетот 37
6. 4. Информациска безбедност 38
6.4 .1.Криптографска заштита на податоците 40
7. Сајбер – простор и видови на сајбер –компјутерски криминал 42
7.1.Поим за сајбер – простор 42
7.2. Дефинирање на сајбер – просторот 42
7.3. Природата на сајбер – просторот 43
7.4. Поим за сајбер – напад и негови потенцијални извори 44
7. 5.Мети на сајбер – напади 47
7.5.1. SCADA-управувачки системи 49
7.6. Видови на сајбер-компјутерски криминал 50

7.6.1 Поим за сајбер (компјутерски) – криминал 50
7.6.2 Начини на извршување на кривични дела од областа на компјутерскиот криминал 52
8. Современиот тероризам и интернетот 61
8.1. Тероризмот и интернетот – нивната поврзаност 61
8.2.Цели за кои се користи интернетот од страна на терористите 65
8.3.Користење на интернетот од страна на терористичките организации 77
8.3.1. Ал-Каеда 78
8.3.2. Хезболах (Lebanese Hezbollah – Party of God) 82
8.3.3. Aum Shinryko (Јапонската Врховна вистина) 85
8.3.4. Ирската републиканска армија (ИРА) 85
9.Сајбер–тероризам, како глобална закана по безбедноста во светот 87
9.1.Поим за сајбер – тероризам 87
9.2. Дефинирање на Сајбер – тероризмот 89
9.3. Закани од сајбер-тероризам 94
9.4. Криминална активност и профил на сајбер терористот 98
9.4.1. Профил на сторителот на сајбер – терористички напад 100
9.4.2. Криминалистичко – виктимолошки карактеристики 108
9.5 Сајбер-тероризмот како атрактивна опција за терористите 110
9.6. Case study – сајбер напад врз информациско-комуникациската инфраструктура на Естонија 112
9.6.1.Грузискиот конфликт 2008 113
9.6.2. Примери за позначајни сајбер – инциденти 114
10.Мерки за делување против сајбер-тероризмот 118
10.1.Општо за мерките за делување против сајбер-тероризмот 118
10.2.Реактивно дејствување 119
10.3. Проактивно дејствување 120
10.4. Преземање на мерки од страна на меѓународни организации во борба против сајбер-тероризмот 121
10.4.1. НАТО 122
10.4.2. ООН 124
10.4.3.ОБСЕ 125
10.4.4.Совет на Европа 126
10.5. Мерки што ги презема Република Македонија во борба против сајбер - тероризмот 128
11. Заклучок 130
12. Литература 134

Вовед

Тероризмот од дамнешно време претставува закана со која човештвото постојано се бори, и се обидува да ги залечи раните предизвикани од оваа зло, но во последната декада сме сведоци на тоа дека тероризмот со своите облици стана глобална закана по безбедноста во светот.

Тоа е овозможено од брзиот техничко-технолошки развој на информационата технологија и компјутерските системи, кои на голема врата влегоа во сите пори на општественото живеење. Оваа информациона револуција донесе рапидни промени во начинот на живеење и секојдневно функционирање, каде буквално се сè промени и на еден начин го олесни животот со технолошките придобивки. Во новото, модерно информатичко општество компјутерот успешно ги замени сите мануелни функции и ги презема сите активности и процеси.

Сето тоа не остана незабележано од страна на терористичките организации, кои информатичката технологија и зависноста на светот од неа, успешно ја искористија за остварување на сопствени цели, а истата како оружје насочувајќи ја и загрозувајќи ги сите сегменти во општеството.

Со помош на интернетот, терористите развија нова форма на тероризам, кој во последната декада ги засени сите претходни форми на тероризам, поради огромните предности што ги има, а поради просторот во кој што се изведува е наречен ***сајбер-тероризам.*** Како што информационата технологија напредуваше, така и тероризмот еволуираше, го менуваше начинот и темпото на дејствување, комплексноста, непредвидливоста, опременоста, што со еден збор кажано се менуваше „профилот на терористот", кои, денес прерасна во модерни сајбер-терористи образовани на најпрестижните универзитети ширум светот, кои опремени со сден компјутер и доволно вештина или знаење можат да предизвикаат илјадници жртви и штети од огромно размери. Сајбер-тероризмот, од досега спроведените сајбер-напади се покажа како доста комплексна појава, бидејќи според огромните предности што ги нуди интернетот: брзина, лесен пристап, анонимност, безграничност и лесна комуникација во било кој дел на светот, им задава огромни проблеми на безбедносните сили за успешно справување со оваа глобална закана на 21-век.

Сајбер-теророзмот како комплексна појава, им нуди голем избор на терористите во одредување на своите цели, планирање, организирање, координирање на своите напади, и тоа без трошење на огромни средства, без потреба од тони на експлозив и огромна војска, туку само со едно кликање со компјутерско глувче и сајбер-терористичкиот напад е извршен. Разноликоста при изборот на целите се потврдува со тоа што сајбер-терористот може да дејствува против цивилни цели, против воени цели, против државни

институции, против влади, но со директно поврзаност со секој корисник на интернет и вршење на пропагандна активност, од претходните акции, спроведување на ужас и терор, обезглавување на војници и цивилни лица, терористите најмногу дејствуваат психички врз целната публика, заради остварување на своите цели. Како за пример: доколку изврши атентат на една личност, не е толку страшно, но доколку постојано се врши сеење на страв и пропаганда дека ќе кренат некоја нуклеарна централа во воздух, или ќе ги изменат состојките при производство на некој лек што масовно се употребува, тогаш имаме загрозување на национална безбедност, па и безбедност од глобален карактер.

Тероризмот, со своето терористичко лудило сè повеќе почна да дејствува ширум светот на кој не му се битни ниту границите, ниту годините, ниту полот, не ги заобиколија ниту големите сили, кои откако го искусија тероризмот на сопствена кожа, и ја увидеа моќта и се поголемата одлучност и жедта за крв на терористите, ги прогласија како глобална закана во светски рамки и им објавија војна на терористите. Тоа за сајбер-тероризмот значи да се војува со невидлив непријател, на кој ниту му го знаеме името, ниту местото и времето на извршување на целта, ниту од каде ќе дејствува.

Современата цивилизација во светски рамки ќе мора да остане будна и претпазлива пред новите сајбер-терористички закани, кои можат да ги надминат сите досегашни претпоставки дали и каде ќе се случат, бидејќи после нападите од 11 септември 2001 година на сите им стана јасно дека терористите не ги бираат своите цели, и удрија токму на земја како САД, која има најразвиен и најсовремен безбедносен систем и разузнавачка служба, кои не можеа ништо да сторат, а се верува дека следниот напад од такви размери ќе биде сајбер-терористички напад.

Од горенаведеното може да се заклучи зошто е круцијално да се изучуваа и истражува оваа тема. Во овој труд преку дефинирање на поимите ***сајбер-простор, сајбер-криминал, сајбер-напади, сајбер-тероризам*** ќе се спознае опасноста од ваквиот вид на тероризам, кој како најнов облик на тероризам, го зазема највисокото место како закана врз глобалната безбедност во 21-от век, а што повеќе го проучуваме и расчленуваме, толку подобро ќе можеме да се заштитиме од него, а и безбедносните сили толку подобро ќе можат да му се спротивстават, затоа што сајбер-тероризмот не е научна фантастика, туку наше секојдневие.

1. Формулација на истражувачкиот проблем

Тероризмот претставува сериозен проблем на општеството кое се бори со сите свои расположиви законски сили и средства да му противречи. Живееме во време во кое што тероризмот не дава сигнали на намалување на неговиот интезитет, напротив сведоци сме на негова експанзија. Имаме појава на нови облици на тероризам, на најсофистицирано оружје и опрема при изведување на терористичките акции, постојано усовршување на организацискатa структура на терористичките организации. Сето тоа води кон зголемување на бројот на жртвите и материјалните штети при изведување на терористичките акти. Сите процеси кои ги донесе транзицијата и глобализацијата го ставиќа самиот човек во општестена емулзија навраќајќи се на обичајот, верата од една страна како и сите модерни случувања од друга страна во која пак жртва е самиот човек во зависност со какви сваќања е и по какви погледи се раководи.

После падот на „Железната завеса", и крајот на Студената војна, временскиот период кој следеше го добил името **пост-индустриска ера**, но се попознат и покористен стана и терминот **информатичка ера.** Доколку во предвид го земеме квантитетот на информации, кои денес во секоја секунда се пренесуваат ширум светот и растот на компјутерските мрежи во последнава декада овој термин воопшто не е претеран.

Компјутерите и интернетот не само што станааа битен дел од секојневниот живот, тие станаа есенцијален дел, дел без кој современото развиено општество не може да се замисли да функционира. Секоја година се повеќе и повеќе луѓе, државни институции, влади, приватни претпријатија, интернационални организации, нуклеарни централи, разузнавачки организаци, го користат интернетот и останатите придобивки на информатичката технологија. Светските телекомуникации, бизниси, берзи, интернационални сообраќајни системи речици се функционира со помош на информационата технологија.

Но освен придобивки, информатичката ера, со себе носи секако и ризици и загуби. Со оглед на тоа што денес, скоро се тргнувајќи од телекомуникациите, радиото,телевизијата, па се до преносот на електрична енергија, системите за греење, банкарските трансакции, сообраќајната контрола и јавната администрација ја базира својата работа токму на ваква технологија, современите информатички општества стануваат зависно од истата. Многу лесно, орудието наречено информатичка технологија, би можело од слуга на човекот, да се претвори во негов господар. А ваквата зголемена зависност на општеството од компјутерите и информатичката технологија, од друга страна значи и негова зголемена ранливост, било од физички, а пред се од т.н. сајбер- напади, односно една „голема електронска Ахилова пета". Непријателската нација или група , би можела да ги искористи

оваа ранливост и да навлезе во слабо заштитените и обезбедени компјутерски мрежи и да предизвика нарушување па дури и уништување на виталните инфраструктури.

Оттука можеме да кажеме дека без разлика дали станува збор за развиена земја, земја во развој, или некоја друга земја во транзиција, многу лесно може да дојде до еден општ хаос кој предизвикан од објективни или субјективни фактори секако продуцира голем број на деструкции и нанесува огромни загуби за државата и директно удира по националната безбедност па дури и на глобалната безбедност во целина.

Со самата глобализација и компјутеризација на на целокупниот општествен и личен имот начинот на пренос на информации ги поттикна терористичките организации т.е го искористија тоа за свои интереси , за свои цели и начин на војување и напаѓање. и земјите кои имаат изградено најразвиен безбедносен систем не останаа имуни на нападите на терористичките организации кои добро ги обезбедија аеродрумите, метроата поставија камери на патиштата и полиција пред училиштата, но сега, наидоа на еден нов вид војување со кое со еден клик на копче на некој болен ум и ќе дојде до уништување на цели постројки, судири на возови ,сообраќаен хаос па дури лансирање на ракети до колку не бидат исполнети нивните барања.Така да разузнавачките и контраразузнавачките служби на високо развиените земји мора да оспособат и да обучат свои тимови и стручни лица кои ќе можат да им одговорат и да се заштитат од ваквите терористички дејствија со кодирање и заштита на информациите и постојано следење на коминикациите т.е заштита од така наречен Сајбер-теторизам.

Во изминатите две декади, започна нашироко да се зборува, а особено пишува во литературата за проблемот поврзан со Сајбер-тероризмот, но сепак авторите заземаат различни ставови во врска со негово дефинирање[1]. Во овој труд ќе се обидеме да го согледаме празнините кои постојат во спротивставените ставови, и да го разгледаме и дефинираме Сајбер-тероризмот како можна претпоставена закана од една страна, и веќе постоечките сајбер-напади, забележани во литературата,кои укажуваат на тоа дека ваквата закана е реална и неизбежна.

За таа цел, потребно е да тргнеме од дефиниција за поимот тероризам, и да укажеме на тоа дека, покрај тоа што терористичките мотиви остануваат непроменети, денешницата и иднината носат нови и досега непознати облици на тероризам, а разузнавачките системи, тактиките, безбедносните процедури и опрема од кои порано се очекуваше да бидат средства за заштита на луѓето, системите и нациите од тероризам, денес се немоќни против новите и

[1]Stohl, M., Cyber terrorism a clear and present danger, the sum of all fears, breaking point or patriot games? ,Crimes, Law and Social Change превземено од http//www.springerlink.com/content/y8166117ww6058jp7/

современи облицина оваа застрашувачко оружје. Освен тоа, и методите за борба против тероризмот во сите негови облици, што светските експерти ги применуваат во изминативе години, се покажуваат како неефикасни против ваков вид на непријател. Ова е затоа што непријателот не го реализира нападот со камиони експлозив, или со актовки полни со Сарин гас, ниту пак со појас нареден со динамит прицврстен на телото на некој фанатиц-самоубиец. Овде станува збор за напад со помош на единици и нули , на местото на кое сме најранливи , на точката каде што конвергираат реалниот (физички) и виртуелен свет[2].

Физичкиот и виртуелниот свет по природа се неспоиви; но токму конвергенцијата,преклопувањето, на овие два света ја дава можноста за развојот И употребата на новото оружје во светот, познато под поимот Сајбер-тероризам.

Не смееме да живееме со лажни претпоставки за нашиот непријател и за околината во која тој дејствува ,времее да го запознаеме и да ја согледаме реалноста.

2.Определување на предметот на истражување

2.1.Теоретско определување на предметот на истражување

Тероризмот како најголема закана по глобалната безбедност во светот, не само помалите и послабите земји во светот туку под него потклекнаа и најмоќните и најразвиените земји, земји со најдобри разузнавачки и контраразузнавачки служби како САД, Велика Британија, Русија и други. Меѓутоа многу важна работа што треба да се искатне е тоа дека тероризмот е дефиниран на различни начини и дека не постои една општо прифатена дефиниција за тероризмот. Имено тоа што за западните земји претставува насилство, заплашување, терор за земјите од блискиот и среден исток, и припадниците на Хамас, Хезболах и Ал Каеда претставува борба за слобода и човекови права. Тероризмот како начин на загрозување на безбедност постои одамна само тогаш не биле свесни луѓето дека тоа е еден вид на тероризам, но во поново време особено со развој на техниката и технологијата тероризмот го доби својот најголем подем односно се искачи на врвот. Така со развојот и усовршувањето на технологијата се разви еден нов вид на терористички акт сајбер тероризмот за кој не треба многу подготовки, многу луѓе ,многу време

---

[2]**Физичкиот свет** се дефинираакако материја и енергија-светлина,темнина,топло и ладно, целокупната физичка материја-она место во кое живееме и фукционираме .
Виртуелен свет е симболичен вистина, невистина, бинарно метафоричко претставување на информациите, она место во кое функционираат компјутерските програми и каде што се пренесуваат податоци

туку само образовен кадар во терористичките кругови и келии ,па затоа во нивните редови се повеќе се среќаваат електо инженијери,машински инженијери ,пилоти,доктори односно се регрутираат луѓе кои се врвни, успешни нема да падне сомнеж на нив, а од друга страна многу опасни и корисни за организацијата. Особено во последната декада настанаа рапидни промени на полето на информатичната наука па така и заканите во сајбер просторот станаа неограничени односно со најразлични облици за војување во сајбер просторот. Тоа не значи дека на проучувањето на новите можности што ги нуди технологијата, не треба да се пријде од аспект на футурологија или научна фантастика, туку напротив, со темелна и разумна анализа, затоа што она што до вчера беше незамисливо, денес станува дел о д секојдневието[3]. Во секој момент, во светот на интернет се приклучени милиони и милиони корисници.

Ако само и мал делод овие индивидуи, ја поседуваат соодветната обученост, вештина и експертиза, суштински потребни за да се изведе еден деструктивен 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 компјутерска обученост, и активно регрутираат лица со вакви капацитети[4].

За разлика од другите терористички методи, сајбер-тероризмот е безбеден и профитабилен и секако тежок за сузбивање без потребната експертиза, знаење и што е најбитно разбирање на умот на сајбер-терористите. Комбинирајќи ја зголемената ранливост, со огромните порасти на на нивото на насилство, зголемената обученост и едуцираност на младите членови на терористичките организации, согледуваме дека на точката на спојување на физичкиот и виртуелниот свет, примената на старите модели на тактика, справување и борба против тероризмот се застарени и надвор од употреба[5].

Дефиницијата за тероризам од Federal Bureau of Investigation (ФБИ, Федералното Истражно Биро) гласи: „Тероризмот е безправно користење сила и насилство против лица или сопственост,за да се заплаши или принуди една влада, цивилно население или кој било друг дел од општеството за остварување на политички или социјални цели".Оттука може да за заклучи за да се заштити било која држава од канџите на тероризмот во однос на кривично правните аспекти треба да ги прифати и имплементира

---

[3]Rathmell, A., Cyber–terrorism: the shape of future conflict. Превземено од http://informaworld.com/smpp/content~db=jour~content=a791623655~frm=titlelink

[4]Verton ,D.,Black Ice:The invisible Threat of Cyber-Terrorism.McGraw-Hill/Osborne,2003,CA.Usa p.7-9

[5]Collin, C., B .,The Future of Cyber-Terrorism:Where the physical and virtual Worlds converge,11 th annual International Symposium on Criminal justice issues, Institute for security ang intelligence,превземено од:http://afgen.com/terrorism l.html

меѓународните стандарди, бедејќи со тероризмот како глобална појава не може да се справи и не е проблен само на една држава ,тој е феномен кој не признава граници и успешно може да се победи само со заедничко залагање и корелација на силите и средствата.

Во Кривичниот законик, во неговите измени и дополнувања од 15.01.2008 година, инкриминирани се „Терористичка организација" (член 394 а), „Тероризам" (член 394 б), „Финансирање на тероризам" (член 394 в)[6] .Со самата инкриминација на овие членови Република Македонија покажа дека активно се вклучи во борбата против тероризмот без разлика на неговите видови.

2.2 Појмовно-категоријален апарат

Во продолжение ќе биде укажано на некои од специфичностите на поимите кои непосредно ке се употребуваат во трудот.

- **Тероризам** се состои од нелегитимна употреба на сила за постигнување на политичка цел кога невини луѓе служат како мета.
- **Тероризам** е задавање страв, предизвикување страв,трепет, ужас, примена на насилство, се со цел физичко уништување на противникот.
- **Тероризам** е вршење терор ,владеење со застрашување, тиранија, уништување на противникот со најсвирепи средства (прогонување, угнетување, убивање.)[7]

Според Котовчевски (2003) постојат голем број на обиди за дефинирање на тероризмот, но досега ниту една дефиниција не е општо прифатена. Сето ова е заради недостаток во нејзиното објаснување. Сепак, можна дефиниција на тероризмот односно терористички акт би можела да биде: нелегална, противзаконска примена на закана за употреба на сила и примена на систематско насилство, односно извршување на убиства, закани, сеење на страв од страна на поединци, групи, или организации, насочени против невиното население (или негови делови), сопственоста и владата со цел, да се промени политичкиот курс и да се остварат нивните политички и социјални цели.[8]

Тероризмот се смета како насилство кое служи, а се оствари определен ефект, насилство кое најчесто не е примарно, а понекогаш воопшто не е насочено за постигнување на физички ефект на актуелната цел туку насилството најповеќе е насочено кон тоа за предизвикување драматично

---

[6]Кривичен Законик на Република македонија, Сл Весник на РМ бр:19 од 30.03.2004 год.

[7]Vujaklija , M, Leksikon stranih reci i izraza стр 947.

[8]Котовчевски М, Современ тероризам Македонска цивилизација. Скопје, 2003 стр 27.

влијание врз аудиториумот. Тероризмот е програмиран за да постигне една или истовремено повеќе цели: добивање на општо светско, национално и локално признавање на нивната цел , да предизвика што погелема реакција од страна на власта и да создаде атмосфера на наклонетост за остварување на влијанија врз решенија на владата, законодавството или влијание за време на изборите како и за одмазда.

- **Терор** претставува цврсто организирана власт над ограничувањата, апарат на принуда така што стравот прави дел од секојдневното живеење.
- **Терористичка организација** претставува илегална организација чие постоење и делување укажува на зголемениот степен на општествена опасност и загрозеност на националната безбедност и делува според однапред поставени политички и други цели.
- Согласно Кривичниот Законик на Р.Македонија **Терористичка организација** е „Тој што создава група, банда или друга злосторничка организација за извршување на кривични дела на: Убиство, телесно повредување, грабнување на лица, уништување на јавни објекти, транспортни системи, објекти на инфраструктура, информациони системии други објекти во општа употреба , грабнување на авиони или други средства за јавен транспорт, производство, поседување или трговија со нуклеарно оружје, биолошки, хемиски, опасни радиоактивни, отровни и други опасни супстанции, или предизвикување пожар или експлозија, уништување на постројки за снабдување со вода , енергија или други основни природни извори, со намера загрозување на животот и телото создавање чувство на несигурност или страв кај граѓаните, ќе се казни со затвор од најмалку 8 години"[9] .
- **Безбедност** е состојба во која државите сметаат дека нема опасност од воен напад, од политичка принудаили економска присила, така што слободно можат да се развиваат (дефиниција изработена во рамките на ООН во 1985 година)[10].
- **Сајбер-простор** е просторот односно средината во која со дигитализираните информации се комуницира преку компјутерските мрежи[11].
- **Информациско-компјутерски систем** е каков било уред или група

---

[9]Ibid , стр.311, Чл.394-а

[10]Котовчевски, М., Национална безбедност на Република Македонија - прв дел, македонска цивилизација, Скопје 2013 , стр 25.

[11]Joint Publication 1-02, "DOD Dictionary of Military and Related Terms", April 2001 превземено од http://afgen.com.terrorism I.html.

на меѓусебно поврзани уреди од кои, еден или повеќе од нив, врши автоматска обработка на податоци според одредена програма[12].

- **Сајбер тероризмот** е конвергенција од тероризмот и сајбер просторот.Генерално земено станува збор за незаконски напади или закани од напади против компјутери, мрежи и информациите складирани 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 сајбер тероризам, истиот треба да предизвика насилство врз луѓето или имотот, или барем да предизвика доволно штета со тоа што ќе генерира страв. Нападите кои резултираат со смрт , телесни повреди, експлозии, авионски несреќи, загадувања на водата , или тешки економски загуби, би биле конкретен пример[13].
- **Сајбер-тероризмот** може да се дефинира како умислено, политички мотивирано насилство, насочено против цели кои не се борци од страна на суб-национални групи или тајни агенти, со помош на компјутерски програми и механизми за пренос на податоци како што е интернетот.
- **Федералното Истражно Биро** го дефинира **сајбер-тероризмот** како умислени политилки мотивирани напади врз информациите, компјутерските системи, компјутерските системи, комјутерските програми и податоци , што резултираат со насилство против цели кои не се воени, од страна на суб-национални групи или тајни агенти[14].

2.3.Операционално определување

Предметот на овој труд се операционализира преку повеќе аспекти на истражувањето.

- Примената на постапките и методите за попречување на современите форми на тероризам со посебен осврт на сајбер-терористичките напади,предистражни и истражни мерки и активности, како и појавата на сајбер-терористи и мотивот за превземање на нивните терористички активности (политички , религиозни , идеолошки карактер).

Истражувањето е операционализирано преку следните димензии:

---

[12]Камбовски , В., Кривичен н Законик , Инегрален текст, Предговор, кратки објаснувања и Регистар на поими , ЈП Службен весник на РМ, Скопје,2009 стр.126, Чл.122, став 26

[13]Denning, E., D ., "Cyberterrorism" ,Testimony before the Special Oversight Panel of Terrorism Committee on Armed services, US House of Representatives, May 2000, превземено од http://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf ,

[14]Pollitt. M., M., "A Cyberterrorism Fact or fancy?", Proceedings of the 20th National Information Systems Security Conference, 1997, стр. 285-289 ,како и The terrorism research center http://www.terrorism.com, види и http://searchsecurity.techtarget.com/sdefinition/0,,sid 14 gci 771061,00.html,

- **Дефинирање на сајбер нападите како облик на криминал и Тероризмот и нивната поврзаност,**

- **Утврдување на врската помеѓу Сајбер нападите т.е обичниот Сајбер криминал и тероризмот по пат на споредување на матриците на истите во однос на: сторители, место, дејствија, цели, средства, здружување и мотивација.**

- **Дефинирање на поимот Сајбер-тероризам по пат на приказ на теориско-методолошките пристапи кон сваќањето на Сајбер-тероризмот како реална закана за безбедноста,**

- **Конструирање на модел кој ја опишува анатомијата на Сајбер-тероризмот,**

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

- **Преку разбирање на тие основни столбови, да се осознае суштината Сајбер-тероризмот.**

- **Анализа на досегашните случаи на Сајбер-тероризам во светот и начините на (не)времена реакција на соодветните структури,**

- **Проценка Сајбер-терористичките можности во светот, преку модел на проценка кој се базира на неколку фактори: постоење, можности , намери ,историја, (минато) и цели.**

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

- **Сајбер-тероризмот како реално очекувана закана по безбедноста во Сајбер-просторот во светот и во Република Македонија и потребата да се унапреди *безбедноста во сајбер просторот со цел успешна одбрана од новиот облик на тероризам.***

3.Цели на истражувањето

3.1. Научна цел

Општата цел на оваа истражување е насочена кон добивање на основни сознанија кои ќе овозможат, следење на самата појава во оваа област и превентивно реагирање како и тактичка подготвеност на безбедносните сили во откривање и попречување на сајбер-тероризмот. Со оглед на фактот дека се работи за доста сериозна проблематика која за жал кај нас не е доволно истражена и за која исто така постојат многу малку податоци, ценам дека оваа истражување ќе овозможи прибирање на низа податоци кои ќе најдат место во науката и научните дисциплини кои се занимаваат со оваа проблематика.Ценам дека собраните податоци ќе овозможат остварување на на научната цел, односно дескрипција на конкретната појава, нејзино постоење и зачестеноста на истата, научно објаснување за причините поради кои оваа појава зазема се поголем замав и станува се посериозен проблем на денешнината.

3.2. Практична цел

Практичната цел на оваа истражување е да се дојде до основните сознанија за природата, карактеристиките и димензиите како и сеопфатно анализирање на податоците кои се онесуваат на појавата на Сајбер-тероризмот, се со цел за унапредување на веќе постоечките, како и воведување на нови постапки и методи за откривање и попречување, воедно и продлабочување на соработката со останатите земји и размена на искуство во однос на тероризмот и начините на кои треба да се справуваме со него. Сознанијата кои што ќе се добијат со ќе истражувањето ќе послужат за обезбедување доволна емпириска основа за конципирање на некои нови, идни продлабочени истражувања, за утврдување на тоа каков е односот на општеството кон овој проблем, односно дас е создаде една богата сознајна основа за натамошно делување во насока на справување со овој проблем.

4. Хипотетичка рамка

Врз основа на проблемот на истражување ќе ја дадеме следната

Генерална хипотеза:
Сајбер-тероризмот со неговите најсовремени појавни облици претставува мошне сериозна закана за глобалната безбедност во 21 - от век.

Посебни хипотези:

1. *Тргнувајќи од неговата природа , на многу начини, Сајбер-тероризмот и Интернетот се идеална арена за активностите на терористичките организации.*
2. *Ниту една земја во светот не е имуна на Сајбер-тероризам, и нема целосна и ефикасна заштита од оваа зло.*
3. *Недоволната правна регулираност на полето на информацискатa безбедност претставува сериозен проблем при справувањето со овој вид на криминалитет.*
4. *Широката достапност и застапеност на современите технички средства со кои може да се изврши упад во мрежите или информационите системи на инфраструктурите од витално значење, го прави поширок спектарот на одблици на напад на системот за информациска безбедност.*
5. *За разлика од другите терористички методи, сајбер-тероризмот е безбеден и профитабилен и секако тежок за сузбивање без потребната експертиза, знаење и што е најбитноразбирање на умот на сајбер-терористите.*
6. *Недоволната заштитеност на информациско-компјутерските системи го користат сајбер-терористите за остварување на сопствени цели.*
7. *По софистицирана опрема и пообучен кадар во редовите на безбедносните структури за поуспешно попречување и неутрализирање на сајбер-терористите.*
8. *Брз проток на информации.*

4.1. Варијабли

-Независна варијабла

Сајбер-тероризмот е релативно нов термин и под истиот се подразбира незаконска употреба на сила или насилство врз лица или имот, со цел да се заплаши или присили одредена влада или цивилно население, заради остварување на политички или општествени цели преку експлотација на информатичко компјутерските системи.[15]

-Зависна варијабла

Глобална безбедност претставува безбедност, детерминирана од глобалните интереси и глобалните закани, која ја опфаќа индивидуалната, националната, регионалната безбедност помеѓу кој постои идеалполитичка и/или реалполитичка врска помеѓу секторите (политичко-правен, воен, економски, социјален и еколошки), чија суштина е меѓусебно корегирање, контролирање и моделирање со цел постигнивање на мирот и безбедноста на планетата и луѓето.[16]

[15]Overview of cyber-terrorism.
Преземено од http://www.cybercrimes.net/terrorism/overview/page/1html
[16]Котовчевски, М., Национална безбедност на Република Македонија-прв дел македонска цивилизација, Скопје 2013, стр.63

5.Тероризам

5.1. Дефинирање на тероризмот

Во теоријата можеме да сретнеме различни ставови во врска со дефинирањето на тероризмот, но речиси и да нема разлики во ставот дека тероризмот од секогаш претставувал метод на политичка борба и еден од нејзините најдрастични насилни облици. Повеќе научници го дефинираат на различни начини, но сè уште не е усвоена една општо прифатлива дефиниција за дефинирање на тероризмот. Причини за неуспехот на овој план се бројни, а како најважни се наведуваат тоа што со тероризмот се опфаќаат најразлични акти на насилство и загрозување на човековиот живот и неговите права, како и тоа дека актите на тероризмот речиси секогаш се политички мотивирани, иста појава со исти последици за едни е тероризам, а за други ослободителна војна (идеолошки разлики). Тој денес зазема глобални размери и станува сè поголема опасност за скоро сите земји во светот, без оглед на целите, мотивите и средствата на терористите, како и на нивната конкретна економска, воена и политичка моќ.

Различни автори различно го дефинираат тероризмот и тоа :

Терминот **Тероризам** потекнува од латинскиот збор ***terrere***, што значи ужас, страв и трепет, примена на застрашување, политичко насилство.[17] Тероризмот е тој што владее со застрашување и насилство, главно од политичка природа и предизвикува страв.[18]

Тероризмот е политичко насилство или закана од насилство од страна на групи или поединци, кои намерно таргетираат цивили или неборци, со цел да влијаат врз мислењето или активностите и однесувањето на таргетираната јавност или владите.[19]

Според **Пол Вилкинсон (Paul Wilkinson, 1974),** еден од најпознатите современи теоретичари, теророт претставува: „користење на застрашување со цел да се оствари принуда од страна на револуционерните движења, режими или поединци со политички мотиви", а тероризмот го смета за „систематско спроведување на организиран терор, било од страна на државата, движење или фракција, или од страна на мала група поединци".[20]

Според Котовчевски (2003) општо прифатена дефиниција за тероризам нема, но сепак како можна дефиниција на **тероризмот** односно **терористички акт** би можела да биде: нелегална, противзаконска примена на закана за употреба на сила и примена на систематско насилство, односно извршување на убиства, закани, сеење на страв од страна на поединци, групи,

---

[17] Мала енциклопедија – Савремена администрација, Београд, 1975, стр. 1079

[18] Спасески, Ј., Аслимоски, П., "Безбедност, одбрана, мир", Охрид, 2001, стр.77

[19] *Nacos, B.,L.,*Mass-Mediated Terrorism: The central Role of the Media in Terrorism and Counterterrorism, New York:Columbia University Press, 2006, стр.32

[20] Paul Wilkinson: "Political Terrorism", London 1974.

или организации, насочено против невиното население (или негови делови), сопственоста и владата со цел, да се промени политичкиот курс и да се остварат нивните политички и социјални цели.[21]

Тероризмот претставува психолошки чин планиран да влијае врз јавноста, негова цел е да предизвика страв, што имплицира дека тој страв е насочен и кон некој друг, а не само кон жртвата. Што значи дека терористичкиот акт не е случаен туку е селективен, планиран и рационален и од таквата проекција се очекуваат и ефектите од терористичкиот напад. [22]најголемото оружје на терористите не претставува нападот врз некоја таргетирана цел, туку целта е да се искористат медиумите колку што е можно повеќе, за да се добие максимален публицитет во јавноста и ќе се привлече внимание, а со тоа и се остваруваат своите зацртани цели и идеали.

Дефиницијата на Federal Bureau of Investigation (Федерално истржувачко биро, **ФБИ**), која е поддржана од повеќе автори[23], гласи дека **тероризмот** е бесправно користење на сила и насилство, против лица или сопственост, за да се заплаши или принуди една влада, цивилно население или било кој друг дел од општеството , за остварување на политички или социјални цели.[24]

Тероризмот е смислено, систематско, противзаконско, аморално, специфично, самостојно насилство во вообичаени (мирновремени) услови, или насилство во рамките на некој вооружен судир меѓу одредени колективитети (недржавни, државни или транснационални), чии припадници се убедени до таа мера во основаноста и оправданоста на сопствените екстремистички цели, и опседнати со омраза во однос на примарната жртва (непријателот), па се решени да применат или применуваат , најгруба физичка сила над непосредната (секундарна) жртва, која воглавно ја сочинуваат приватни лица –цивили, со цел нејзино брутално убиство, привремено или трајно повредување, киднапирање и психолошко злоставување, со намера да предизвикаат максимален психолошки ефект (страв), во однос на примарната жртва (владата на земјата која ја напаѓаат) и да ја принудат да ги направи бараните отстапки-чекори, кои значат остварување на крајните политички цели на конкретниот политички колективитет и задоволување на сопствените потреби т.е исполнување на целта.[25]

Голем број на експерти во најголем број на случаи не можат да се сложат за тоа што претставува тероризмот (бидејќи за едни ако некои организации се прогласени за терористички, за други тоа се борци за слобода), затоа и има проблеми во изнаоѓање на една општо прифатена дефиниција, но од друга страна се согласни во тоа што нее тероризам. Една од најсеопфатните и најпрецизни дефиниции за тероризмот, настанала во втората половина на 80-тите години на XX век, и која без оглед на тогаш

---

[21] Котовчевски, М.,Современ тероризам-Македонска цивилизација Скопје, 2003 стр.27
[22] Котовчевски, М.,Современ тероризам-Македонска цивилизација Скопје, 2003 стр. 48
[23] Милошевиќ, М.,Систем државне безбедности, Београд, 2001, стр. 218
[24] Спасески, Ј., Македонија-столб на безбедноста и мирот на Балканот, Скопје, 2005, стр. 185
[25]Мијалковски, М., Тероризам против људске безбедности,Дефендологија-атеоријско стручни часопис за питања заштите, безбедности, одбране, образовања, обуке и оспособљавања, Бања Лука, Јуни, 2009, стр.45

непосакуваната „преобемност" доста успешно се одржала низ времето. Истата гласи: „Современиот тероризам како повеќедимензионален политички феномен, претставува сложен облик на организирано, индивидуално и ретко институционализирано политичко насилство, обележан со застрашувачки физички и психолошки методи на политичка борба, со помош на кои обично во време на политички и економски кризи, а ретко во услови на остварена економска и политичка стабилност на едно општество, систематски се прават напори за остварување на 'големи цели' на начин потполно несоодветен на дадените услови, пред сè општествена ситуација и историските можности на оние кои го практикуваат како политичка стратегија."[26]

Тероризмот е вршење терор, владеење со заплашување, тиранија, уништување на противникот со најсвирепи средства (прогонување, угнетување, убивање).[27]

Тероризмот е специфичен облик на политичко насилство кој поседува неколку јасно изразени особини. Попрецизно кажано станува збор за неколку (зависи кој експерт ги дефинира) основни карактеристики на тероризмот и тоа:

1) *Терористичкиот акт има широко психолошка димензија која има за цел да предизвика терор, исплашеност, несигурност и страв;*

2) *Тероризмот не признава правила, бидејќи самиот се гради и функционира без определен "систем на правила", односно „правила на игра". Тероризмот е кривично дело кое е точно прецизно пресметано од страна на неговите извршители кои располагаат со „свест и совест" за актот што треба да го извршат и тоа секогаш со умисла.*

3) *Не постојат лица, групации или имот кои се имуни и целосно заштитени од терористичките напади;*

4) *Нема невини терористички групации (организации);*

5) *Терористите секогаш однапред со умисла и мошне прецизно ги определуваат своите цели (каде, кога и како напаѓаат);*

6) *После нападите ги чекаат вестите за стравичните напади и бројот на жртви од нивниот грозоморен чин за да добијат на публицитет и тоа што повеќе се крева паника во јавноста тие подобро поминуваат па дури владите потклекнуваат и да преговараат со нив.*

Од самото дефинирање на Тероризмот, произлегуваат и

[26] Симеунович, Д., Теорија политике,наука и друштво, Београд, 2002, стр. 159
[27]Vujaklija, M., Leksikon stranih reci i izraza стр. 947

терористичките цели кои најчесто се од политичка, верска, етничка или идеолошка природа.

Терористичкиот акт се разликува од некој друг акт на насилство, во следниве елементи:

1) Пораката која се пренесува е проследена со страв, ужас, недоверба, убиства;
2) Политичка, верска, етничка или социјална мотивираност;
3) Јавност на актот и обелоденување на организацијата која стои зад извршувањето.

Терористите намерно го користат стравот како средство за постигнување на своите цели. Ефектите на тероризмот врз општеството се фокусираат на чувство на страв, паника и несигурност.[28]

Меѓутоа треба да се нагласи дека терористичките организации не можат да опстојат и да функционираат сами, туку секогаш позади нив стои некоја држава која ги поддржува со пари, со средства, со логистика, политички ги оправдува нивните активности (напади, рекети, масакри и др.) па така терористичките организации за едни се терористи (за тие што се во директен судир со нив), а за други се борци за слобода.

Таа улога што ја играат државите во извршување на терористичките активности условно можеме да ги поделиме во три групи :[29]

1) Држави кои не го поддржуваат тероризмот, меѓутоа тој се спроведува на нивна територија;

2) Држави кои не го спроведуваат тероризмот, меѓутоа го поддржуваат;

3) Држави кои го поддржуваат тероризмот, или од кои доаѓаат програмите и силите кои го спроведуваат;

Рековме дека тероризмот во својата суштина, отсекогаш бил, и останува насилство, но не било какво, туку инструментализирано и целно насилство. Како што потенцира Савиќ, тероризмот е delictum sui generis, специфичен вид на политичко насилство односно системска примена на грубо насилство, вообичаено заради постигнување на политички цели.[30]

Некаде до 90–тите години на тероризмот големите сили гледаа на опасност , но во рамките на една држава, некој помал инцидент со кој верските фанатици или одредени незадоволни групи ќе го искажат со поставување на бомба или киднапирање на одредена личност, но не се сметаше дека тероризмот може да стане глобален проблем пред кој ќе потклекнат и големите сили како САД особено по нападите по 11 септември 2001 година, по што на сите им стана јасно дека тероризмот нема одредени граници или одредена територија на војување, туку претставува глобално војување кое во одреден момент може да зафати се и секого.

Иако помеѓу различни терористички организации постојат многу разлики во однос на нивната големина, методите на дејствување, техниките на вршење на напади, средствата за напад и сл, но како заедничко нешто што

---

[28]Petrovic, D., Samoubilacki terorizam, institute za upotrebno pravo, Beograd, 2009, стр. 97

[29] Котовчевски, М., Национална Безбедност ,Бомат Графикс, Скопје 2011 стр.416

[30] Савиќ, А., Од традиционалног ка постмодерном тероризму, Безбедност, часопис МУП, Р.Србије, број 5, 2004, стр. 661

ги поврзува се мотивите за нивно дејствување, а не како што кажав начинот на кој ќе го изведат теророт. Притоа треба да се прави разлика помеѓу рационалните и психолошки и културни мотиви. При планирање на терористичките напади, организациите секогаш водат грижа за средствата за постигнување на целите, и за целите што всушност сакаат да ги постигнат, притоа раководејќи се од т.н. cost-benefit анализа, односно со што помал влог и ризик до максимален исход. Ако одредена цел може да се постигне со многу помал степен на ризик по егзистенција и дејствување на организацијата, се пристапува кон примена на такви терористички методи кои водат до тој степен на ризик. Психолошката мотивација кај терористите произлегува од нивното лично незадоволство од сопствените животи, и цврстата убеденост дека само како дел од организацијата можат да ја остварат својата замисла во овој живот. Веруваат дека сите луѓе надвор од организацијата се нивни непријатели, и заради тоа им е многу полесно да ги дехуманизираат жртвите на нападите. Поради тоа и не чувствуваат грижа на совест по вршење на делото, и горе-долу им е сеедно каква ќе биде нивната судбина.

Од друга страна, тероризмот е доктрина и метод на борба за одредени цели по пат на систематска употреба на сила.[31] Терористите тежнеат да ја остварат својата цел т.е да го изведат конкретно зацртаниот напад без ни грам повеќе ризик или употреба на сила туку точно толку колку што е потребно за да се добие посакуваниот психолошки ефект, а не што поголем физички ефект. Терористите се борат 'од под земја', и со ограничени ресурси и моќ, против противник кој е непобедлив со воени средства. Затоа и терористичките групи честопати себе се нарекуваат како борци за слобода , кои користат неконвенционални методи за борба, за да компензираат за својата воена инфериорност, и на тој начин избегнуваат директно воено конфротирање.

Терористите генерално прибегнуваат кон вршење на терористички акти, за да ги искажат нивните поплаки и барања, како резултат на повеќе фактори, рационални или ирационални. Овие основни причини најчесто се состојат од повеќе статички или динамички комбинации на фактори и околности, кои се движат од општи кон специфични услови, мотиватори и помагачи. Можат да бидат глобални,регионални или локални, општествени, структурни или психолошки, а некои од нив се поважни од другите.[32]

5.2. Правна легислатива за сузбивање на тероризмот во домашното законодавство

За успешно справување и сузбивање на тероризмот како закана по националната безбедност на државата и безбедноста на граѓаните, Р.Македонија донесе закон со кој сите што ќе преземат акт против државата или други лица од типот на тероризам, или било кој начин ќе го помогнат неговото извршување директно или индиретно ќе бидат казнети. Според Кривичниот законик на Република Македонија насловен како ***'Кривични***

[31] Лексикон на странски зборови и изрази – М. Вујаклија, Просвета 1970

[32] Boskstette, C., Jihadist Terrorist Use of Strategic Communication Management Techniques, George C.Marshall European Center for security studies, Number 20, December,2008, стр.9

дела против државата ' посебно место зазема членот 313 насловен како ' ***Терористичко загрозување на уставниот поредок и безбедноста*** ' *„Тој што има намера да го загрози уставниот поредок или безбедноста на Република Македонија ќе предизвика или сериозно ќе се закани со предизвикување експлозија, пожар, поплава или друго општоопасно дејствие или акт на насилство, создавајќи чувство на страв или несигурност кај граѓаните, ќе се казни со затвор најмалку 10 години".*[33]

Тероризмот како кривично дело е инкриминиран во Кривичнио законик на Р.Македонија, во триесет и третата глава ***'Кривични дела против јавниот ред' во член 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 лица, уништување на јавни објекти, транспортни системи, објекти на инфраструктура, информациони системи и други објекти во општа употреба, или трговија со нуклеарно оружје, биолошки, хемиски, опасни радиоактивни, отровни и други опасни супстанции, или предизвикување на 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 чувство на несигурност или страв кај граѓаните,ќе се казни со казна затвор од најмалку 10 години или со доживотен затвор."*[34]

Кривичното дело тероризам, според описот, содржи повеќе дејствија на извршување, или припрема за нејзино извршување како на пр: вршење на обука или на друг начин подготвување на други лице за извршување на дела од ваков тип, организирање на изработување, како и самата подготовка, купување, изработка и продажба на експлозиви или друго огнено оружје или опасни супстанции кои се наменети на извршување на дела од ваков тип, се казниви и подеднакво се третира како терористички акт и се смета за кривично дело исто по член 313.

Освен наведените дејствија со истиот член се опфатени и закани и извршување на дела –непосредно или посредно со примена на електронски средства или на друг начин, како и инкриминациите – повикување со ширењеили на друг начин, ставање на располагање на јавноста - порака со намера за поттикнување или повикување на извршување на такви дејствија.

За постоење на делото, доволно е да биде превземено само едно од наведените дејствија, и со истото да биде остварена целта, а тоа е загрозување на животот и телото и создавање на чувство на несигурност кај граѓаните.

Во Кричниот Законик на Р. Македонија, во **член 394-а,** инкриминирано е создавањето на ***Терористичка организација,*** *" Тој што создава група, банда или друга злосторничка организација за извршување на кривични дела на: убиство, телесно повредување, грабнување на лица, уништување на јавни објекти, транспортни системи, објекти на инфраструктура, информациони системи и други објекти во општа употреба, грабнувањена авиони или други средства на јавен транспорт, производство, поседување или трговија со нуклеарно оружје, биолошки, хемиски, опасни радиоактивни, отровни и други опасни супстанции, или*

---

33 Камбовски, В., Кривичен Законик,Интегрален текст, предговор, кратки објаснувања и Регистар на поими, ЈП Службен весник на РМ, Скопје, 2009 стр.257, Чл.313

34Ibid, стр.312, Чл. 394-б, став 1

предизвикување на пожар или експлозија, уништувањена постројки за снабдување со вода, енергија или други основни природни извори, со намера загрозување на животот и телото и создавање чувство на несигурност или страв кај граѓаните."[35]

Нашата држава како и другите држави во светот заради успешно справување со тероризам и со терористички акти предвидела со закон кривична одговорност за припадниците на група, банда или друга злосторничка организација, а инкриминирано е и јавно повикување, поттикнување или подржување на создавање на терористичка организација.

Во **членот 394-в,** е предвидено и кривичното дело ' ***Финансирање на тероризам***' каде се предвидува кривична одговорност за лицето кое обезбедува или собира средства на било кој начин директно или индиректно, незаконски или свесно, со намера тие да бидат употребени или со знаење дека ќе бидат искористени целосно или делумно заради извршување на конкретно пропишаните кривични дела:

- Тероризам;
- Меѓународен тероризам;
- Загрозување на лица под меѓународна заштита;
- Загрозување на безбедноста во воздушниот сообраќај;
- Терористичко загрозување на уставниот поредок и безбедноста;
- Злосторство против човечноста;
- Земање заложници [36]

И друго дело на убиство или тешка телесна повреда извршени со намера да се создаде чувство на несигурност и страв кај граѓаните. Крајната цел на сите терористички дејствија што се презимаат против безбедноста на државите или поединците е политичка заднина за остварување на своите барање и доведување на владите во состојба на преговори со нив за остварување на своите цели.

Домашното законодавство при кривично - правното одредување на тероризмот води грижа за меѓународно-правната легислатива и усогласување на нашето законодавство со истата.

Ваквите континуирани промени во националната законодавна регулатива во Република Македонија, одат во прилог на воспоставување на солидна база за успешно спротивставување на тероризмот, а особено на неговите современи форми.

---

[35] Камбовски, В., Кривичен Законик, Интегрален текст, предговор, кратки објаснувања и Регистар на поими, ЈП Службен весник на РМ, Скопје, 2009, стр.311, чл.394-а

[36] Подетално за секое од наведените КД, види во Камбовски,В., кривичен Законик, Интегрален текст, Предговор, кратки објаснување и Регистар на поими, ЈП Службен весник на РМ, Скопје, 2009

5.3. Одредување на тероризмот како асиметрично војување во глобалниот свет

Доколку ги разгледуваме и анализираме војните, воените дејствија, начинот на војување до ерата на тероризмот ке увидиме дека ни тогаш не постоела некоја симетрија во војувањето – војување помеѓу еднакви опоненти односни противници, а асиметричното војување всушност било правило, односно нормата.

Меѓутоа, после Студената Војна на сите им беше јасно дека стариот традиционален начин на војување веќе не постои па почна да се развива ерата, т.е да доаѓа времето на тероризмот каде многу помали опоненти односно групи па дури и поединци ќе ги тресат многу посилните, помоќните при што станува збор за нов тип на војување, за војни без терени и бојни полиња.Во борба против тероризмот непријателот е без профил и име.

Доколку зборуваме за вештината на војувањето, во предвид мораме да земеме 5 димензии:

1) Простор–ги опфаќа местото, длабочината, сферата;

2) Генијалност–се однесува на поседувањето на лидерски квалитети, употреба на неконвенцијални активности и/или одбивање да се следат конвенциите;

3) Знаењето–тоа подразбира високо квалитетна, и од значење за мисијата информација, која е достапна на едната страна , но се држи во тајност да не ја дознаат противниците, со цел да се гарантира супериорноста во поглед на квалитативното знаење;

4) Време–се однесува на брзината, издржливоста, посветеноста или комбинација од сите нив;

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

Големите воени раководења се всушност уметност во креирање и примена на асиметрија во сите пет димензии.[37]

Карактеристично за асиметричните конфликти и асиметричното војување е тоа што станува збор за противници кои имаат значајни квантитативни и квалитативни разлики и тоа :

- ✓ Разлика во мотивите;
- ✓ Разлика во квалитетот или карактерот на самите методи;
- ✓ Различно легитимирање;

[37]Baskstette, C.,. Jihadist Terrorist Use of strategic Communication Management Techniques, George c. Marshall European Center for security Studies, Number 20, December, 2008, стр. 7

- ✓ Разлика во аплицирањето на методите;
- ✓ Дисбаланс на силите.

Најголема одлика на терористите и на тероризмот претставува асиметричноста на војување каде се војува со противник кој е многу понадмоќен, се војува против цела армија, со најмодерно оружје т.е против цела држава, а од друга страна се наоѓа една организација, група или поединец (во случај на сајбер-тероризмот) кои во најголем број случаи на заплашување и сеење страв кон населението, со акции од типот да се удри каде најмалку очекува и по недолжно цивилно население, кое доколку владата не преземе нешто ја губи довербата кон неа, а владата е немоќна да се справи и да ги предвиди потезите на терористите кои напаѓаат брзо, кога најмалку се очекува и со голем ефект и шок врз населението.

Таа асиметрија на војување на терористите кои многу умно и пресметано ја користат уште побрз и поголем ефект добиваат во комбинација со мас-медиумите без кои нивните подвизи би останале локализирани на едно подрачје и не би добиле глобални размери, што е уште едно оружје кое терористите успешно го користат.

Еве размислувања на некои автори во врска со асиметричноста во војувањето:

- Терористите ги знаат своите цели, додека државите војуваат против невидлив[38]непријател, бидејќи наспроти огромниот државен безбедносен апарат вообичаено стои еден или помала група на терористи.

- Бомбаш–самоубиец или сајбер-терорист можа да крене во воздух нуклеарна централа со што може да уништи илјадници животи, па и цел град.

- Државите стојат наспроти наднационалните терор-организации;

Глобалната војна против тероризмот е *асиметрична* по повеќе основи.[39] Таа би требало да претставува доказ за новиот вид војни, кои во иднина ќе доминираат и ќе се водат меѓу државни и недржавни актери. Асиметријата не е само во видот на противници, туку и во начинот на војување, употреба на средства/оружје, но Мец ја нагласува и етичката асиметрија. Но, критичарите додаваат дека во ваквата војна во која „светот е обединет против најголемото зло" асиметријата се состои во тоа што противникот се декларира како нечовек.[40] Според нив, асиметричната војна е конфликт во кој опремениот дел на предоминантна воена сила се обидува да го уништи непосредливо послабиот непријател војувајќи на неконвенцијален, па и на нелегален начин.

---

[38] Непријател (сајбер-терорист) кој има лажно име, може да дејствува од другата страна на светот,

[39]Steven Metz, "Strategic Asymmetry", *Military Review*, July-Avgust, 1997.

[40]Alessandro Dal Lago, "The Global State of War", *Ephemera – Global Conflicts*, vol. 6, no 1, February 2006

Драстичното зголемување и интернационализација на тероризмот, неговото глобално дејствување и се поголеми ефекти, дозволи со право да зборуваме за ескалација на тероризмот.[41]

Тероризмот по Студената Војна еволуираше и стана суштинска закана за меѓународната безбедност. Затоа ќе мора да ги прифатиме анахроните начини на размислување и парадигми ако сакаме да му се спротивставиме.[42]

5.4. Карактеристики на современиот тероризам

Тероризмот уште со самиот почеток на новиот милениум, остави јасна порака дека деновите во иднина ќе почнуваат и ќе завршуваат со неговите разорни и застрашувачки ефекти.

Терористичките напади изведени на 11-ти септември 2011 година само ја потврдија неговата решеност тој да се промовира како најголема и најопасна глобална безбедносна закана. Тероризмот секојдневно се менува и денес најмалку е само маргинален, локален и безначаен проблем, трансформирајќи се во нови софистицирани облици на кои драматично се разликуваат од оние во минатото.[43]

Можеби стариот начин на терористичко војување терористите го менуваат со нов поефикасен, поенергичен, што на голема врата тоа им го овозможи брзиот развој на информациско – комуникацискиот бум што го зафати светот во последната деценија, но сепак идејата, карактерот на тероризмот е таа без разлика со кој метод се постигнува целта, да се заплаши, да се нанесе штета, да се уништи без притоа водејќи сметка дали ќе се нанесе удар врз воена база, метро, училиште, градинка или аеродром.

Карактеристично за нападите на терористите од поново време е тоа што порано нивните напади се симболизираа со помал број на жртви, само што поголем степен на паника и страв што во поново време предизвикуваат смрт на огромен број на луѓе. На тој начин, својот традиционален принцип"зад нас ужас, а пред нас паника" го издигнуваат на највисоко можно ниво.[44]

Анализирајќи ја еволуцијата на тероризмот низ годините, важно е да се забележат големите разлики внатре во самата поставеност и начин на организирање, целите, мотивите и врските во самите групи. Воочени се карактеристики, кои во период пред десет или дваесет години не постоеле:

- Глобализација на тероризмот (дејствуваат во две, три или повеќе држави односно континенти)–најголема одлика на современиот тероризам;

---

[41]Милошевиќ, М.,Стајич, Љ., Модалитети борбе против тероризма у савременим условима, НБП Наука-безбедност-полиција, Часопис Криминалистичко-полицијске академије, Београд, Vol III No.2, 91-105, 1998, стр. 105

[42] Кронин, К., О., Лудс, М., Ц.,Напад на тероризмот: Елементи на грандиозна стратегија, Скопје, Нампрес, 2009, стр. 1

[43] Котовчевски, М., Борба против тероризмот, Македонска цивилизација, Скопје, 2004 стр.11

[44] Мијалковски, М., Тероризам против људске безбједности, Дефендологија- Теоријско стручни часопис за питања заштите, безбједности, одбране, образовања, обуке и оспособљавања, Бања Лука, Година XII, Бр. 25-26, Јуни2009, стр. 44

- Користат широко достапна технологија за брза и безбедна комуникација;
- Нападите во поновиот период им се многу посмртоносни, и предизвикуваат што поголем број жртви, а не само предизвикување паника и страв;
- Нивните финансиски и логистички мрежи ги надминуваат националните граници, се повеќе имаат извори од свои симпатизери и подржувачи ширум светот;[45]

Самите карактеристики на современиот тероризам, упатуваат на мултидимензионалноста на појавата и потребата од мултидисциплинарен пристап во нејзиното спротивставување.[46] Тероризмот мошне брзо го менува својот карактер, но не и своите цели, кои се многу поамбициозни, подраматични и веќе добиваат глобални димензии. Тој е 'флуиден непријател', но со јасно поставени цели кои секојдневно предизвикуваат страв, ужас, бес, желба за одмазда и крв, и нов психолошки и безбедносен амбиент, во кој луѓето во светот почнуваат да се чувствуваат како да се во војна.[47]

Современиот глобален тероризам им остава јасна порака на големите сили дека ниедна држава не е имуна на нивните напади, дека нивните операции стануваат се посмртоносни и дека не се бираат начини и средства за нивно извршување, оттука може да се заклучи дека со брзиот развој на технологијата и компјутеризацијата на секој дом, терористот може да допре до секое семејство .

5.5. Современи форми на тероризам

Иако тероризмот и терористичките тактики се усовршуваат начините на извршување во најголем број случаи останува ист.

Како најраспространет и најомилен метод на терористите се бомбашките напади, освен нив мошне популарни се и киднапирањата и вооружените напади, како и земањето заложници, атентатите, киднапирањето авиони, сакатењето и подметнувањето пожари.

Сепак како најсовремени форми на тероризмот во литературата се споменуваат ***самоубиствениот тероризам*** *и* ***тероризмот со примена на оружје за масовно уништување.***

- ***Самоубиствениот тероризам*** или како што ги нарекуваат бомбаши – самоубијци претставуваат нови камикази односно нова,

[45]Савиќ, А., Од традиционалног ка постмодерном тероризму, Безбедност, Часопис МУП, П.Србије, број 5, 2004, стр. 664

[46]Derencinovic, D., Novi antiterorizam na razmedju depolitizacije I dejuridizacije, Zbornik Pravnog Fakulteta u Zagrebu, 2002/3-4, str. 3-4

[47] Димовски, З., Тероризам, Скопје, 2007, стр. 105

современа верзија на претставниците на современата секта позната како Асасини.[48]

Значи овој начин на тероризам постои од дамнешно време само што се повеќе се усовршува и применува од страна на терористите.

Најчест начин на дејствување на терористите самоубијци е со динамит или во возило со експлозив да влезат на непријателска терирорија и да се активираат, за доброто на својата организација, народ или вера.

Боаз Ганор, извршен директор на Институтот за противтероризам од Израел распознава шест карактеристики на самоубиствен напад:

- Привлекува широка медиумска репортажа и со тоа влијае на наметнување на саможртвувањето меѓу терористите и идните регрути;
- Самоубиствениот напад резултира со многу несреќни случаи и предизвикува екстензивна штета;
- Многу е тешко да се спречат и предвидат самоубиствените напади кога терористите ќе нападнат и која ќе им биде метата;
- Самоубиствениот напад е многу прост и примитивен. Употребата на самоубиствената тактика гарантира дека нападот ќее биде извршен во најсоодветно време и на најсоодветно место со оглед на локацијата на метата;
- Планирањето и изведувањето на на бегство после терористичкиот напад е вообичаено најтешкиот дел од нападот. „самоубиствениот терористички напад не бара план за бегство";
- За терористот-самоубиец не постои страв дека ќе биде заробен и испрашуван од страна на безбедносните сили и дека ќе даде информации кои можат да ги загрозат останатите активисти.[49]

❖ Освен самоубиствениот тероризам, се почеста и поприсутна е заканата од страна на терористичките организации за биолошки, хемиски или нуклеарен напад т.е да употерби ***оружје за масовно уништување*** (WMD)[50] за остварување на терористички цели.

Биолошки тероризам претставува употреба и ширење на различни опасни материи од биолошко потекло (различни видови микроби) во големите градски центри и пошироко, со цел да се предизвикаат бројни опасни последици и да се поткопа моралот на нападнатата нација.[51]

Можноста за употреба на ***биолошко оружје*** од страна на терористите е многу реална и во иднина уште повеќе ќе се зголемува поради:

- Огромни човечки загуби;

---

[48] Котовчевски, М., Борба против тероризмот, Македонска цивилизација, Скопје, 2004, стр.71

[49] Ganor,B., достапно на:http://www.ist.org.il/articles/articledetcfm?articleid=128

[50] Под WMD (weapons of mass destruction) – го опфаќа арсеналот на нуклеарното, биолошкото и хемиското оружје.

[51] Котовчевски, М., Современ тероризам Македонска цивилизација, Скопје, 2003, стр. 195

- Релативна достапност на технологија за производство;
- Можност тајно да се употреби;
- Не дозволува можност за одговор;
- Економска штета.

Хемиско оружје го сочинуваат хемиски материи познати како бојни отрови – кои претставуваат токсични соединенија кои применети за остварување на терористички цели, предизвикуваат повреди на цивилното население и безбедносните сили и ја контаминираат животната средина во која се применуваат.

Првиот напад со хемиско оружје светот го искуси во блиската 1995 година, кога јапонскиот култ Аум Шинрикјо испушти хемиски средства во токиското метро. Ефектите од овој напад беа 12 мртви, илјадници повредени, но најтежок беше психолошкиот ефект кој беше постигнат.[52]

Хемиските агенси можат да бидат во вид на капки, пареа, дим или гасови во опасни концентрациина одредено подрачје, воздух и вода или во одреден затворен простор.

Нуклерно оружје е таков тип на оружје кое при нуклеарна експлозија (фусија и фисија на честиците), односно термонуклеарни реакции доаѓа до ослободување на огромно количество на енергија и радиоактивни продукти и тоа за многу краток временски период. Од класичната експлозија се разликува по количината на ослободената енергија и природните промени до кои доаѓа кај експлозивот.[53]

Според бројот на човечки жртви, материјална штета и психолошки ефект можната употреба на вакво оружје би имало драматични последици.

Меѓутоа употребата на нуклеарно оружје за терористички цели, е многу помалку веројатно од употреба на биолошко и хемиско оружје.

Освен ***самоубиствените терористички напади, и оружјето за масовно уништување,*** во современите општества, со развојот и напредокот на технологијата , се јавуваат и допуштаат можности за појава на тероризмот во ***нови појавни облици.***

Брзиот развој на технологијата, кој беше замислен да биде достапен за секого со намера да им го олесни животот на луѓето, особено со воведување на интернетот и неговата широка застапеност покрај позитивните донесе и негативни страни кои беа искористени од луѓе спремни да го искористат како оружје и да ги злоупотребат неговите можности.

Новиот современ облик на тероризам–го доби префиксот Сајбер[54],во

---

[52] Котовчевски, М., Национална безбедност, Бомат Графикс–Скопје, 2009, стр. 428

[53] Кеча, Р., Тероризам – глобална безбједносна пријетња – Европски дефендологија центар за научна, политичка, економска, социјална, безбједносна, социјална и криминолошка истраживања, Бања Лука, 2012, стр. 158

[54] Префиксот **сајбер** (англиски-cyber) е дефиниран како префикс поврзан со компјутерите, и се употребува во најголемиот дел на кобаниците кои се однесуваат на компјутерскиот свет:сајбер-простор(cyberspase), сајбер-култура(cyberculture) итн. Изведен е од терминот cybernetics(кибернетика) кој пак потекнува од тсрогрчки термин kybernao (управувам , владеам), и со кој се означува науката за комуникацијата и теоријата на управувачките

литературата познат како ***Сајбер-тероризам.*** Сајбер тероризмот е развој на традиционалниот тероризам во една нова арена со користење на други средства, но соисти политички и идеолошки цели.

Сајбер–тероризмот всушност претставува конвергенција од тероризам и компјутерска технологија, на начин што терористите на незаконит начин ги искористуваат информациско-комуникациските системи и прибираат податоци кои ќе им помогнат за напад на критичните инфраструктури. Сајбер-терористичките напади можат да бидат насочени против воени објекти, владини објекти, цивилни лица, а сето то се постигнува со директен напад врз база на податоци, со цел да се да се соберат чувствителни информации за одредени цели, нивната структура и нивото на информацискатa сигурност, како и да се постават корумпирани информации во чувствителните бази на податоци кои се под контрола на терористите или со самото нивно уфрлување во системот би се предизвикал хаос и би се изгубила контрола над системот. Целта на сајбер-нападите се исти како и кај останатите видови на терористички напади да се предизвика штета и да се генерира страв кај населението.

Тероризмот со своето лудило во минатиот век, им зададе големи маки на безбедносните сили за негово справување и сузбивање, што ни покажува фактот дека во XXI-от век, тој стана уште поголемо зло и закана за глобалната безбедност кој напредува со своите облици со ширење на терор, и неможноста на системите за создавање на успешен механизам за борба против него.

Со оглед на тоа дека предмет на наш интерес е токму сајбер – тероризмот, како современ облик врз глобалната безбедност во светот, на истиот ќе му посветиме централно место и ќе го разработиме посебно и поопширно.

системи. Превземено од http://www.Komunikacija.org.rs/komonikacija/casopis/sociologija/XLI2/d006/html ser lat# ftn 1

6. Информационата технологија и нејзиниот развој

6.1.Историски осврт

Информатичката технологија, стана круцијален ресурс за сите промени, кои во помала или поголема мера континуирани се одвиваат во сите сегменти на планетата. Денеска е тешко да се замисли , а уште потешко квалитетно и успешно дасе одработат и основните работи без употреба на информатичката тахнологија, бидејќи таа е навлезена ви сите пори на на човековата егзистенција до таа мера да човековата зависност од ваквата технологија стана толку висока на дури и ранлива.

За да во целост ги сфатиме и разбереме процесите, кои во глобалната општествена заедница се одвиваат под влијание на инфор-технологија, корисно е да се погледне кон не толку далечното минато. Првите комерцијални компјутери во однос на денешните, димензионално биле поголеми, со повисока цена, со скромни перформанси и со не-толку јасна намена.[55]

На крајот од работното време, корисниците морале да ја бришат компјутерската меморија, да ги приберат искористените магнетни ленти, да ги сместат во складишни простори наменети за чување.

Значи безбедноста на компјутерите пред неколку децении била перцепирана како дел од планот за физичка заштита односно се водело грижа за спречување на кражби на компјутерска опрема и дискови.

Со тек на времето, компјутерската технологија непрекинато се развивала, па корисниците се почесто започнале да остваруваат инеракција со компјутерите, а можноста за пристап до компјутерите од оддалечени места, ја еволуираше и компјутерската ера. Со ширењето на телекомуникациите, се бележи раст и на компјутерските мрежи, кои освен што станувале се поголеми, растела и нивната комплексност. Многу големи фирми започнале да гиавтоматизираат и складираат податоците за своите клиенти, снабдувачи и комерцијални трансакции.

Образовните установи ја откриле можноста за поврзување во големи компјутерски мрежи и за централизација на компјутерски бази на податоци. Компјутерската достапност, за студентите значеше можност за експериментирање и доусовршување.

Воведувањето на персоналните компјутери во канцеларите и во домовите во 80-тите години, овозможи пристап до уште поголем број на корисници. Како што цената на компјутерите започна да опаѓа, многу мали фирми во тоа видоа можност да ги автоматизираат своите операции, за да останат конкурентни на поголемите компании. Но со развој на персоналните компјутери се намалуваше информационата безбедност. Луѓето сега можат дома да креираат програми за да крадат информации или да ги нарушуваат операциите, а можеа и слободно да комуницираат едни со други со помош на компјутерските-мрежи. Така во таа слобода на компјутерско поле се отвори едно ново игралиште за корисниците кои добро се снаоѓаа во тој амбиент. Ако

---

[55] Податоци превземени од „ Избор на компјутер –звездата што сјае" Дејан Ристановиќ, Racunari 1984, januar broj 1 str.6

претходно тие можеа во исто време да навлезат во еден единствен систем и тоа преку модем, сега имаат потенцијал да пристапат кон многу системи во светот со еден единствен упад. Ако минатото безбедноста не претставувала главна грижа, со појавата на интернетот, и можноста да се досегне до било која мрежа, таквата грижа стана глобална.

Во поново време сме сведоци на тоа до каде стигна информационата технологија каде што имаме се почести случаи на директни јавувања и преноси на воjни, протести, масовни немири со помош на комуникациски програми како Скајп, потоа користејќи ги социјалните мрежи како Фејсбук, Твитер, блогови или разни снимки на Youtube се покажа во праксата дека тие се моќни средства за ширење на пропаганда, перење мозоци, наметнување на јавно мислење со манифестирање на на сопствени акти, пуштање на снимки за заплашување кои се достапни до секој дом, сето тоа ни укажува на сложеноста на глобалното општество и придонесот на информационата технологија за тоа.

6.2.Интернетот како глобална мрежа

Интернет (*engl.Internet)* во буквален превод би значел „меѓумрежа" или семрежје е јавно достапен систем на меѓусебно поврзани персонални сметачи во мрежи од целиот свет, кои пренесуваат и складираат податоци во форма на пакети со користење на стандардно множество на протоколи означено како **TCP/IP**. Интернетот се состои од голем број мали и големи, домашни, странски, деловни владини и невладини мрежи кои што заедно пренесуваат различни информации и услуги, како електронска пошта, директен разговор, како и меѓусебно поврзани мрежни места (websites) и други документи од **web** односно *Пајажина* (Светска пајажина – World Wide Web, WWW).

Како зачеток на интернетот се смета 1969 година кога е направен првиот успешен обид за мрежно поврзување на повеќе компјутери во компјутерска мрежа кои меѓусебно комуницираат.[56]Мрежата се нарекувала со името Advanced Research Projects Agency Netwrok (ARPAnet)[57], и е создаден со иницијално меѓусебно поврзување на четири персонални сметачи на различни универзитети во САД и тоа:

- Калифорнија Универзитет во Санта Барбара, (University of California, UCSB – Santa Barbara);
- Калифорнија Универзитетот во Лос Анџелес, (University of California, UCLA-Los Angeles);
- Јута Универзитетот во Солт Лејк Сити (University of Utah- Salt Lake City);
- Истражувачкиот институт Стенфорд, (Stanford Research Institute, SRI).

Основна намена на ARPAnet мрежата била одржување на одбрамбената

[56] Достапно на веб http://www.let.leidenuniv.nl/history/ivh/chap2.htm

[57]History of ARPANET достапно на http://inventors.about.com/library/weekly/aa091598.htm

политика на државата т.е за потребите на Американското министерство за одбрана со која би се овозможила комуникација и во услови на нуклеарна војна (која во тој пероид била под постојана закана), и оваа мрежа функционирала се до 1989 година кога била заменета со пософистицираниот мрежен систем The National Science Foundation Network (NSFnet).[58]

Интернетот првично беше замислен како огромна база на податоци за користење на научни и образовни цели кој го користеле само компјутерски професионалци, инженери и научници кои биле запознаени со неговиот комплексен начин на функционирање.

Како што е истакнато погоре замислата на министерството за одбрана на САД да развие мрежа што ќе овозможи пренос на информации и комуникација во услови на војна па дури и нуклеарен удар прерасна подоцна во глобална развиена светска мрежа. Интернет која денес има неколку милијарди луѓе кои имаат пристап до мрежата и се нејзини корисници. Значи тоа се зачетоците на интернетот, но кога би ја спомнале и TCP/IP мрежата согласно расположивите податоци, истата е направена на 1 јануари 1983 година, така да овој датум многу научници го сметаат за датум на создавање на Интернетот.[59]Во тој период интернетот бил ограничен и бил достапен за употреба на универзитетите, војската и некои други државни организации во САД и бил наречен национална научна фондација–(National Science Fondation, NSF).[60]

Во средината на 1989 година Тим Бернерс-Ли (Tim Berners Lee) од Европската организација за нуклеарно истражување (The European Organization for Nuclear Research, CERN) го доставил проектот *Worl Wide Web* за изработка на единствен хипер текстуален програм за дистрибуција на податоци помеѓу луѓето, а две години подоцна се претставени и HTTP протоколот и HTML кодот. Неколку години подоцна во ноември, 1993 година бил создаден и првиот пребарувач наречен *Mosaic Web Browser*.[61]

После повеќе од пола век постоење на електронската технологија, луѓето успеале да го прошират електронскиот нервен систем во глобални рамки, надминувајќи ги границите на просторот и времето, успеале да ја покријат нашата планета се до каде што се простираат нејзините физички граници. Интернетот го направи тоа што визионерот на комуникацијата Маршал Меклуан (Marshall McLuhan) го нарече 'глобално село'[62] конечно да стане реалност.

Поради брзиот пренос и проток на информации интернетот стана најраширена глобална мрежа која го зафати целиот свет. Во повеќето делови во светот корисници на интернет се веќе 80 % од населението како на пример САД, Австралија 53%, а Европската Унија околу 50 %. Најголеми корисници на интернетот се најразвиените земји.

---

[58]The Launch of NSFNET достапно на
httpwww.nsf.gov/about/history/nsf0050/internet/launch.htm
[59]Joe Casada Teach Yourself TCP/IP in 24 hours, 2003, third edition, p11
[60]The Launch of NSFNET достапно на
httpwww.nsf.gov/about/history/nsf0050/internet/launch.htm
[61]Michael Calore *Mosaic Browser Lights Web With Color, Creativity, 2010* достапно на веб http://www.wired.com/thisdayintech/2010/04/0422mosaic-web-browser/
[62]*MarshallMcLuhan Foresees The Global Village,* Преземено од: http://www.livinginternet.com/i/ii_mcluhan.htm

Како корисници на интернет на големи врата влегоа и терористи и терористички групи кои го користат за ширење на својата пропаганда, да остваруваат контакти и комуницираат со своите подржавачи, да ги придобиваат симпатиите на јавноста за нивните каузи, да организираат протести, дури и да планираат и извршуваат операции.

Денеска интернетот овозможува повеќекратни услуги:

1. **Информации**, преку
   - World Wide Web - Светска пајажина (WWW);
   - Новински групи–споредливо со списанија посветени на различни теми.

Како комуникациски системи се јавуваат новинските групи преку кои луѓето искажуваат различни интереси и хобија, разменуваат информации, дискутираат на различни теми, општи и одредени или поставуваат прашања.

2. **Комуникација**, преку
   - Праќање и примање на писма:
     - Програма за разговарање: преку директна врска слична со телефонски разговор, што се овозможува преку програма која овозможува разговор во реално време[63]
     - Конференции: преку директна и истовремена врска помеѓу повеќе корисници
     - Електронска пошта (e-mail): преку индиректна врска, слична на пошта[64]
     - Дискусни групи: преку размена на пораки во рамките на една група(дискусни групи, новински групи)[65].

VoIP-Voice over Internet Protocol овозможува телефонски разговор преку комјутерски, податочни мрежи како што е на пр.интернет наместо преку старата телефонска мрежа. Иницирање на VoIP може да се направи преку стандарден телефонски апарат поврзан на адаптер или преку персонален компјутер поврзан на интернет. И во двата случаи можно е да се повика стандарден телефонски број каде било во светот или друг персонален

---

[63] Оваа услуга овозможува комуникација во реално време преку впишубање 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 коминицираат истовремено.(Yahoo Messenger, MSN Messenger)

[64] Пораката која се нарекува и-меил претставува пишан текст на кој корисникот може да прикачи слики и звуци или други видови на документи.

[65] Дискусиски форум (скратено форум) е множество од веб страници каде корисниците можат да ги читаат пораките испратени од членови на различни категории класифицирани во однос на теми. Корисниците можат да одговорат на пораките во однос на испратените теми или можат да испратат порака на нова тема во рамките на претходно постојна категорија, или пак да создадат целосно нова категорија.секој форум има администратор кој ги поставува правилата на испраќање на пораките и правата на корисниците. Пр. Форумот на Македонската управа за јавни приходи е: http://www.ujp.gov.mk/forum.forum.php

компјутер поврзан на интернет.[66]

- Пренос на податоци:
  - Прикачување на датотеки кон пренесуваните пораки со помош на електронска пошта (e-mail);
  - FTP услуга (протокол за пренос на датотеки), што овозможува брз пренос на датотеки, особено за поголеми датотеки, на пример во креирањето на сложени веб-страници, со богати информациски содржини);
  - P2P (peer to peer) мрежа од точка до точка, што овозможува копирање на датотеки од други компјутери бесплатно или по одредена поволна цена;[67]
  - Преземање од интернет преку WWW.

Интернет е глобална поврзана компјутерска мрежа (Global Area Network, GAN) која овозможува пристап до информации и други ресурси. Кој било компјутер поврзан на интернет може да комуницира со секој друг компјутер исто така поврзанна интернет, па оттука на интернет се глада како огромна мрежа составена од милион компјутерски мрежи од сите видови (LAN[68] +MAN[69]+WAN[70]).

За да станеме корисник на интернет, мораме да се логираме што значи дека треба да поседуваме корисничко име и лозика без кој не би можеле да ја користиме интернет мрежата. Една личност може да име повеќе интернет адреси и кориснички имиња.

Со оглед на тоа дека секој може да се поврзе на интернет без никакви ограничувања, тој се смета за јавен сервис.[71]

Интернетот е децентрализирана мрежа во смисла на тоа што не постои ниту една институција или држава која управува со работата на интернетот. Тој е финансиски и логистички подржан од страна на компаниите кои имаат пристап до него, а неговата организација од гледиште на техниката е надгледувана од страна на комисија наречена-*Internet Corporation for Assigned Names and Numbers (ICANN).*

Како технологија интернетот нуди многу можности што другите

---

[66] Најпопуларниот претставник на VoIP технологијата денес, со најголем број на корисници е Скајп (Skype, види: www.skype.com), кој што е слободен за преземање и разговорите од персонален компјутер кон персонален компјутер се бесплатни, додека пак разговорите кон стандарден телефонски број се наплаќаат, но по значително пониски и поповолни цени.

[67] Во моментот најпопуларна употреба на P2P апликациите е заедничко користење и префрлање на датотеки.

[68]LAN (Локална компјутерска мрежа)–локалните мрежи се во рамките на еден стан, зграда, делови од училиште/факултет или територија на едно претпријатие. Тие најчесто не надминуваат неколку стотици квадратни метри.

[69]MAN (Метрополска мрежа)–попроширени мрежи кои опфаќаат области на една локација/град меѓусебно поврзани со LAN во самата област.

[70]WAN (Отворена мрежа)–мрежи кои покриваат поголеми области како на пример една земја или цел континент.

[71] Прирачник за информатичка и комуникациска технологија, USAID, Проект за електронска Влада, Скопје, 2006, стр. 15

медиуми не го можат како на пр:

1) Интернетот е евтин и едноставен за користење. Спрема другите начини на комуникација цената е занемарлива;
2) Интернетот овозможува безгранична комуникација од ширум светот, без никакви правила или законитости;
3) Интернетот овозможи комуникацијата во сите делови на светот да се одвива со голема брзина што не го може ниту еден друг медиум;
4) Интернетот овозможува мулти – насочен обликна комуникација. Интерактивноста е многу важна алатка за градење на одредени групи и за само определување на групите;
5) Им со помош на мас-медиумите и социјалните мрежи интернетот овозможува глобализација на своите проблеми, како и искажување на својот револт по пат на ширење на апел или повик за масовни движења привлекувајќи широка народна маса и публикација;
6) Интернетот овозможува интеграција и конвергенција на различни медиуми во форма на текст, аудио и визуелен запис;
7) Интернетот се користи како алатка " par excellence " бидејќи е неминовно средство за планирање, организирање и координирање на терористите и нивните активности. Мобилизацијата, регрутирањето и обезбедувањето на подршка, е многу олеснето преку интернетот.[72]

Како современа информациона технологија, интернетот има имресивни резултати во сите области на секојдневното функционирање, и без него би се нарушило успешно фукционирање на општеството:

- Одбраната;
- Националната безбедност;
- Државната управа;
- Работењето;
- Научно – истражувачката работа;
- Здравствената заштита;
- Едукација.

Интернетот претставува важна алатка за ширењето на информации, навлегувајќи во сите пори на човековото работење и егзистирање со тоа што им го олесни начинот на работа и комуникација. Сите операции од најпрости до најсложени денеска поминуваат низ интернет мрежата од видео игри за деца па до трансфери на милионски суми на пари. Исто така граѓаните имаат неограничен пристап до јавни информации[73].

---

[72] Terzis, G., Smeets, B., E-initiatives and the information Management of Ethnopolitical Conflicts vo *Cyber-Terrorism and the information Sword, National University of Ireland, cork, August 1-5, 2006, str. 18*

[73] Закон за слободен пристап до јавни информации, Службен весник 13/06, достален на http://www.pravo.org.mk/documentDetail.php?id=448.

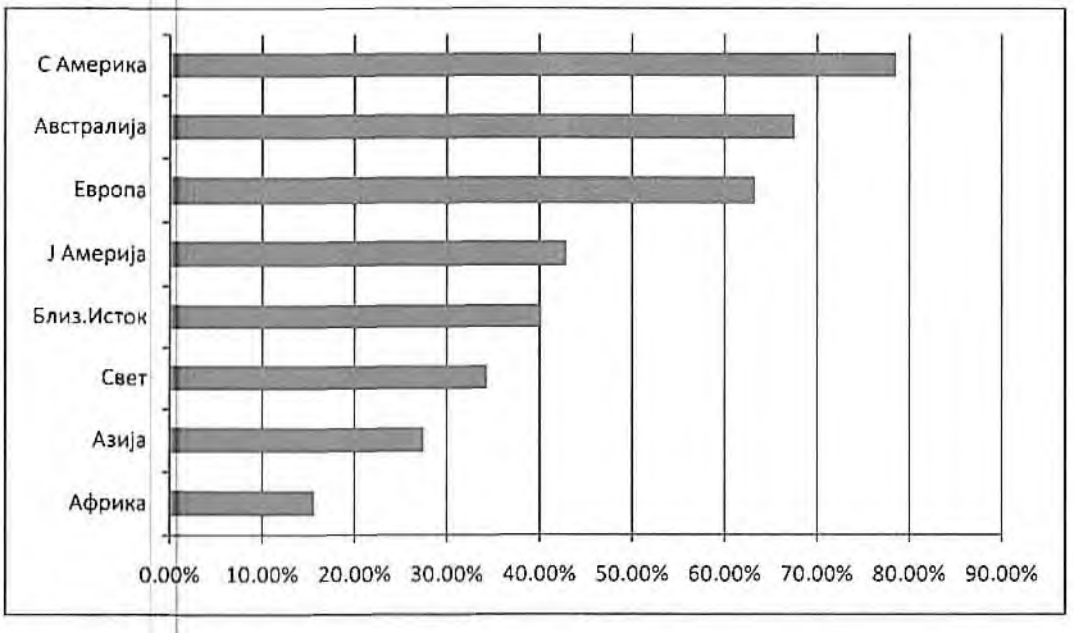

График 1. **Процентуална застапеност на корисници на интернет по региони во светот во 2012 година**

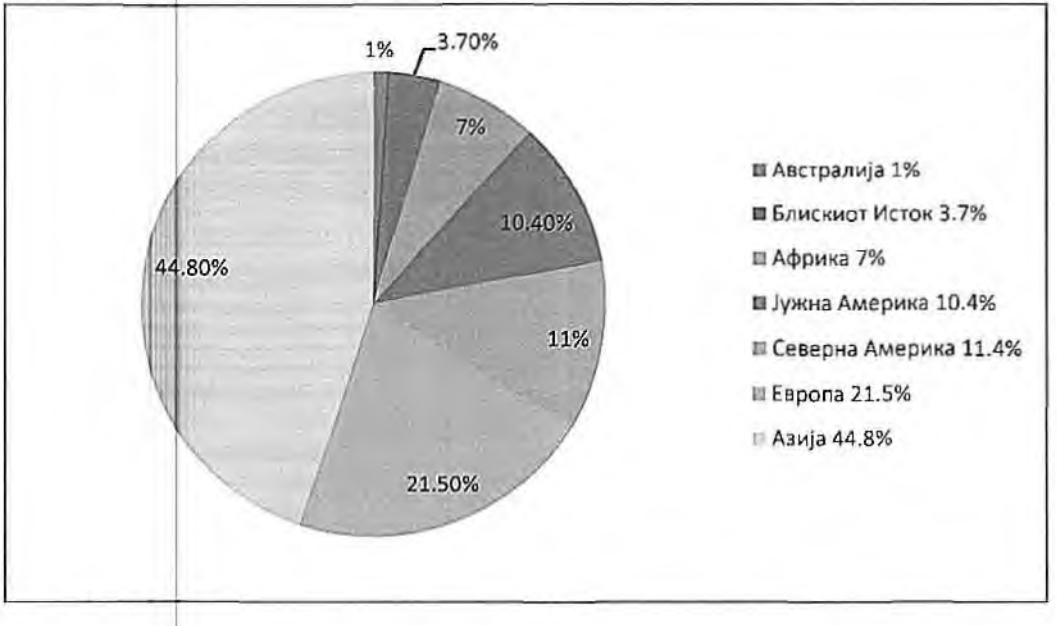

График 2. **Дистрибуција на интернет корисници корисници во светот по региони во 2012 година**

6.3. Закани од интернетот

Тоа што до сега е познато за потенцијалните закани и опасности, чии причинител е првенствено човекот е екстремно е вознемирувачки. Бројните и разновидните можности на напад во сајбер простор формираат широк спектар на закани–опасности, заради полесно и подобро согледување и разбирање на суштината, обемот и сложеноста можеме да ги класифицираме во четири категории:

- Компјутерски криминал;
- Сајбер тероризам;
- Разузнавачко делување;
- Информатичко војување.

Основен критериум за оваа класификација е мотивот за остварување на оваа цел.

Така да, накратко, компјутерскиот криминал како главен мотив за своето делување има материјална добивка.[74] Кај сајбер-тероризмот мотивот е најчесто тежнеење да се оствари некоја политичка цел.[75] Разузнавачкото делување како мотив има откривање на туѓи и чување на сопствени тајни.[76] И на крај, кај информатичката војна мотив е остварување на информатичка доминација над противникот.[77]

Од аспект на националните интереси категориите се рангирани во растечки редослед на значење, имајќи ги во вид степенот на општествени опасности кои се појавуваат. При тоа, мора да се знае дека секоја од овие категории претставува сложен поим, од аспект и начин на реализација, потекло (изворот), извршителите, мотивот, употребените ресурси и крајната цел.

Секако, се поставува и прашањето кои се потенцијалните извршители и од каде доаѓаат нападите. Дали е опасен напаѓач дванаесто годишен „ сајбер – шетач", кој на изглед, нема право ни на возачка дозвола, или е тоа добро платен припадник на странска разузнавачка служба, анархист или индустриски шпион? Дали заканата доаѓа од странски или домашни извори? За жал, тоа може да биде било кој или дури и мешавина од напред набројани, кои имаат пристап до интернетот, одредено техничко знаење и зланамера, независно од полот, боја на кожата, раса, образование, политички убедувања, староста и вероисповеста. Сите тие можат да нападнат и од надвор и од внатре, во секој момент, без оглед на одалеченоста, на годишното време, дали е ден или ноќ, временските прилики и неприлики.

---

[74]Petrovic. R. S.,Kompjuterski criminal, op.cit.

[75]Petrovic. R.S., Kiberterorizam, Vojno delo, god. LIII, br. 2/2001, str 100-122

[76]Petrovic R. S., *Neki aspekti nacionalne bezbednosti u informacionom dobu, Nauka, Tehnika, Bezbednost* (NTB), Rad po pozivu, UDC:681.324:65.012.8, Godina XI, broj 1, Septembar 2001, str. 7-27

[77]Petrovic R. S., Globalno informaciono ratovanje, Zbornik radova(CD-ROM), YU INFO 99, Kpaonik, 22-26 marta 1999, *Kiber proctor – peta dimenzija ratovanja, Vojni informatory, br.4,* jul-augusy 2001, str. 29-50

6. 4. Информациска безбедност

Со развојот на компјутерските комуникации и користењето на електронските и мобилните уреди се зголемува бројот на корисниците, а со тоа и трансферот на податоци. Низ мрежите и електронските уреди се пренесуваат многу чувствителни податоци: лични податоци, банкарски трансакции, договори меѓу фирми,податоци за национална безбедност итн.

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 систем, база на податоци и телекомуникациски мрежи кои го покриваат целиот национален сајбер простор и кој ги чини електронските податоци и сервиси да се широко расположиви и достапни до секого, што од друга страна значи и да се добро заштитени.

Развојот на информатичката технологија, пред сè на интернетот во голема мера ја олеснува комуникацијата меѓу корисниците и нуди многу поволности. Но сепак, недоволното искуство за користење на услугите, нивното погрешно користење или пак злоупотреба на некои ресурси , може да доведе до катастрофално последици.

При преносот на податоци не може да се гарантира дека тие нема да бидат пресретнати од друг корисник на мрежата, прочитани и злоупотребени.

Напаѓачот (компјутерски криминалец или сајбер терорист) може да ги уништи нашите податоци, да ги украде, да и предаде на конкурентите, да ги фалсификува или да ги измени податоците. Во зависност од природата на податоците кои се пресретнати, штетата може да биде огромна. Тоа доведува до потреба од заштита на податоците при нивниот трансфер.[78]

Начини на заштита на критериумите кои треба да бидат исполнети за статус на безбедна информација се :

- ✓ ***Доверливост (Confidentiality)***– информацијата треба да биде креирана и користена од субјекти кои имаат право на неа;
- ✓ ***Комплетност (Integrity)*** – информацијата треба да биде доставена во нејзината изворна форма (без неовластени промени), целосна и точна;
- ✓ ***Достапност (Accessibility)***– информацијата треба да биде достапна до сите кои се овластени;

Сведоци сме на секојдневни упади и злоупотреби на информациските податоци и упади и користење на конто на туѓи сметки со кои одредени групи на луѓе, па и цели организации се занимаваат со таа дејности кои за своја сметка и за сопствени потреби прибавуваат средства, односно само со добро поткова и баратање со интернет стануваат богати. Штетите од ваквите

[78] Димитрова, В., Ацковска, Н., Криптографски аспекти за безбедна комуникација, Институт за Информатика, Природно – математички Факултет, Скопје, стр.2-3

трансфери и не се толку критични бидејќи средствата кои се чуваат во банките се во најголем број осигурани, но терористичките организации вршат упади во строго доверливите податоци на државите чувани од разузнавачките и контраразузнавачките служби кои имаат за цел уривање на нивните влади, нарушување на националните безбедности на државите на кои нивната политика не им одговара, крадење на шифрите за нивните нуклеарни постројки и начинот за нивна изработка и др. не само терористичките организации туку и самите држави ја поткопуваат безбедноста на други држави кои не се пријателски настроени кон нив. Онаа што посебно ги храбри ваквите компјутерски па и сајбер напади е тоа што 90 % тие остануваат неоткриени и неможноста да им се суди и докаже делото туку се преземаат чекори за заштита на системите и оневозможување толку лесно па и воопшто да се дојде до таквите воени и цивилни (банкарски) досиеја.

Значи, информацискатa не-безбедност е присутна. Општествената и лична зависност од информациите и информатичко-комуникациски технологии (ИКТ) е неопходна. Општеството и секој поединец лично треба да се грижат за обезбедување на услови за безбедност на информациите и ИКТ со кои се служат.[79]

За заштита на електронски трансфер на податоци најчесто се користи шифрирање на податоците. Шифрирањето или (енкрипција)[80] најчесто се користат за заштита на електронските податоци и овозможува тајната комуникација да се остварува преку јавните средства за комуницирање. Предноста на шифрираниот текст е што тој нема потреба да се држи во тајност, може да биде испратен по електронски пат и само оној кому му е наменет ќе може да го прочита. Со тоа се обезбедува тајност и веродостојност на податоците.

Високо развиени држави кои во тајност држат многу документи за нуклеарни, хемиски и биолошки оружја, разни проекти и истражувања од програмата на НАСА, имаат формирано цели служби програми за заштита на податоци се со цел да ги зачуваат тие тајни програми, кои се на посебен удар и на мета на терористички организации и странски разузнавачки служби. Порано шифрирањето на податоци беше карактеристично само за владините служби, полицијата како и службите за национална безбедност, што не е пракса денес туку секоја институција може да врши шифрирање на подотаци и безбедна испорака до крајните корисници за кои се наменети информациите. Доколку тие не можат тоа сами да го направат работата им ја доверуваат на некоја од софтверските компании кои нон-стоп развиваат алатки за заштита и безбедност на информации и на целокупната електронска комуникација.

---

[79] Трајковски, Љ., Смерници за подготовкана Националната стратегија за Информациска безбедност на Република Македонија, Version 0.0, IT Association, MASIT, Macedonia, 31.01.2007, str.4

[80] Под енкрипција се подразбира конверзија на податоци од една форма во друга заштитена,шифрирана форма, Превземено од Поимник на Македонски зборови од областа на информатичка технологија, Министерство за Информатичко општество и администрација на Република Македонија, стр.20

6.4 .1.Криптографска заштита на податоците

Сите витални институции на државите користат разни заштити на своите информациони системи, како на пример: армијата, полицијата, банките, важни комуникациски објекти, јавен превоз, здравствени установи и др, за да не дојде до нивно пробивање т.е крадење на податоците и искористување за свои потреби. А потребите на терористите знаеме кои се, уништување и загрозување на безбедноста и животите на што поголем број на луѓе.

Затоа мора да се преземат сериозни мерки, заштитата на податоците од државен интерес да бидат на максимално ниво.

Дигиталните податоци се заштитуваат од: неовластен пристап, недозволено копирање и понатамошно дистрибуирање, како и докажување на автентичноста на податоците.

Не постои систем што може во целост да ги заштити системите од упад, крадење на податоци, или нивно менување, копирање или слично бидејќи се што е заштитено може и да се открие, а сопственикот сам одлучува за нивото за методот и нивото на заштита.

Еден од методите за заштита податоци е криптографија. Целта на криптографијата е заштита на дигитални податоци од неовластено користење, при што содржината на информациите се менува и станува нечитлива. На тој начин се врши нивно заштитување се додека не се изврши обратна операција, и не се добијат оргиналните податоци. Процесот на енкрипција за:

- Можност за утврдување на автентичноста на пораката или идентификација–утврдување на идентитетот на личноста, компјутерскиот терминал, кредитна картичка итн;
- Осигурување на интегритетот на податоците;
- Осигурување на приватноста и тајноста на податоците;
- Можност за идавање на дигитално уверение–потврда дека информацијата доаѓа од проверен извор;
- Можност за вградување на дигитален потпис во пораката;
- Можност за издавање на сметка–потврда за прием на информацијата;
- Осигурување на анонимноста;
- Осигурување на можноста за отповикување на авторизацијата и уверението.[81]

За да се изврши криптирање на податоците, потребно е тие да бидат во дигитализиран запис. За енкрипција на дигитализираниот запис се користи клуч за шифрирање, со кој се преобликува записот да не биде препознатлив, при што без познавање на клучот не може да се врати во својот изворен облик. Постојат два начини на шифрирање на дигиталните податоци: шифрирање со користење на симетричен клуч (*symmetric – key encryption)* и шифрирање со користење на јавен клуч (*public-key encryption).*

[81] Stancic, "Digitalizacija grage"

За заштита и пренос на своите податоци, институциите преземаат мерки за зголемување на информационата безбедност. Така, цели научно – истражувачки тимови, во светски рамаки работат на полето на криптологијата, односно шифрирање на податоци. Со криптологијата се врши шифрирање на податоци, значи така заштитени се пуштаат во мрежата, а други тимови по шемата за дешифрирање, што ја прават оние што шифрираат вршат дешифрирање.

Освен криптографијата како метод на прикривање и заштита на податоци, постојат и секојдневно се усовршуваат и други начини како на пример стенографија, [82]која во буквален превод значи 'прикриено пишување'. Сокривањето, односно прикривањето на тестуални пораки се врши во слики или аудио фајлови. [83]

И Република Македонија не заостанува на ова поле и развива свои тимови за криптозаштита, кои работат на Институтот за информатика на Природно–математичкиот факултет кој работи на развивање на алатки и алгоритми за криптирање[84] и декриптирање.[85] Нивните резултати се забележливи и доста успешно се покажаа на ова поле.

Со експанзијата на информатичката и мобилната технологија, како и на електронско банкарство и интернет трговија, безбедноста на податоците и комуникациите во целост ќе добива сè поголемо значење. Од сè поголем интерес стануваат и откритијата во областа на биоинформатиката, нанотехнологијата, вселенските истражувања, итн.[86] Криптографските техники се основа за изградба на информатичка безбедност. Криптолошката сигурност на криптографските техники со текот на времето се намалува поради постојаниот напредок на методите за компромитирање, што имплицира на неопходност од постојано усовршување и развој на нови криптографски техники.[87]

---

[82] Повеќе за компјутерска стенографија види во Sinkovski, S., kriptografske osnove informacione bezbednosti BISEC, 25 MAJ 2010 METROPOLITAN UNIVERZITET, Beograd, str.12-13

[83]Nagpal, R., CYBER TERRORISM IN THE CONTEXT OF GLOBALIZATION, PAPER PRESENTED AT: II WORLD Congres on Informatics and Law, Madrid, Spain September 2002, str. 10

[84] Под криптирање се подразбира операција со која се шифрираат податоците така што корисник кој не ја поседува потребната лозинка, не може да ги користи преземено од http://rechnik.on.net.mk/#/recnik/en-mk/encrypt",

[85] Под декриптирање се подразбира процес на конверзија на енкриптираните податоци назад во нивната првобитна форма, односно нивно дешифрирање. превземено од поимник на Македонски зборови од областа на информатичка технологија, Р.Македонија, стр.16

[86]Bozinovski, S., Jovancevski, G., Bozinovska, N., DNA as a real time, database operating system, SCI 2001 str65

[87]Mihaljevic, M., kriptologija-kriticno ishodiste za informacionu bezbednost, zbornik radova, druga konferencija o bezbednosti BISEC, 25 maj 2010, Metropolitan Univerzitet, Beograd, str.3-4

7. Сајбер – простор и видови на сајбер –компјутерски криминал

7.1.Поим за сајбер – простор

Во досегашното човеково постоење најзначаен домен како поле за егзистирање и дејствување беше копното, водата и воздушниот простор.

Во 1957 година, вселената е новиот и четврти домен на дејствување на човекот. Наскоро кон овие домени беше додаден и сајбер-просторот[88] Сајбер – просторот, како нешто ново и дотогаш непознато, започна да се истражува, но истовремено се прават обиди и да дефинирање на овој домен.

Преносот на информации се одвива во еден голем ново креиран виртуелен простор означен со префиксот *сајбер*, кој е преземен од од зборот *Cybernetics* (наука за управување) и кој треба да укаже на целата технолошка сложеност, зависност и проблематичност кои се присутни во тој нов, ама сè уште неуреден информатички амбиент, кој се разликува од обичниот и физичкиот свет на материјата и енергијата, во кој владеат знаењето, електронските и импулси на дигитални броеви.

Што е сајбер просторот? Прашањето не е лесно, ниту пак одговорот е еднозначен. Ако истот би се поставило на десетици познавачи на проблематиката, сигурно би се добиле исто толку различни одговори. Сајбер – просторот е термин кој прв го вовел Вилијам Гибсон (William Gibson) 1984 година во својата позната новела *Neuromancer*. Во оваа новела, Гибсон го опишува сајбер-просторот како акумулирана можност на светот на компјутерскиот систем. Сајбер–просторот е, теоретски простор во кој податоците можат да се складираат, пренесуваат и реконфигурираат[89].Постојан уште многу други, дефиниции и опис на овој термин. Авторот се определил за дефиниција која сајбер-просторот го толкува како виртуелен свет обележан со компјутери, компјутерски мрежи, информатички настани и информатичка содржина во дигитална форма.

7.2. Дефинирање на сајбер – просторот

Сајбер–просторот е сè почесто, ако не и најчесто употребуван збор во денешницата. Како светските сили се движат напред со својата визија така на нивниот пат се попречува сајбер- просторот е непознат простор односно место кое претставува предизвик. Во обидот да се дефинира, авторите до сега не успеале да изнајдат заеднички усогласена дефиниција.

Сајбер–просторот (cyberspace) всушност претставува најголемата компјутерска мрежа.[90]

Во однос на оваа област, се издвојуваат неколку дефиниции за сајбер – просторот кои се најцелосни:

- **Сајбер–просторот** претставува комбинација на виртуелните структури и физичките компоненти, како и информациите кои се

[88]Kuehl, D., From Cyberspace to Cyberpower: Defining the problem, Information Resources management College/National Defense University, str. 2

[89]Clarke, R., *Information Technology & Cyberspace:Their Impact on Rights and Liberties, mietta's, Melbourne, January 1996*, превземено од http://www.anu.edu.au/people/Roger. Clarke/II/index.html.

[90] Лазарова, М., **Слободата на изразувањето во сајбер просторот**, превземено од http://www.ii.edu.mk/.../слободата%20на%изразувањето%20во%20сајбер%20просторот.Pdf

во комбинација со истите, воедно и протокот на информации во рамките на тие структури.[91]

- **Сајбер–просторот** претставува меѓународна мрежа на поврзани компјутери која овозможува трансфер на информации од компјутерите на најразлични владини и невладини институции и лица со можност за нивна достапност преку модем.[92]

Врз основа на горенаведените дефиниции, можеме да заклучиме дека ***Сајбер просторот претставува систем кој со употребата на виртуелен и физички ентитет (електроника и електромагнетниот спектар) овозможува создавање, модифицирање, зачувување, споделување, и секако експлоатација на информациите од страна на меѓусебно поврзани информатички средства.***

Сајбер- простор е просторот односно средината во која со дигитализираните информации се комуницира преку компјутерските мрежи.[93]

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.[94]

Компјутерите и телекомуникациската технологија се важни компоненти на информациониот систем. Терминот информационен систем е информационатехнологија која се користи за извршување одредени организациски или индивидуални објекти.[95]

7.3. Природата на сајбер – просторот

Сајбер–просторот е поле со кое се врши пренос на информации во една друга димензија, невидлива средина, но уникатна по своите особини:

- Асиметрична и анонимна;
- Агеографска односно безгранична;
- Може да биде прикриена;
- Има виртуелно неограничен опсег и брзина;
- Брза е, едноставна и ефтина.[96]

Токму сајбер-просторот беше искористен за упростување на преносот на информации и упростување и олеснување на начинот на комуникација

---

[91]Fischer, A.,E Creating a National Framework for Cybersecurity:An Analysis of Issues and Options, CRS Report for Congress, RL32777, February 22, 205, str.5

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

[93]Joint publication 1-02, "DOD Dictionary of Military and Related Terms", April 2001 превземено од http://afgen.com.terrorism I.html

[94] Камбовски, В., Кривичен Законик, интегрален текст, Предговор, кратки објаснувања Регистар на поими, ЈП Службен весник на РМ, Скопје, 2009 стр. 126, Чл.122, став 26

[95] Превземено од http://e-biznisi.net/index.php?option=com_content&view=article&id=2009:-10-16-16-12-39&catid=73:2009-10-19-20-53-47&Itemid=98,

[96]Превземено од Anatomy of Cyberterrorism Is America Vulnarable?. www.au.af.mil./au/awc/awcgate/awc/ashley.pdf

бидејќи по својата природа овозможува лесен пристап до сечиј дом. Но, од друга страна и лесен за обработка и пристап до тие информации до терористите и терористичките организации особено поради:

- Општо народна прифатеност и лесен начин на користење;
- Лесниот пристап;
- Слабата (или отсуство на) законска регулација, цензура, и други форми на државна контрола;
- Потенцијално огромниот аудиториум, ширум светот;
- Анонимноста во комуникацијата – интернетот дава можност за анонимно користење;
- Ефтиниот развој (креирање и одржување) на веб-страниците;
- Мултимедијалната средина (можност за комбинирање на текст, графика, аудио и видео, како и можноста корисниците да симнуваат и превземаат филмови, слики, книги, постери и песни;
- Брзиот проток на информации;
- Способноста да го обликуваат медиумското покривање на настаните во традиционалните мас – медиуми, кои се почесто го користат токму интернетот како извор за нивните приказни.

Дел од пропустите и инцидентите направени во компјутерско-информатичките системи не можеме веднаш да ги поврземе како атак врз компјутерските системи или доколку не можеме да се логираме или шифрата на сметката во банката не ни се прифаќа дека тоа е дело на на некој криминалец или сајбер-терорист. Тука можат да настанат пропусти ненамерно предизвикани во грешка во системот, софтверски пропусти или маани, недоволно обучен персонал,човечка грешка како фактор[97] или слаба техничка или административна имплементација на безбедносните процедури.

7.4. Поим за сајбер – напад и негови потенцијални извори

Сајбер или компјутерски напад – претставуваат дејствијата кои имаат за крајна цел уништување, нарушување, деградирање, блокирање или друг начин на оштетување на информациите складирани во компјутерите и компјутерските мрежи.[98]

За да означиме или пак да одбележиме сајбер – напад како сајбер – криминал, всушност претставува екстремно тешко, поради постоечката неможност да точно се одредат следните нешта: **мотивот, целта или намерата.**

Потенцијални сајбер – напаѓачи, би можеле да ги сврстиме во 4 категории:

1) Терористички групи

---

[97] *Bosch, O.*, defending against cyber terrorism:preserving the legitimate economy, BUSINESS AND SECURITY, SIPRI, 2004, стр. 189, превземено од http://www.sipri.org/.

[98] Податоци превземени од http://dictionary.reference. Com/browse/cyberattack

Терористите водени од своите побуди, постојано вршат напади и се на еден начин во војна во виртуелниот свет.[99] Познато е дека терористите ја користат компјутерската технологија и интернетот да остваруваат закани, напади, комуникација, да формулираат планови, да ја шират својата пропаганда и идеологија, регрутација но и да прибираат средства и финансии.

2) Таргетирани држави

Многу држави во светот ја сфатија корисноста на интернртот и можностите што ги нуди, како и можностите и начините за развивање на техника за спроведување на сајбер – напади, со цел вршење на разузнавачки како и шпиунски активности кон други држави или корпорации, или за водење на информациска војна. Како такви се вбројуваат: Ирак, Либија, Северна Кореја, Куба и Русија за кои се верува дека развиваат можности за сајбер – војување.[100]

3) Антикапиталистички движења

Анти – капиталистичките движења ширум светот, своето незадоволство против западните земји како плодна почна за прибирање и организирање на своите истомисленици го најдоа интернетот и социјалните мрежи.

Тука не заостануваат ниту терористичките симпатизери која својата подршка ја искажуваат на нивните сајтови, а тоа го искористуваат терористичките водачи за нивна мобилизација ширум светот и насочување кон прифатните центри па дури и во војни.

4) Други сајбер-напаѓачи

Во оваа категорија спаѓаат лицата кои работат на своја рака и за своја сметка кои и не мора да имаат политички или идеолошки причини како своја мотивација, туку едноставносе водени од желбата да се фалат за своите подвизи,[101] или дел од престапите и криминалот што го прават е поради забава, или не знаење дека со своите дела некому штетат.

Безбедносните служби на САД задолжени за информатичка безбедност, даваат преглед на изворите на закано по информатичка безбедност, како и детален опис на таквите закани на следниов начин:[102]

---

[99]Arquilla, J., Ronfeldt, D., networks and Netwars:The future of terror, crime and military Rand, 2001, str.117

[100]Hildreth, A.,S., Cyberwarfare, CRS Report for Congress, June, 2001, стр.2, превземено од www.fas.org/irp/crs/RL30735.pdf ,

[101]Cyber Attacks During the War on Terrirism: A Predictive Analysis, Institute for Security technology Studies at Dartmouth College, September, 2001, стр14, превземено од http://www.ists.darmouth.edu/projekts/archives/syber attacks.html

[102] Адаптирано според Unitet State Government Accountability Office, Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk превземено од Buckland, S.,B.,Schreier, F., Winkler, H.,T., Demokratsko upravljanje izazova sajber bezbednosti, Forum za bezbednost I demokratiju, Beograd, 2010. str 14

***Табела 1.* Извори и опис на заканите**

Извори на заканите	Опис на заканите
Држави	Странски разузнавачки служби ги користат информатичките средства за прибирање на информации и шпионажа[103].
Хакери[104]	Лицата и средства за напад се пософистицирани, лесно достапни и едноставни за примена.
Корпорации	Фирмите и корпорациите (понекогаш во соработка со организирани криминални групи) спроведуваат индустриска шпионажа[105] или саботажа[106].
Хактивисти	Хактивизмот претставува политички мотивиран хакерски напад на интернет.
Инсајдери или внатрешни лица	Инсајдери или лица од внатре претставуваат огромна опасност, ако го имаме во предвид нивното детално познавање на системот на жртвата, кое и овозможува непречен пристап. Мотови кај инсајдерите најчесто се предизвикување штета на системот или кражба на осетливи податоци.
Фишери[107]	За остварување најчесто на финансиски добивки, овие лица користат т.н спам или шпиунски/малициозни софтвери.
Спамери[108]	Преку дистрибуирање на несакана пошта вршат фишинг измами, или растураат зло намерен софтвер.
Автори на шпионски софтвер	Поединци или организации кои со зла намера спроведуваат напади врз корисниците користејќи и растурајќи шпионски и малициозен софтвер.
Терористи	Терористите сакаат да ја уништат, онеспособат или искористат клучната инфраструктура, да ја загрозат националната безбедност, да предизвикаат масовни жртви, да ја ослабнат економијата и да ги нарушат јавниот морал и довербата. Иако можеби повеќето терористички организации моментално немаат капацитети за спроведување на сајбер напади, тоа не значи дека и во иднина нема да ги имаат.
Педофили[109]	Педофилите се почесто го користат интернетот за размена на детска порнографија како и за изнаоѓање на жртви (најчесто користејќи ги социјалните мрежи[110] и форумите).

---

[103] Поимот компјутерска шпионажа се дефинара како најмодерен облик на разузнавање

[104] Терминот **хакер** се однесува на луѓе кои користат различни техники и програми за да пронајдат начин за нарушување на сигурноста без знаење 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 ранливоста на компјутерите во мрежа, откривање на лозинки (преку таканаречените снифер програми), добивање лозинки од некого и др. Превземено од http://www.ucenje.org.mk/eLearning ,

[105] Под поимот компјутерска шпионажа може да се дефинира еден од најмодерните облици на разузнавање, а индустриската шпионажа е компјутерска шпиунажа само од комерцијална природа.

[106] Компјутерска саботажа имаме во случај кога некој ќе уништи, избрише, промени, прекрие или на друг начин ќе онеспособи податок, програма или ќе го оштети компјутерот кој е од значење за државен орган, институција, јавна служба.

[107] Поединци или мали групи кои по пат на измама вршат кражби на идентитет со цел остварување на финансиски добивки.

[108] Спамери се поединци или организации кои дистрибуираат небарана пошта (често со прекриени или лажни информации) со цел да продадат одреден производ, да извршат фишинг измама или да растурат шпионски/злонамерен софрвер.

[109]**Сексуалната злоупотреба (педофилија)** се дифинира како било каков вид на сексуален контакт (директен или индирејтен) помеѓу лице (кое е постаро 5 или повеќе години од детето жртва) и дете. Сексуалната злоупотреба се случува кога лицето (возрасен или тинејџер) го користи детето за задоволување на своите сексуални потреби, при што го: наведува-подведува му се заканува, го насочува и присилува на сексуален контакт и притоа не се гружи за психичките, емоционалните и секаков вид трауми и последици што му ги нанесува. Превземено од http://www.stop-pedofilija.org.mk/stopepedofilija.html.

[110] Двете најпознати социјални мрежи facebook-http://www.facebook.comи twitter-http://www.twitter.com .

7. 5.Мети на сајбер – напади

Националната инфраструктура е можна и посакувана мета за сајбер – напади поради нејзиното влијание врз зачувувањето на трајните витални и важни национални интереси исто како и поради сервисите и добрата што таа ги нуди на граѓаните.

Дел од нив всушност се од витално значење за зачувување на националната безбедност, економската состојба, виталност на општеството и општественото уредување па поради тоа и се нарекува критична инфраструктура.

Во САД критична инфраструктура се дефинира како : „Критична инфраструктура претставуваат физички и сајбер базирани системи, кои се од суштинско значење за остварување на минималните операции на економијата и владата".[111]

За значењето и импактот кој еден од овие напади ќе го претрпи општеството, со што ќе се оневозможи фукционирање на основните државни системи (како системите за вода, системите за електрична енергија, телекомуникациите, системите за итни случаи, системите за транспорт, банкарските и финансиските системи)[112] е тема на која САД и НАТО се фокусирани.

Според гледиштето на професорот Jeffrey Addicott (2011), постојат 5 основни типови на критична инфраструктура:[113]

1) Производни индустрии: (енергија, хемиски индустрии, производство на оружје и муниција и сл)
2) Услужни индустрии: (банкарство и финансии, транспортот, ПТТ услугите и сл
3) Опстанокот и здравјето:(земјоделство, храна, вода, јавно здравје)
4) Федерални и државни: (Владата, итните служби)
5) Информатичка технологија: (интернетот и телекомуникациите).

Секоја од овие категории на критична инфраструктура претставува засебна цел на сајбер – нападите. Успешноста на сајбер-нападите ќе зависи од тоа колку нивната инфраструктура и податоците им се заштитени, со тоа и последиците ќе им бидат поблаги. Но доколку сајбер-нападот биде успешен тогаш ќе се наруши целосниот систем на функционирање, а не е исклучена и можноста за ослабнување на самата држава и општеството во целост.

---

[111]John Moteff and Paul Parfomak, Critical Infrastrukture and Key Assets:Definition and identification, October 1 , 2004 del 4

[112]Ibid 30 del 3

[113]Jeffrey, F., Addicott .,Terrorism Law: Materials, Cases, Comments, 6th edition(2011), Center for Terorism Law Issues for Discussion- Cyber Security, 11 March 2011 CLE.

Најчести и најомилени сајбер дестинации се следните:

- Владини инфраструктурни објекти и служби;
- Банките и финансиските институции се доста ранливи и најчесто напаѓани;
- Воени бази и нуклеарните централи;
- Комуникациските системи, се исто така ранливи на сајбер – нападите особено одвнатре, од страна на лица на кои им се познати техничките детали за системите;
- Електрична инфраструктура – електричните централи и мрежата за напојување;
- Водените ресурси и водоводната инсталација;
- Здравствените установи, болниците, центрите за производство и развој на лекови;
- Инфраструктурите за нафта и гас, кои во голема мера се потпираат на Supervisory Control And Data Asquisition (SCADA).

Дел од објектите т.е институциите што се можни цели на сајбер-напади доколку успешно се изведат како што кажав би имале голреми и катастрофални последици и би предизвикале огромни штети, но други пак би значеле и загуба на човечки животи како на пример предизвикување на хаварија во нуклеарна централа кој аи после сто години ќе стојат трагите од таквиот немил настан. По 11 септември 2001 година и таквите напади се неостварливи бидејќи терористите се повеќе се жедни за крв и не бираат средства и начин за остварување на своите мрачни цели и задоволување на болните умови.

7.5.1. SCADA-управувачки системи

Систем за супервизорно управување и аквизација[114] на податоците (употреба на на компјутеризиран систем за да се автоматизира задачата)- ***SCADA*** *(Supervisory Control And Data Acquisitio)*во минатот подразбирал систем кој собира и испраќа информации на далечински локации. Вообичаено има само надзорничка улога бидејќи нее потполно одговорен за примарната управувачка функција. Во најголем број на случаи некој друг систем (како што е PCL-то[115]) е одговорен за примарно управување, а SCADA системот едноставно ги надгледува и пријавува активностите. Во денешно време SCADA системите имаат проширена управувачка функција и овозможуваат моментална пресметка и менување на дефиниранитеточки и вредности при нивната комуникација со примарните управувачки системи.

Во најголем број на случаи сите дигитални системи за управување можеме да ги распределиме во три категории:

1. Програмабилни логички контролери – Programmable Logic Controller (PLC),

2.Распределени управувачки системи– Distributed Control System (DCS) и

3.Систем за супервизорно управување и аквизација на податоци – Supervisory Control And Data Acquisition System (SCADA)

SCADA претставува систем наменет истовремено мерење и управување. Системот има функција да собира информации, ги пренесува до централата, ги спроведува потребните анализи и управувања за да на крај ги прикажа на неколку операторски екрани.

Овие системи се компјутери преку кои се мониторираат и оперираат операциите на мноштво критични инфраструктури.[116] Ваквите SCADA компјутери, многу од експертите веруваат дека се атрактивни таргет- цели за терористите.[117]

Примарна одлика на SCADA системите, која значајно ги одделува од останатите системи за дигитално управување, е нивната можост за комуникација користејќи многуразлични методи. Ова ги прави многу корисни за собирање и испраќање на информации и управување до и од различни други дигитални системи. Со помош на различни протоколи, SCADA системите се способни за комуникација преку телефон, UHF/VHF радиа, етернет, микробранови системи, сателитски системи и фиберoптички кабли. Типичен SCADA систем се состои од мастер единици – MTU (Master Terminal Unit) и една или повеќе далечински единици – RTU (Remote terminal Unit).

Зошто SCADA системите се толку значајни и корисни за општеството, а од друга страна и најпримамливи и опасна цел доколку дојдат во рацете на

---

[114] Лат(acquisition) 1.придобивка, стекнато добро, заработка, 2. Набавување, стекнување

[115] Програмабилен логички контролер – PLC (Programmable Logic Controller) претставува комбинација на хардвер и софтвер кој извршува две функции- управување и аквизација на податоци. Типична PLC архитектура се состои од процесор и влезно/излезен подсистем.

[116]Wilson, C., Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, April, 2005, стр. 10

[117]Nagre, D., Warade, P., CYBER TERRORISM, Vulnerabilities and policy issues "Facts Behind the Myth", стр. 23, превземено од: http://www.andrew.cmu.edu/user/dnagre/,

терористите?

Причината е затоа што SCADA системите се инсталираат на критичните инфраструктурни објекти со многубројни операции, а токму SCADA системите ги контролираат, управуваат, мониторираат таквите објекти како браните, електричните постројки и мрежи, хидро и термо централи, и другите инфраструктурни објекти. Со нападот и влезот во SCADA системот, потполната контрола веќе е во рацете на терористите и можат слободно да вршат управување на системот, кој ќе изврши било каква зададена задача од страна на терористите, без разлика дали се работи за хаварија, експлозија, прекин на енергија, преголема енергија и сл. Доволно е само да го пореметат системот за работа на овој електронски уред и резултатите би биле катастрофални.

Еден пример за пробивање на SCADA системите во Австралија, укажува на можните последици од ваков напад. Имено, по 44 неуспешни, но и недетектирани обиди да се пробие системот, еден незадоволен поранешен консултант, отпуштен од работа, во својот 45-ти обид успеал да га пробие SCADA системот и да испушти 1 милион литри отпадни води во потокот од кој се користела вода за пиење. Водниот свет изумрел, водата од потокот станала црна, а смрдеата била неподнослива за жителите од околните места.[118]

7.6. Видови на сајбер-компјутерски криминал

7.6.1 Поим за сајбер (компјутерски) – криминал

Глобалните компјутерски мрежи овозможуваат создавање на нов облик на криминал. Се појавува посебен, софистициран, продорен технички едуциран, бескрупулозен, опседнат понекогаш одмазнички настроен поединец со кого справувањето е многу тешко. Тој често не сака да биде сам, при што му е потребно друштво, а исто така и публика. Тој криминал е наречен **сајбер – криминал** кој е многу често и широко толкуван во поново време кој е овозможен или насочен против компјутери. Сајбер–криминалот може да опфати кражба на интелектуална сопственост, злоупотреба на патент, трговска тајна, банкарска малверзација и др, но исто така вклучува и напади против компјутери со цел намерно нарушување на нивното функционирање, или недозволено копирање на класифицирани информации складирани во компјутерските системи.[119]

Поголем временски период бил потребен за дефинирање на компјутерскиот криминал и за вметнување на компјутерскиот криминал во законските нормативи како казниво дело.

Во обидите за разјаснување на начините и намерите , и размерите до кои може да достигне компјутерскиот криминал и опасноста од него е прецизирано во документот „Криминал во спрега со компјутерските мрежи" (*Crime related to computer networks)* од десетиот конгрес на Обединетите Нации посветен на превенцијата од криминал и третирањето на овој вид на

---

[118]Lemos, R., What are the real risks of cyber terrorism? Превземено од http://www.zdnet.com/news/what-are-the-real-risks-of-cyberterrorism/124765,

[119]Wilson, C., Botnets, Cybercrime and Cyberterrorism: Vulnerabilities and Policy issues for Congress, January, 2008, стр. 7

криминал. Експертската работна група под овој криминал подразбира „криминал кој се однесува на било кој облик на криминал кој може да се извршува со компјутерски системи и мрежи, во компјутерски системи и мрежи или против компјутерски системи и мрежи." Тоа е криминал кој во суштина се одвива во електронска околина. Ако под компјутерски систем се подразбира „секој уред или група меѓусебно поврзани уреди со кои се врши автоматска обработка на податоци (или било која друга функција)", како што е дефинирано во Конвенцијата за сајбер-криминал, тогаш е јасно дека без електронска околина нема да постои ваков вид на криминал.

Компјутерот најчесто се јавува и како субјект и како објект на напад, бидејќи многу компјутерски криминални дела се реализираат на тој начин што се користи еден компјутер за напад на друг.

Сајбер – криминалот може да се дефинира како извршување на кривични дела кои како свој субјект или објект го имаат интернетот како глобална компјутерска мрежа, и кои се вршат од страна на информатички обучени лица, со цел предизвикување на штети или придобивање на противправна имотна корист.[120]

Сајбер – криминалот, како и останатите облици на криминал, има свој сопствен modus operandi, кој од страна на сторителите е постојано усовршуван и надополнуван со нови елементи, кои се поврзани со примената на компјутерската техника и користењето на криминалистичка информатика.[121]

Се поставува прашањето зошто обичните криминалци и терористите толку добро го прифатија компјутерскиот теторизам и сјбер-тероризмот како нивна алатка за извршување на своите (зло)дела. Бидејќи се што им е потребно е компјутер и вештина и без никакво ограничување можат да делуваат и да оперираат во своите области. Користејќи ги сеуште слабо обучените безбедносни служби за успешно справување со овој вид на криминал и слаба соработка на меѓународно ниво, тие се без малку недопрени и многу малку од нив се изведени пред лицето на правдата да одговараат за своите постапки.

Многу автори дебатираат околу тоа дали постои разлика помеѓу сабер-тероризмот и сајбер-криминалот или овие два поими се синоними.

Така да има размислувања дека сајбер тероризмот е политички мотивирано, и примарна цел на сајбер-тероризмот е да се инфилтрира во системот на одредена институцијакаде што има за цел да предизвика штета (финансиска загуба, жртви, хаварија и сл) со што ќе се предизвика дестабилизација на безбедноста на самата држава.[122] Додека пак сајбер-криминалците обично хакерите кои се добро потковани со информатичката технологија тоа го прават за сопствени потреби, за свој личен интерес и корист.

---

[120]Stamenkovic, B., kriminalu IT oblasti u Srbiji danas: od otkrivawa do presude, centar za razvoj internet- seminar o informacionom drustvu za novinare-27-29. Februar 2004, стр. 47

[121] Банович, Б., Обезбеџење доказа у криминалистичкој обради кривичних дела привредног криминала, стр. 136

[122] Надица Мирчевска, научен труд сајбер тероризам – современ облик на тероризам, колку Република Македонија е ранлива од сајбер-тероризам.

Заедничко нешто за овие два термини (сајбер криминал и сајбер тероризам) е тоа што се користи компјутерот како заедничко оружје за вршење на кривичното дело.

Софистицирани алатки за сајбер – напади, можат без проблем да се најдат, купат или изнајмат преку интернет, на посебни веб – страници,а се бараат и регрутираат новиталентирани студенти, од областа на програмирање и мрежната администрација.

Мое размислување е дека исто така треба да им се посвети внимание на сајбер-криминалците бидејќи тие веќе запливале во водите компјутерскиот криминал и многу лесно може да се охрабат и да продолжат понатаму со своите потфати, па дури и да постанат сајбер-терористи доколку ги намамат терористите во своите редови и ги ангажираат за поголем зафат и, а можеби и самите нема да знаат дека извршуваат задачи за сајбер терористичка организација.

Постојат четити основни начини за користење на компјутерот за вршење на криминални активности, и тогаш компјутерот се јавува како:

1. Средство за измама;
2. Објект на напад;
3. Средство за извршување;
4. Средство за планирање, прикривање и раководење на криминалот;

Многу почести се случаите кога компјутерот се јавува како субјект на напад, односно средство за извршување. Компјутерските процеси се користат за да се овозможи, олесни или забрза реализација на одредени криминални активности.[123]

7.6.2 Начини на извршување на кривични дела од областа на компјутерскиот криминал

Компјутерскиот криминал претставува облик на криминално однесување, каде компјутерската технологија и информационите системи се искористуваат за извршување на кривични дела, или компјутерот се употребува како средство или представува цел, каде се создава последица во кривично – правна смисла. Самиот криминал кој се реализира со помош на компјутер може да има облик како било кој од традиционалните видови на криминалитет, како што се кражби, затајување, проневери, додека податоците кои неовластено се собираат со злоупотреба на информационите системи, може на разни начини да се користат за стекнување на противправна корист.

Ќе набројам дел од појавните облици на компјутерски криминал:

- Нелегални навлегувања во поголеми мрежи на видни компании;
- Противправно користење на услуги и неовластено собирање на информации;
- Компјутерски кражби;
- Компјутерски измами;

[123]Тањевич, Н., Компјутерски криминал-правна заштита на националном нивоу, Безбедност, Теоријско стручни часопис Министарства унутрашњих послова Републике Србије, Београд, 1-2 2009, стр.155

- Компјутерска саботажа и компјутерски тероризам;
- Криминал поврзан за компјутерските мрежи;
- Загрозување на интегритетот на компјутерските мрежи;
- Загрозување на приватноста;
- Пиратски компјутерски софтвер, и било какво криминално дејствие каде компјутерот е главен фактор за криминален престап.[124]

Врз основа на тоа, во најчести случаи појавни облици на кривични дела од областа на сајбер-криминалот влегуваат:[125]

1) ***Изработка и употреба на компјутерски вируси и црви*** *Компјутерските вируси* се многу мали програми, од неколку килобајти, кои имаат исклучиво за цел да направат штета на заразен компјутер. Се размножуваат воглавно на начини што се „вгнездуваат" кај други фајлови, а штета предизвикуваат така што ги бришат или менуваат фајловите на дискот. Во случај доколку се работи за информациони системи, вирусот од заразениот компјутер може да зарази друг компјутер во компјутерска мрежа, со цел да измени или оштети фајлови од оперативниот систем на компјутерот. Нивни основни одлики се:
   - ✓ Не се забележливи, односно најчесто се невидливи за корисникот на компјутерот, посебно ако на компјутерот не е инсталиран специјализиран софтвер за нивна детекција.
   - ✓ Се копираат (реплицираат) самите себеси на секој компјутер со кој ќе дојдат во контакт.
   - ✓ Автоматски извршуваат одредени команди како бришење на кориснички податоци на компјутерот на жртвата, или пак ги испраќаат податоците на одредена друга локација на мрежата без знаење на сопственикот на компјутерот.[126]

Многу се опасни, се шират многу брзо, а дури и најмалку штетниот вирус би можел да биде фатален. На пример компјутерски вирус со кој би се запрела работата на апаратите за вештачко дишење во болниците. Како најпознати вируси во литературата се споменуваат: Mellisa, Cascade, ExploreZip, Chernobyl, I Love You, Pakistani Brain и Michelangelo.[127]

---

[124] Преземено од http://www.fbi.gov/about-us/itb

[125] Интервју со Марјан Ристески, Инспектор за компјутерски криминал, Македонско сонце, 06.02.2004, стр. 32

[126] Интервју со Марјан Ристески, Инспектор за компјутерски криминал, Македонско сонце, 06.02.2004, стр. 34. Преземено од http://www.makedonskosonce.com/broevis/2004/sonce501.pdf/32_36_cekmedje.pdf

[127] Nagpal, R., CYBER TERRORISM IN THE CONTEXT OF GLOBALIZATION, Paper presented at: II World Congress on informatics and Law, Madrid, Spain September 2002, стр. 6

„Црв" (worm) е дел од софтвер кој „гризе" низ само еден компјутерски систем или низ мрежа на компјутерски системи, манипулирајќи, менувајќи или уништувајќи податоци или програмски кодови на местата до каде има пристап. Црв не се реплицира, туку се движи наоколу и остава штета на својот пат. Доколку биде откриено неговото присуство, може да го „одбегне" неговото „фаќање". Многу вируси имаат вградено „црви".

Најчести начини на кои компјутерите можат да се заразат со вируси и црви се:

- ✓ Преку разни медиуми кои се носачи на информации кои се заразени од вирус, црв или тројанец;
- ✓ Преку фајлови односно датотеки применети по електронска пошта или програм за комуникација од видот на ICQ, Skype ;
- ✓ Преку уредите за пренос на податоци (USB, Надворешен хард диск-External HD, CD и сл.);
- ✓ Преку фајлови симнати од разни веб-страни на интернет кои воглавно се поставени на бесплатни сервери и содржат скрипта која во компјутерот ќе уфрли вирус или црв.

За борба против вирусите се користат **Антивирусни – програми** кои спречуваат компјутерот да се инфицира и кои ги уништуваат вирусите, доколку дојде до „инфекција" на компјутерот.

Антивирусните програми спречуваат „зараза"така што ги скенираат фајловите кои се употребуваат во барање на кодот (со програма внатре во програмата) и доколку најдат код кој дава присуство на вирус, тие го спречуваат стартувањето на програмата.

Во Кривичниот Законик на Р.Македонија, овој облик е инкриминиран во членот 251 – а, како кривично дело ***Правење и внесување на компјутерски вируси*** и е казниво со закон согласно кривичниот закон на Р.Македонија.

2) Компјутерска измама

Компјутерските измами се извршуваат со намера за стекнување за себе или за друг со противправна материјална корист, со тоа што кај нив во заблуда не се доведува или одржува некое лице, како што се случаите со обичните измами, како материјалните кривични дела со кои се предизвикува штета, туку заблудата се однесува на компјутер во кој се внесуваат неточни податоци, или се пропушта внесувањето на точни податоци, или на било кој друг начин, компјутерот се користи за остварување на измами во кривично – правна смисла. Компјутерските измами претставуваат најраширен облик на компјутерски криминал.

Компјутерските измами се карактеризираат со многу големо продирање, заради големината на интернетот како пазар, бидејќи брзо се шират со интернетот како медуим со кој се се случува многу брзо, а исто така и заради ниските трошоци за извршување на ваквиот вид на измами.

Аукциските он-лајн (on-line) измами преку интернет, кои вклучуваат

неиспорачување или лажно претставување на стоките од 'црниот пазар' се едни од најчестите компјутерски измами.[128]

Компјутерската измама како кривично дело е инкриминирано во членот 251-б од ЗКП на Р.Македонија.

Казниви дејствија се невнесување на вистинити податоци во компјутерски систем, фалсификување на електронски потпис, или на друг начин предизвикување невистинит резултат при електронска обработка и преносот на податоци, заради прибавување противправна имотна корист за себе или за друг. Казниво е и неовластено изработување, набавување, продавање, држење или правење достапни на друг посебни направи, средства, компјутерски програми или компјутерски податоци наменети за извршување на делото.[129]

3) Финансиски кражби злоупотреби на кредитни картички

Финансиските кражби и злоупотреби со помош на компјутер се едни од најчестите компјутерски криминални дела и се однесуваат на **злоупотреба на кредитни (платежни) картички**[130] кои пак се едни од најмодерните платежни средства, и на разни навлегувања во заштитени сиситеми и правење на недозволени финансиски трансакции.

Изработка и употреба на лажна платежна картичка претставува кривично дело по член 274-б од ЗКП на РМ.

Злоупотребата на кредитни картици т.е правење на лажни кредитни картици со која можат да се подигаат пари на сите банкомати и платежни станици како и купување на разна роба се едни од најчестите кривични дела кои со кои се соочува домашното законодавство. Прибавувањето лажна картичка со таква намера, или давањето на друг на употреба, употребата на лажна картичка како вистинска, како и прибавување на банкарски податоци од вистински платежни картички и податоци за носителите на тие платежни картички, со намера искористување на истите за изработка и употреба на лажна платежна картичка или доставување на така прибавените податоци на друг со таква намера се казниви со закон.

4) Фалсификување на податоци и документи

Компјутерско фалсификување на податоци и документи имаме во случај кога неавторизирано се менуваат податоци во компјутерска форма. Во овој како и во претходните примери, компјутерските системи се мети на криминална активност. Компјутерите можат да бидат употребени за изведување на фалсификат. Особено се зголемија фалсификатите со појавата на компјутеризираните колор ласер печати. Овие печати имаат можност за печатење со висока резолуција, модификација на документи, дури и креирање на лажни документи, пари, договори, а нивниот квалитет не се разликува од

---

[128] Петрович, Р., С., Полицијска информатика, Криминалистичко-полицијска академија, Београд, 2007, стр. 100

[129] Камбовски, В., Кривичен Законик, Интегрален текст, Предговор, кратки објаснувања и Регистар на поими, ЈП Службен весник на РМ, Скопје, 2009 стр.210-211, Чл.251-б, став 1-9

[130] Под платежни картички се подразбира секаков вид средства за плаќање издадени од банкарски или други финансиски институции, кои содржат податоци за лица и електронски генерирани броеви со кои се овозможува вршење на каков билвид финансиски трансакции(Член.122,ст.15, КЗ на РМ)

автетичните.
Најчести фалсификувани податоци и документи:

- Фалсификување на пари
- Фалсификување на хартии од вредност (акции, обврзници)
- Фалсификување на документи (исправи, дипломи, уверенија, потврди и сл.)
- Фалсификување на знаци од вредност (таксени, поштенски марки и други знаци од вредност)
- Фалсификување на знаци за обележување на стоки, мери и тегови (печати, штембили, жигови).

Како и финансиските кражби така и фалсификувањето на податоци и документи стана едно од најчестите кривични дела со кои се среќава домашното правосудство. Нивните фалсификати благодарение на појавата на скенерите и ласерските печатачи во боја, како и софтверските пакети за графичка обработка, може да циркулираат на пазарот и по неколку години, некои се откриваат при користење во други држави, каде има пософистицирана опрема за таков вид на криминал, а некои и воопшто не се откриваат поради автентичноста со оригиналите.

5) Компјутерски кражби

Компјутерските кражби заземаат високо место во областа на компјутерскиот криминал, а во однос на наведената проблематика од посебно значење претставува кражбата на идентититет. Овој вид на кражба има особено значење во општетството бидејќи покрај се останато, ја намалува довербата во интегритетот на комерцијалните трансакции и ја загрозува индивидуалната приватност. Проценките на експертите се дека компјутерските кражби ќе се зголемуваат со елекпронско тргување. Снагдени со индивидуални персонални информации, криминалците со украден идентитет може да прават банкарски трансакции, да купуваат, продаваат, можат да добијат документи за раѓање, пасош и сл, а се тоа во име и од сметка на личноста за чии податоци се работи.Со лажен идентитет криминалците може да добијат кредити од банки, да купат автомобил, стан и др, при што на тој начин да предизвикаат финансиско оштетување на жртвата, а во некои случаи и да и се направи кривично досие. Оштетената странка всушност и не знае дека нејзиниот идентиттет се користиза туѓо име од своја сметка се додека не стигнат сметките за наплата.[131]

6) Компјутерска саботажа и шпионажа

Како дел од сајбер–нападите кои се поврзани со разузнавањето, контраразузнавањето и безбедноста од воен аспект се саботажите и шпиунажата кои се јавуваат во две типични форми и тоа:

---

[131] Југослав Ачковски, Методија Дојчиновски скрипта – Сигурност на компјутерски системи, компјутерски криминал и компјутерски тероризам.

- **Физичка саботажа** – подразбира физичко оштетување на опремата (истурање на течност врз електронските елементи, предизвикување на кратки споеви, предизвикување на прегревање по пат на саботажа на уредите за разладување на системите, донесување на јаки магнети во близина на системите и сл.) и
- **Логичка саботажа** – бришење, оштетување илчи модификација на податоците, програмите или деловите на оперативниот систем кој е од значење на државен орган, институција, јавна служба, а најчесто се врши со користење на стандардни услужни програми, сопствени програми или користење на вируси.[132]

Основно обележје на делото **компјутерска шпионажа**, е одавање на тајна, по пат на соопштување, предавање или правење достапни податоци, кои се од доверлива природа.

Компјутерската шпионажа е всушност еден од најмодерните облици на разузнавање, бидејќистранските разузнавачки служби се почесто гокористат интернетот за вршење на економски шпиунажи, како едноставен, ефтин, ненасилен и релативно безопасен начин на прибирање на разузнавачки податоци.[133]

[132] Петрович, Р.,С.,Полицијска информатика, криминалистичко-полицијска академија, Београд, 2007, стр. 105

[133] Повеќе за Компјутерска шпионажа – Cyber espionage, на http://itlaw.wikia.com/wiki/Cyber_espionage

7) Хакерство – оштетување и неовластено навлегување во компјутерски систем

Хакерство е модерен феномен и претставува предизвик да се пробие заштитата на одреден информатички систем и да се навлезе во него.Предизвикот е толку поголем, колку што е заштитата посилна.[134]

Како најчести мотиви, за хакирање во литературата се наведуваат:

- Мотиви кои привлекуваат помало внимание:
  - ✓ Самодокажување;
  - ✓ Интелектуален предизвик;
  - ✓ Финансиска добивка;
  - ✓ Моќ;
  - ✓ Монотонија.
- Како други мотиви ќе ги наведеме (најчесто се врбувани од терористички организации или други држави) :
  - ✓ Тероризам;
  - ✓ Напад на систем;
  - ✓ Одмазда;
  - ✓ Напад на систем;
  - ✓ Земање на правда во сопствени раце;
  - ✓ „тестирање" на сигурноста на системите.[135]

За хакерството би рекол дека претставува една основа за развивање и пробива на сцената на сајбер – тероризмот, бидејќи добро обучените хакери може да навлезат во најобезбедените системи, во државните служби за безбедност, во владини и воени системи и др, па врбувани од терористички или добро платени од странски разузнавачки служби лесно можат да развијат сајбер – терористичка мрежа и напади а кои ќе стане збор во следните поглавја.

Типови на хакери:

- *Хакери од старата школа* – тоа се најчесто мајстори на својот занает, професионалци кои долго време тоа им била професија.
- *Внатрешни хакери* – тоа се воглавно лица кои се вработени, но се разочарани од управувањето или функционирањето на организацијата, или поранешни вработени кои знаат за безбедносните пропусти во организацијата и за процедурата за водење на интерна истрага.
- *Професионални криминалци и Сајбер*-терористи – тука спаѓаат хакерите кои својот талент го искористуваат за криминални дела

---

[134] Затоа како најчести мети на вакви напади се воени и разузнавачки компјутерски системи, и компјутерските системи на други државни институции (м.з)

[135]Grabosky, P., Smith, R., *Crime in the digital age.* Sydney, Federation Press, 1998, str. 52-53, преземено од http://www.aic.gov.au/publications/current%series/hteb/1-20/hteb006.aspx.

или образовани информациони инженери кои ги врбуваат терористите и ги претопуваат во сајбер-криминалци.

- *Скрипт –тинејџери* – станува збор најчесто за тинејџери кои сакаат да се претстават како искусни хакери, но им недостига способност и искуство. Користат програми кои се изработени од други, со цел да направат штета на нападнатиот систем. Скоро во сите случаи, истите се откриени, пред се затоа што една од нивните цели е токму тоа – да се сврти вниманието кон себе.[136]

Легендата во светот на хакерството е секако Кевин Митник, алијас Кондор кој претставува културен херој и инспирација за новите хакери кои го учат тој занает.

Митник, роден 1946 година во предградие на Лос Анџелес, со компјутери започнал да се занимава од средно училиште.[137]

Првото обвинение против него е покренато уште во 1995 година поради фалсификување на кредитни картички, неовластено навлегување во системите на компаниите Моторола (Motorola), Нокиа (Nokia), Фуџитсу (Fujitsu) и многу други, и предизвикување штета која е проценета на 80 милиони долари. Честопати навлегувал и во системите на државните институции на САД како системот на Северноамериканската команда за одбрана НОРАД уште во 1983 година, НАСА (National Aeronautics ans Space Administration, NASA), па дури и ФБИ и долго време беше помеѓу 10- те најбарани криминалци на сајтот на ФБИ. Инспирација е за неколку Холивудски филма како „War Games" од 1983 и „Takedown" од 2000 година.[138]

Втор најпознат хакер е Владимир Левин, Русин по потекло од Петроград кој успеал да навлезе во системот на Citibank во САД во 1994 година и да извлече 10 милиони долари. Ова е неговиот најголем потфат, но е откриен и уапсен, а Citibank успева да го поврати најголемиот дел од сумата.[139]

Прв случај на хакерство кај нас е забележан во 1997 година, а конкретен пример претставува нападот т.е хакирањето на веб-страната на Албанскиот премиер Бамир Топи,[140] во мај 2009 година.

Во домашното законодавство, односно во Кривичниот законик на Република Македонија, казниво со закон е ***Оштетувањето и неовластеното навлегување во компјутерски систем*** како кривично дело во членот 251.

Значи можеме да заклучиме дека основни карактеристики на хакирањето се:

- Неовластено навлегување (упад) во системот, кое се базира на високо професионално знаење,

---

[136]За повеќе различни типологии на хакери видина http://www.drtomoconnor.com/3400/3400lect06a.htm

[137]Повеќе за биографијата на Митник, види на http://www.takedown.com/bio/mitnick.html.

[138]Преземено од http://edition.cnn/SPECIALS/1999/mitnick.background/

[139]Повеќе за случајот на http://www.sccs.swarthmore.edu/users/08/ajb/tmve/wiki100k/docs/VladimirLevin.html

[140]Повеќе за настанот на http://www.24sata.info/tehnologija/internet/6182-makedonija-Hakeri-napali-internet-stranicu-albanskog-predsjednika-Bamira-Topija.html

- Насилен планиран пристап, бидејќи станува збор за пробивање на заштитата на системот,
- Местото на 'упадот' е по правило оддалечено од местото каде што се наоѓа напаѓачот,
- При самото хакирање, напаѓачот истовремено врши и други дела: измами, кражба на идентитет, саботажа, дистрибуција на вируси и др.
- Неовластено навлегување можат да вршат поединци или групи,[141] физички или правни лица.

Она што е битно да се напомене е дека како кривично дело е инкриминирано ***Оштетувањето и неовластеното навлегување во компјутерски систем,*** но во КЗ на Р. Македонија не е инкриминиран ***Сајбер – тероризмот*** како одделно кривично дело.

8)Останати облици на сајбер – криминал

Овде влегуваат уште неколку облици на сајбер-криминал, како што се:

- ***Компјутерски вандализам*** –намерно уништување на информационите системи (со директен физички напад или преку електронски упад и уништување).
- ***Изнудата*** – нуди можност за реализирање на изнуди по пат на сериозни закани за уништување или оштетување на компјутерските компоненти, софтверот и податоците.
- ***Уцената*** – со оглед на тоа дека голем број на најразновидни лични податоци, и податоци кои се дел од тајните и интимниот живот на корисникот се содржаниво компјутерските системи, истите се мошне погодно средство за уценување на корисникот на кој се однесуваат.
- ***Софтверското пиратство*** – неавторизирана репродукција на компјутерски програми, умножување и дистрибуција на програми набавени на илегален начин што носат економски загуби за законскиот поседувач.
- ***Вознемирувањето*** – кое најчесто подразбира испраќање на електронски пораки кон одреден корисник, кој не сака да биде воконтакт со испраќачот на истите, со цел предизвикување на емоционален стрес.

---

[141]Петрович, Р.,С., Полицијска информатика, Криминалистичко-полицијска академија, Београд, 2007, стр.111

8. Современиот тероризам и интернетот

8.1. Тероризмот и интернетот – нивната поврзаност

Тероризмот како најголемо општествено зло на денешнината, не само што не го намалува својот интезитет на дејствување туку со равојот на информационата и електронската технологија и тој еволуира искористувајќи ги тие придобивки за свои криминогени цели.

Модерниот тероризам може да се сфати како обид за пренос на пораката преку организирана употреба на насилство, по пат на искористување на технологијата а особено предностите на Интернетот.

На сцена е постмодерен тероризам, кој 'ја игра старата игра, по нови правила'.[142]

Познат е фактот дека терористите атакувајќи на еден или повеќе делови од физичката инфраструктура, можат да разорат цели системи и да предизвикаат значајни проблеми. Меѓутоа, многу помалку е познато дека терористичките напади врз виртуелната мрежна инфраструктура можат да предизвикаат исти, ако не и многу поопасни национални проблеми.[143]

Со самиот развој на човештвото и осовременување на општеството, со развојот на комуникациите, електрониката и информационата технологија, нивниот моќен потенцијал може да биде насочен кон градење на толеранција, хумани општествени односи и зачувување на прокламираните универзални човекови права и слободи. Меѓутоа, ваквата моќ, многу брзо беше забележана и од оние кои сакаат да ја искористат истата за нечесни намери, генерирање на страв, агресивност, омраза и војна.

Кога идните аналитичари ќе ја истражуваат втората половина на дваесетиот век, сигурно ќе биде дека ќе го проучуваат периодот на Информатичката Револуција. Човештвото има напреднато последните педесет години како никогаш до сега. Една од причините за брзиот техничко-технолошки развој е токму компјутерот. Технолошките можности се зголемени до таа мера што е дозволено конструирање на поголеми и пософистицирани системи со многу посложени и критични операции што пред тоа не можеле ниту да се замислат.

Информатичката технологија денес допира до секој аспект од животот, без разлика на локација во светот. Дневните активности на било кој човек не можат да поминат без користење на компјутер и погодностите што тој ги нуди. Се повеќе и повеќе бизниси, индустрии, економии, болници и влади стануваат зависни од компјутерите т.е веќе се зависни. Не само што се користат за да извршуваат индустриски и економски функции во општеството, туку компјутерите извршуваат и многу функции од кои зависат и човечки животи. Медицинските услуги и воздушната контрола се само две од многуте одговорни функции каде што ако затаи компјутерот како систем, или пак се направи намерна грешка ќе предизвика смрт на многу луѓе.

---

[142]Lawuer, W., Postmoderen terrorizam, Foreign Affairs, 75/5, 1996, стр.24-36

[143]Петровиќ, Р., С., Прилог националној стратегији заштите Кибер-простора, Војно дело, Општевојни научно-теоријски часопис, Министарство Одбране Републике Србије, 2010, стр.191

Комуникациите, науката и индустријата рапидно се развија благодарение на компјутерската технологија, така што и најсложените операции или воспоставување на комуникација и контакти со другата страна на светот се одвива во милисекунди.

Распространувањето на информатичката технологија во светот, сепак има и негативна страна: ја отвори можноста за криминално дејствување на начин што до сега не бил возможен, за жал со помош на компјутерот. Компјутерските системи нудат нови и високо – софистицирани можности за кршење на законот, и креираат потенцијал за развој на нов вид на криминал, сосема различен на оној од традиционален тип. Меѓутоа, и покрај заканите од компјутерски криминал, општеството и понатаму се потпира на компјутерските системи за се, скоро се, во животот, од воздушна и железничка сообраќајна контрола, координација на медицинските сервиси, владини и воени сервиси и др. Потребна е мала грешка во работењето на овие системи за да се стават човечки животи на конец. Брзата експанзија на големите компјутерски мрежи и можноста да се пристапи до многу системи преку само обично логирање од било кој персонален компјутер ја зголеми ранливоста на овие системи и ја отвори можноста за злоупотреба и криминална активност. Консеквециите од компјутерски криминал можат да придонесат за сериозни економски кризи, како и нарушување на безбедноста, [144] особено како поголема закана би ја издвоил заканата од сајбер – терористички напади.

Компјутерскиот криминал вклучувајќи го и компјутерскиот тероризам за кој како што рековме претходно не може да се изведе без компјутер почна да претставува светски проблем од глобални размери, но државите без исклучок и на големите сили некако тешко им оди со справувањето со оваа закана. Зошто е тоа така? Бидејќи законските нормативи не беа изменети на време за поуспешно справување и казнување со овој вид на криминал, слабата интернационална соработка на мултилатерално ниво, како и слаба опременост на безбедносните сили со пософистицирана опрема за детектирање и заштита од ваков вид на криминал.

Кога ова прашање се оценува на меѓународната сцена, проблемите на неадекватностите се воочливи. Компјутерскиот криминал е нова форма на меѓународен криминал и за да се разгледа ефективно, неопходна е меѓународна соработка. Но, соработка и заеднички став очигледно не постои, така што секоја држава на свој начин го толкува тероризмот и компјутерскиот криминал, некои дејствуваат против нив, некои ги подржуваат, затоа и тероризмот од било кој вид и доживеа толкави размери. (За некои држави терористите се оквалификувани како терористи, а за други како борци за слобада).

Некои од проблемите врзани околу меѓународната соработка во областа на компјутерскиот криминал можат да бидат:

1. Недостиг на глобален консензус на тоа кои типови на однесување ќе влезат во рамките на компјутерскиот криминал;
2. Негостиг на глобален консензус на дефиниции на криминално однесување;

---

[144] Златко Шушлевски скрипта за компјутерски криминал стр. 204.

3. Недостиг на стручноста во областа на полицијата, обвинителството и судот на оваа поле;
4. Недостиг на согласност меѓу различните национални процедурални закони во врска со истрагата на компјутерскиот криминал;
5. Меѓународниот карактер на компјутерскиот криминал;
6. Недостиг на екстрадиција и заедничко помагање и синхронизирани механизми за спроведување на законот на меѓународно ниво.[145]

Компјутерските криминалци и сајбер – терористи знаејќи сите погоре наведени недостатоци и слабата меѓународна соработка, ја искористија за свои сопствени цели и почнаа да го употребуваат како оружје компјутерот, а сето тоа што институциите со помош на него ја олесниј а и упростија работата, го искористија како објект и цел за напад и идеална арена за субверзни активности.

Според Dorothy E. Denning (2000), како најчесто цитиран автор, постојат три методи на дејствување од страна на недржавни актери и тоа: хактивизам, активизам и сајбер-тероризам, притоа потенцирајќи дека границите помеѓу овие термини честопати се тешко одредливи и нејасни.

- **Хактивизам**–се однесува на единството од хакирање и активизам, односно термин кој се користи за да се опише "врската" помеѓу хакирањето и политичкиот активизам, на пр. Употреба на техники и методи за хакирање на одреден интернет сајт односно страница, која е земена како мета, со цел нарушување на нормалното нејзино функционирање, но нема за цел предизвикување на сериозна штета. **Активизам**–како термин се однесува на нормалниот и ненасилен начин на користење на интернетот заради поддржување на одредена агенда или кауза, како на пр: 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 пошта (e-mail) и користење на интернетот за дебати и дискусии, формирање на сојузи и коалиции и планирање и координација.
- **Сајбер-тероризмот** е конвергенција помеѓу сајбер–просторот и терористичките активности, на пр. Политички мотивирано хакирање, кое има за цел да предизвика сериозна штета како загуба на човечки животи или сериозни економски последици.[146]

Хактивизмот иако што има за цел нарушување на работата на компјутерите, вршење на различни напади и хакирање на страните, сам по

---

[145] Златко Шушлевски скрипта за компјутерски криминал стр. 205

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

себе не генерира некоја огромна загуба, штета или пак ја загрозува безбедноста на институциите се до моментот кога не се искористени од страна на терористички организации за задоволување на нивните потреби, а искористувајќи го нивното знаење.

Хактивистите генерално земено, на располагање имаат неколку вида на "оружје" кое можат да го употребат за напаѓање на одреден сајт, се со цел да се забави или блокира комуникациската мрежа на одредена владина служба или Law enforsement agency[147], и на тој начин да се зголеми веројатноста за успешен напад по пат на одложување на брзото откривање, предупредување и реакција на нападот:

1) ***Виртуелни блокади*** се генерира толку голем сообраќај односно посетеност на страницата, што истата ја прави недостапна за посета на други корисници. На тој начин го нарушува нормалното функционирање на истата.
2) ***Автоматските е-маил "бомби"-*** се користат за бомбардирање на цели со испраќање на илјадници пораки одеднаш, со цел блокирање на системот.
3) Во третата категорија на хактивистичко оружје се свртени ***компјутерските вируси и црви,*** во форма на малициозни кодови кои ги инфицираат компјутерите и компјутерските мрежи.

Меѓутоа, иако сите сме свесни за тоа колку во последно време се нагласува опасноста од тероризмот, се поголема опасност од сајбер – тероризмот како нов начин на војување со кој се губи стариот традиционален начин, на судир на две различни војски на фронт и водење на војна, сепак не треба да се исклучи и можноста дека малку е пренагласена опасноста од тероризмот, односно како тоа да сака некој да го наметне за да го држи светот во страв. Постојано ни се пласираат информации дека заканата од тероризмот постојано присутна така што светот како да е во постојана војна против невидлив непријател.

Така на пример според една позната констатација на светски познатиот политиколог Даглас Лумис „бомбардирањето е државен тероризам, односно тероризам на богатите. Тој уби повеќе невини цивили во последните шест децении отколку што убиле сите антидржавни терористи во историјата".[148]

„Опасноста од глобален тероризам " е погоден за манипулација покажуваат и податоците за смртноста на американската популација од 2001 година (во споредба со 2500 загинати на 9/11): истата година од сообраќајни несреќи загинале 42.000, а 3.500 од неухранетост, 14.000 од СИДА, најголемиот „убиец" (срцевите болести) однеле дури 700 000, а од убиства загинале 20.000 луѓе.[149]

Не треба да се занемари опасноста од тероризмот, туку со самата постојана присутност во мас-медиумите, како да се наметнува и преувеличува

---

[147] Агенција за спроведување на законот

[148] Цитирано од William Blum, *Rogue State: A Guide to the World's Only Superpower*, (Monroe:Common Courage Press, 2000).

[149] Билјана Ванковска, Меѓународна безбедност критички пристап, Бомат графикс-Скопје 2011, стр. 213

опасноста од него. Факт е дека терористите и терористичките напади можат да направат вистински хаос, многу жртви, но последиците сепак можеби би биле помали отколку светот постојано да се држи под страв, а народот во паника.

8.2.Цел. за кои се користи интернетот од страна на терористите

Тероризмот мошне брзо го менува својот карактер, но не и своите цели, кои се многу поамбициозни, подраматични и веќе попримаат глобални димензии. Тој е „флуиден непријател", но со јасно поставени цели кои секојдневно предизвикуваат шок, ужас, бес, страв, желба за одмазда и нов психолошки и безбедносен амбиент во кој луѓето во светот почнуваат да се чувствуваат како да се во војна.[150]

Секоја терористичка организација е создадена за остварување на одредени цели, кои си ги поставува сама или им ги наметнува владата што ја подржува, без разлика на методот кој ќе го употребат за остварување на таа цел со помош на грабнување, закани, терористи самоубијци, поставување бомби или пак сајбер-терористи крајните цели им се исти и тоа:

1. ***Признавање*** – на почетокот целта е признавање на нивната кауза во национални или меѓународни рамки, привлекување на кадар, воспоставување на фондови или демонстрирање на сила. Затоа и првичните акции им се со поголем шок и предизвикување на што поголема штета.
2. ***Присилување*** – обид да се принудат поединци, групи или влади кон одредено посакувано однесување какво што им одговара на терористите, што најчесто се добива со уцена да не дејствуваат повторно.ж
3. ***Заплашување*** – подразбира обид да се спречат поединците или групите од одредено дејствување, со што се намалува ефикасноста на безбедносните сили, се обесхрабруваат луѓето да прифатат функции во владата, или преку насилство се влијае врз населението.
4. ***Провокација*** –сама по себе е доста специфична бидејќи режира жестока реакција од страна на безбедносните сили, при што врз терористите се врши тортура, репресија, тие наводно се жртви, борци за своите права при што собираат симпатии од пасивните посматрачи и активна подршка.
5. ***Подршка на побуната*** – по пат на заплашување, провокација и др методи, ја присилува владата да ја заштити можната мета, и ја демонстрира својата сила, а немоќта на државата и губење доверба во неа.[151]

Без разлика на кој начин ќе дејствуваат терористите т.е која ќе им биде

[150] Котовчевски, М., Борба против тероризмот, Македонска цивилизација, Скопје, 2004 стр. 11
[151] Котовчевски, М., Современ тероризам, Македонска цивилизација, Скопје, 2003 стр. 277

примарната цел на напад и со каков метод ќе се послужат нивната крајна цел е психолошкиот ефект со кој влијаат врз севкупната јавност, тоа е нивната приоритетна цел.

Интернетот го искористија терористите, за пласирање на својата кауза до домовите на сите граѓани, до сите влади, воени и цивилни организации, на некои заради заплашување па и директни напади, а за други за подршка и учество во нивните терористички операции. Терористичките оперативци исто така поради мрежната безграничност го користат интернетот за да можат да планираат, организираат, координираат и извршуваат планиви од нивната агенда. Ал Каеда како една од најозлаглосените терористички партии во светот, е меѓу првите која го искористи сајбер-просторот за промовирање на своите идеолошки цели преку интернет, привлекување и регрутирање на нови борци и мозоци во своите редови, како и повикување на сето муслиманско население на џихад[152], ширум светот. Ал Каеда ја уведа можноста за непречено вршење на своите активносто со помош на информатичката технологија, и тоа го искористи многу успешно, така при анализа на нивните напади се гледа дека сите се организирани, спремани и подржувани од интернет.

По примерот на Ал Каеда и другите терористички организации ширум светот, како на пр.и Хамас[153], Хезболах, Ира[154]и др, почнаа да ја шират својата пропагандна активност на своите веб-сајтови, пренесување на инструкции, планови и програми, прибирање на средства и опрема и слично. Таа психолошка војна и пропаганда беше искористена за емитување на слики, обезглавени војници, за ширење страв и закани, застрашувачки слики и видеа од нивните подвизи, и тоа без никаква грижа на совест или пак одговорност од нивните членови бидејќи веб-сајт можа да отвори секој, најчесто под лажно име и да пласира се што сака, а притоа да не одговара за таквитр последици.

Различна е примената на интернетот и искористеноста од страна на терористичките организации, го користат интернетот првенствено за прибирање на информации, но некои го искористуваат овој медиум слично на традиционалните политички организации – на пример за прибирање на средства и за ширење на пропаганда, оправдување на своите дејства пред другите, верските терористички организации тоа го пласираат како божја волја, и дека сите други кои не припаѓаат на нивната вера се безбожници и дека треба да платат, за тоа и сл.

Оттука, од аспект на тоа како терористите го користат интернетот, односно за што, генерално земено, можеме да ги поделиме на неколку начини, иако задните намери и мотиви сепак остануваат исти, а тоа се пред се

---

[152]Џихад, (напор/борба) е религизна обврска кај муслиманите, најчесто преведувана како "света војна", преземено од Encyclopedia Britannica,dostapno na http://www.britannica.com/EBchecked/topic/303857/jihad

[153]Хамас е основан од 1987 година, од милитантно крило на муслиманското братство, а во него од 1988 година, се формирани неколку радикални исламски групи, од кои најпозната е Исламскиот џихад. Хамас може да се каже дека е најголемо палестински фундаментално движење, и пред се претставува екстензивна мрежа за социјална помош и создавање, но има и терористичко крило кое планира и изведува самоубиствени бомбашки напади во Израел.

[154]Irish republican News, достапно на http://209.68.13.153/aprn/index.html

како што рековме најчесто политички во спрега и подршка од други држави кои се кријат позади терористичките организации, или други недржавни актери.

1) Водење на психолошка војна

Психолошката војна претставува, начин на војување од современ тип, која без разлика дали се води во мир или за време на војна, крајниот ефект им е психолошки да делуваат врз противникот.

Психолошката војна претставува облик на специјална војна, усмерена против противникот, со психолошко делување на него и постигнување на сопствената цел. Психолошката војна претставува политичка или војна стратегија, со која се настојува со примена на разни средства, да се намали силата нан непријателот, неговата отпорност, и спремноста за борба, а од друга страна зголемување на моралот во сопствените редови и придобивање на што поголем број на сојузници.

Има случаи, под јака психолошко-пропагандна активност, цели војски да се предадат, или да дезертираат од своите редови, а другата страна да ја добие битката без ниту еден испален куршум.

Психолошката војна, не дека не била практикувана и во периодот пред тоа, за време на Втората светска војна, и пред тоа, меѓутоа туку зборуваме за време каде психолошкиот ефект се пренесува директно до секој човек со ширење на застрашување, страв, терор, разни слики од масакри, генерирање паника и чувство на беспомошност кај граѓаните. Порано психолошката војна се спроведувала преку разни гласила, летоци и сл, но потешко било диструбуирањето и ширењето на ваквата пропаганда, што сега за терористите интернетот претставува арена што им овозможува постојано перење на мозоците и заплашување на граѓаните како што спомнав погоре, со разни слики од сопствени акции и тортури и мучење, што директно влијае на аудиториумот, а во корист на терористите, кои што повеќе страв ќе посејат и што повеќе народ ќе го види тоа преку нивните веб-сраници и мас-медиите кои ги контролираат, психолошкиот ефект ќе биде поголем .

Психолошкото оружје, како модерно оружје, кое е се помоќно со информатичката модернизација се разликува од останатите оружја по тоа што:

- Психолошкото оружје делува на психата, а не на телото;
- Психолошкото оружје има најголем дострел, не познава ни граници ни фронтови;
- Може да делува без престан и без одмор;
- Психолошкото оружје се употребува за време на војна и во мир;
- Основна девиза му е да ги прикаже сопствените сили како надмоќни; обучени, безмилосни, а непријателите како неспособни да се справат со нив, со цел да ги придобијат.[155]

---

[155] Википедија, психолошка војна. Превземено од: http://mk.wikipedia.org/wiki/%D0%9F%D1%81%D0%B8%D1%85%D0%BE%D0%BB%D0%BE%D1%88%D0%BA%D0%B0_%D0%B2%D0%BE%D1%98%D0%BD%D0%B0

Терористите го користат психолошкото дејствување како најмоќно нивно оружје, така што сведоци сме дека тероризмот е прогласен како најголема глобална закана на денешнината, каде што целиот свет е вклучен во борба против терористите, и постојано се пласира закана од нов терористички напад, и дека никој не е безбеден од нивните акции, што претставува стратегија на терористите да се дојде до што поголемо медиумско внимание, преку своите медиумски канали и он-лајн пристапот на интернет каде постојано се заплашува таргетираната публика или влада со нови терористички напади. Ефектот ќе биде поголем доколку се опфати што поголема публика, особено продира кон цивилната популација, крајниот цел е промена на владите што не им одговараат и постигнување на политички промени.[156]

Терористите се повеќе го форсираат и ја нагласуваат опасноста од сајбер-тероризмот кој на голема врата влегува особено последната декада и тоа, преку закани со грабнување на авиони или нивно уривање по пат на контрола на лет, блокирање или празнење на банкарските, уништување на реакторите на нуклеарни централи и предизвикување на хаварии слични како онаа од Чернобил, уништување на постројките за нафта и гас и сл, што секако дека во голема мера влијае врз граѓаните и секако дека се јавува страв дека нападите стварно може да се случата терористите не одступуваат и се повеќе засилуваат со таквите убедување, се додека не ги принудат владите да преговараат со нив.

И Ал-Каеда својата активност ја насочи со водење на психолошка војна особено против западниот свет, постирајќи на нивните сајтиви, слики, ЦД-ња од нивните акции, соопштенија и сл, што во голема мера успеја да делува на голем број на нивни приврзаници, и успешно делување и на останатите емитери ширум светот. Тоа особено се продлабочи по нападите од 11 септември 2001 година, каде што на нивните веб-страници постојано се вртеа слики и соопштенија дека се подготвуваат нови напади насочени против САД, кои беа проследени со широка медиумска покриеност, што уште повеќе делуваше психолошки врз светската јавност, и еден општ страв ширум светот секаде каде ќе се споменеше Ал-Каеда и Осама Бил Ладен, а особено на тлото на Америка на кои и после нападите, не престанаа заканите од нови напади.

2) Добивање публицитет и водење на пропаганда

Психолошко-пропагандната активност што постојано ја емитираат терористите преку сите можни начини на пренесување до крајниот аудиториум (граѓаните и владите), има една единствена цел добивање на публицитет-што поголема гледаност и што повеќе застапеност во медиите – поголем ефект.

Порано терористите како средство за стекнување на публицитет т.е за ширење на своите пропагандни активности ги користеа новините, списанија, телевизиите, летоците и разен друг начин, што денеска таа активност се изведува исклучиво на интернетот како најраспространето, безгранично гласило.

---

[156]Hoffman, B., Inside Terrorism (Revised Expanded Edition). New York: Columbia University Press, 2006 стр.174

Интернетот како медиум, навистина значајно ги прошири можностите за терористите да дојдат до безбеден публицитет.

Пропагандата мора да биде уверлива, доступна до секого, разбирлива и привлечна. Ефектот е нели да генерира страв, заплашување, да го бутне моралот на противникот, но од друга страна служи и за привлекување внимание на своите истомисленици, што, подобра пропаганда, толку повеќе подршка морал во своите терористички редови, на пр (сите терористи самоубијци ќе идат право во рај и ќе уживаат на небескиот свет).[157]

Всушност, врската меѓу публицитетот односно медиумите и тероризмот не е едностана, тие се надополнуваат и испреплетуваат. Како што медиумите се од значење за тероризмот, така и тероризмот има значење за медиумите, бидејќи терористичките напади значат зголемен рејтинг, што е и целта на повеќето (ако не и на сите) медиуми.[158]

Психолошко-пропагандната активност не само директно со закани за напад на одредени цивилно-воени цели, можа да се однесува и на други сегменти од секојдневното живеење, што може да допре и да го загрижи секој граѓанин, како : климатски-промени, економска борба, политичка (подршка и поставување на свои влади, претседатели, штрајкови, саботажи, атентати и се друго што може да опфати психолошката пропаганда.

Денес е многу лесно терористите јавно да ги искажуваат своите ставови, да си креираат слики и страници кои тие мислат дека треба да стојат, да пропагираат активности што на нив им одговара, да подржуваат одредени лидери други да ги оцрнуваат, да ги оправдуваат своите ликови и дела и да ја уверуваат широката публика дека тие вршат добри дела, дека тие не се терористи како ги нарекува западниот свет дека тие се угнетени и дека морада се супростават на тој режим, па дури се декларираат и како борци за слобада и дека морада убиваат за да бидат сватени озбилно, другите ги претставуваат како агресори, како непријатели и сл, што особено им го овозможи интернетот и затоа стана нивно најопасно оружје.

Пропагандата е од особено значење за терористите, тие мора да имаат медиум преку кој ќе ја испраќаат својата порака и ќе ги 'оправдуваат' своите активности.[159]

Терористите, прибегнувањето кон насилство, го оправдуваат со три изговори:

а)Терористите тврдат дека не постои друг начин, и дека единственот избор кој им преостанува е прибегнување кон насилство, кое е единствено средство за одговор кон тиранијата на непријателот. Додека на веб-страниците се избегнува споменувањето на насилство спроведено од нивна страна над други, страдање и терор врз недолжно цивилно население. Наспроти тоа, терористичките организации се опишани како постојано прогонувани, а нивните водачи како субјекти на постојани обиди за атентати, нејзините подржавачи како масакрирани, слободата на изразување како

---

[157] Википедија пропаганда и нејзиното делување.

[158]Terrorism and the media, Transnational Terrorism, Security & the Rule of Law, A project financed by the European Commission under the Sixth Framework Programme, July 23, 2008, стр.2 преземено од http://www.transnationaterrorism.eu ,

[159]Charvat, P., Cyber Terrorism: A New Dimension in Battlespace, Centre of Excellence defence Against Terrorism, 2005, стр. 4

ограничена, а нејзините следбеници како предмет на неправедни апсења. Ваквата тактика, со помош на која организацијата се портретира како прогонувана, угнетувана, без права и слобода се најчести пароли на терористите.

б) Нивните членовите се прикажуваат како борци за слобода кои се принудени против сопствената волја да применуваат насилство, бидејќи немилосрдниот непријател ги крши нивните права и го нарушува дигнитетот на нивниот народ или група. Притоа, како нивни окупатори и угнетувачи ги посочуваат владите на државите против кои се засегнати и не им одговараат, и дека освен со борба и промена на таквите недемократски власти друго решение не постои.

в) Откако ќе ги принудат владите да преговараат со нив, терористичките партиите го преземаат следниот чекор, а тоа е трансформација во политички партии, со кои преку своите медиуми и веб-портали пласираат во јавноста дека мирот е постигнат со демократски решенија, со преговори, без насилство, дека правдата е задоволена и сл. (трансформација наОслободителна Народна Армина-ОНА во политичка партија 2001 година)

3) „Ископување" на податоци

Интернетот односно интернет мрежата претставува широка и најраспространета мрежа во сајбер просторот, која и воедно претставува глобално најголема мрежа во информатичкиот свет. Интернетот е всушност систем кој ги поврзува луѓето и информациите преку компјутерите и компјутерските системи. Со право глобалната мрежа интернетот го нарекуваат „автопат на информации".[160]

Светската елекртонска мрежа (WWW),нуди можност за креирање на страници каде без никакво ограничување, секој може да внесува разни информации поврзани со секојдневниот живот, семејството, број на телефон,каде работи и сл, со што всушност си ја нарушува безбедноста и лесно може да биде нечија цел.

Таквиот брз и лесен пристап, овозможува комуникација со луѓето кои веќе ги познаваме и ни се пријатели, но и запознавање на нови профили за кои не сме ни свесни со кого споделуваме информации и мислења бидејќи:

- Луѓето што ги среќаваме на интернет не се секогаш такви какви што ни се претставуваат (прикриен идентитет),
- На интернет не постои приватност во изразена мерка односно информациите кои се објавуваат и појавуваат он-лајн во принцип не остануваат приватни,
- Отвореноста на глобалната интернет мрежа за споделување на содржини сеуште е недоволно ограничена, односно било кој може да објави било каква информација,
- Постирањето на одредени сензационални информации со примамливи содржини, се трејдмарк на одредени интернет

[160] Безбедно на интернет-проектот CRISP (Children's Right on the internet – Safe and Protected) или Заштита на безбедност на децата и нивните права на интернет, достапно на веб: http://crisp.org.mk/content/view/13/40/lang,mk/

сајтови, на нив треба посебно да внимаваме и да им веруваме на се што ќе закачат.

На интернетот може да се гледа како на бесконечна дигитална библиотека, односно сајбер просторот е бескрајно депо на знаење и упатство кои што терористичките мрежи активно ги користат.

Интернетот ни нуди и голем број на алатки со помош на кои многу лесно и брзо ќе дојдеме до посакуваните информации, адреси броеви, испраќање и примање на пораки, пошти, графички слики, звучни датотеки, преземање, скенирање и др, начини на полесна и поуспешна комуникација како на пример што се: E-mail, Download, HTML, Upload, HTTP, URL и други.

Големите индустриски компании, банките, електраните и др, капацитети постојано ги објавуваат податоците околу тоа колку вработени имаат, каков систем за заштита користат, со колкави средства располагаат, кои им се предностите и недостатоците незнаејќи дека сето тоа некој го гледа и снима.

Преку таквиот неограничен пристап и милиони податоци од секакви можни цели, терористите имаат широк спектар на избор и информации за се што може да им користи за идните напади, прибираат и изработуваат упатства, даваат инструкции, ги анализираат и бараат можните слаби точки и најранливи места, прибираат податоци за најсовремените оружја, како се произведуваат, кај ги чуваат, какви системи за заштита користат, изработка на бомби, па дури постои и закана дека терористите развиваат и оружје за масовно уништување.

Како и сите други корисници на интернет , така и терористите имаат лесен пристап на скици, шеми, карти, слики од објектите кои им се потенцијални мети. Првите планови за нападите почнуваат токму тука, каде постојани ги анализираат, пратат, изработуваат можни начини за дејство, упад и сл. При запленет компјутер на припадник на Ал-Каеда пронајдени се такви слики и скици од брана која била детелно разработена за можни напади, експлозии, предизвикување и симулирање на дефекти, електрично напојување, системите за испуштање на вода што ни укажува на тоа дека имале за цел или оштетување на критични точки со експлозија или сајбер-напад на дигиталните системи.

Муслиманскиот хакерски клуб креира веб-страници и објавува линкови на кои може да се најде продукција и ширење на вируси, стратегии за саботажи и хакирање на други страници, имиња на лица кои работат во тајните служби на САД, како и линкови на други Исламистички и терористички веб-адреси.[161]

4)Прибирање на средства

Освен за организирање, планирање и координирање на различни напади ширум светот, терористите преку интернетот успешно успеваат да прибираат финансиски средства, со помош на кои тие опстојуваат, се

[161] Повеќе во Unitet State Institute of Peace, Special Report 116, March, 2004, стр. 7, достапно на http://www.usip.org,

организираат и ги трошат за набавка на оружје и друга опрема која што им е потребна за извршување на нападите.

Терористичките организации на своите веб-портали ја истакнуваат потребата од финансиски средства, и оставајќи број на жиро сметка нивните подржавачи и симпатизериуплаќаат средства кои се слеваат директно на касата на терорисичката организација. Поголем број на терористички организации егзистираат и се финансираат со помош на донации, токму на овој начин. Доколку безбедносните сили им ги блокираат сметките тие на име на невладини организации, добротворни организации, разни фондации и слично ја продолжуваат својата активност на прибирање на финансиски средства. И најголемата терористичка организација Ал-Каеда не би можела да егзистира без донации, кои го полнат најголемиот дел од нивното салдо, а исто така како извор за финансирање го користат и производството и продажбата на дрога и оружје.

Приврзаниците и симпатизерите на терористичките организации, својата подршка ја изразувале уплаќајќи одредена сума на парични средства на банкарски сметки на организацијата. За да биде делокругот уште поширок се барало од нив да отворат електронска пошта каде и тие, во име на организацијата ќе го прошируваат кругот спрема свои пријатели и истомисленици и ќе прибираат средства.

И при разни трансакции од црните пазари при продажба на дрога или оружје парите им се уплаќани на сметка на организацијата како донација, или на некоја невладина организација блиска до терористичката органицација заради прикривање на финансиските средства т.е перење на парите.

Во еден конкретен пример, во јануари, 2004 година во, САД обвинет е студент од Саудиска Арабија, дека заговарал да им помогне на терористички организации во ширење на "светата војна – џихад", на тој начин што го користел интернетот за прибирање на средства и регрутирање на лица, и лоцирање на воени и цивилни цели. Иронијата е во тоа што студентот, бил кандидат за докторски студии по компјутерски науки на Универзитетот во Ајдахо, студии кои се спонзорирани од Агенцијата за национална безбедност на САД.[162]

Најчесто лицата кои редовно донирале средства за организацијата, на тој начин подржувајќи ја нивната кауза и борба, биле регрутирани како свои членови, кои понатаму уште повеќе ќе допринесуваат за придобивање на што поголем број на донатори и симпатизери.

4) Регрутирање и мобилизација

Придобивките на интернетот терористичките организации успешно ги користат и при привлекување и регрутирање на нови активни членови. Пред некој симпатизер да биде регрутиран за активен член во терористичката организација, регрутерите прибираат информации за тоа лице, преку следење на неговиот профил, неговата досегашна активност и реакции што идниот

[162]Weimann, G., How Modern Terrorism uses the Internet, Special Report 116, United States Institute of Peace, March, 2004, стр. 8. Преземено од http://www.usip.org/publications/wwwterrornet-how-modern-terrorism-uses-internet.

терорист ги искажува за нивната кауза, како коментари слики и сл.

Терористите порано преку разни интернет форуми ги ловеа најзагреаните кадри, со предиспозиции што на нив најмногу им одговараат, но сега преку социјалните мрежи тие можат буквално да влезат во секој дом и директно да разговараат со секој поединец и преку отворен контакт тие одлучуваат дали ќе го регрутираат. Тие не само што разговараат со него туку вршат еден вид на разузнавање врз него како личност, врз околината, неговиот дом, работното место и сл, бидејќи терористите особено сајбер-терористите најголем проблем на безбедносните сили им е откривањето на нивните идеи и цели. Потполен удар за организацијата би било инфилтрирање на човек од своите редови во некоја од терористичките ќелии и разотрикавање на што поголем дел од големите умови на организацијата. Затоа и самите регрути кои тоа го знаат многу добро, внимаваат кого ќе регрутираат, и доколку биде регрутиран треба да се истакне во своите подвизи (не секој може да биде бомбаш-самоубиец).

Според Гарбиел Вејман (Gabriel Weimann, 2014)[163], кој вршел истражување по оваа прашање и се потврдува тезата дека терористичките организации постојано се присутни на интернет особено на социјалните мрежи Фејсбук (Facebook) и Твитер (Twitter), каде постојано се врши пропаганда, се величат своите дела и борци, се пуштаат клипови од нивните акции, слики, на големо се шири нивната кауза и имаат огромни резултати од ваквиот начин на ширење на својата пропаганда преку интернет и регрутирање на нови борци.

Анти владината кампања исто така е постојано присутна на веб-порталите на теророите, славење на своите подвизи, оддавање почит на паднатите борци кои го дале својот својот живот во некоја терористичка акција против недолжно цивилно население, пропагирање на верска омраза и испишување на пароли од типот смрт за неверниците, обезбедување на прирачници како да станат терористи, сето тоа претставува чекор по чекор за да привлечат и поттикнат свои идни следбеници.[164]

Во последно време и тероризмот почна да ги менува своите димензии и начини на дејствување, сајбер-тероризмот го нуди сето тоа како и традиционалниот вид на војување, затоа како целна мета на терористите при регрутација се млади лица кои многу добро знаат да ракуваат со компјутер, а уште подобро ако се студенти на некој од високо образовните установи особено од САД, па и од други места. Затоа во последно време се повеќе во редовите на терористите се појавуваат информациони експерти, инжиниери, хемичари, пилоти и сл, и нивните акции како нападите на Кулите Близначки се изведени точно и прецизно, без никаква грешка.

Моќта на интернетот за мобилизирање на активисти се илустрира преку примерот си апсењето на Абдула Очалан, лидерот на Курдската работничка партија, Кога турските власти го уапсија Очалан, десетици илјади

---

[163]Weimann, Gabriel. New Terriorism and New Media Washington, DC: Commons Lab of the Woodrow Wilson International Center for Scholars, 2014. Преземено од: http://www.wilsoncenter.org/sites/default/files/STIP_140501_new_terrorism_F.pdf

[164]Nacos, B., L., Mass-Mediated Terrorism: The Central Role of the Media in Terrorism and Countertrrorism, New York: Columbia University Press, 2006, стр. 240

Курди од целиот свет, излегоа на протести за само неколку часа, како резултат на повиците за протест упатени преку веб-страниците на симпатизерите.[165]

Или пак повиците на муслиманските братства за Арапска пролет, преку социјалните мрежи повик за немири, демонстрации, насилно симнување на власта по пат на употреба на сила и поставување на влада што на нив ќе им одговара. Државите во тој случај се немоќни да се справат со толку народ на улица, разгневен против полицијата, власта, рушејќи се пред себе и најчесто власта капитулира како што беше примерот со Египет.

5) Вмрежување (мрежно поврзување) и комуникација

Новиот софистициран начин на комуникација, кој се одликува со брз и лесен пристап, безграничност и анонимност, беше предуслов сите други начина на комуникација и на поврзување на паднат во втор ред. Особено за терористичките организации, за нивните лидери и најблиските соработници анонимноста особено им оди во прилог, што најголем дел од врбуваните терористи не знаат кој е водачот, кај се наоѓа, која е целта за напад, па дури за откривање на некоја информација не знаат дека се врбувани од терористичка организација, бидејќи потребните инструкции го добива по електронска пошта, а воопшто не знае кој седи од другата страна на компјутерот. Затоа терористите својата активност ја насочија кон дејствување од помали групи наречени ќелии, така да во една зграда може да има и повеќе такви групи, а воопшто и да не се познаваат меѓу себе.

Освен за меѓусебна комуникација, внатре во една организација терористичките организации се меѓусебно мрежно поврзани и остваруваат соработка меѓу себе. Така на интернет можеме да сретнеме веб-портали ширум светот кои неизмерно даваат подршка и го величат тероризмот во име на „светата војна против неверниците – Џихад". За време на војната во Чеченија, од скоро сите Исламистички држави ширум светот бае испраќани финансиски средства, опрема, војници организирани токму на овој начин.

Постојат неколку причини, кои објаснуваат зошто модерните технологии за комуникација, особено компјутерската технологија, им е од толку голема корист на терористите во воспоставувањето и одржувањето на нивните мрежи.

- Распространетост на мрежата и достапност до сечиј дом;
- Со новите технологии значително се намали времето потребно за пренос на информации, што им овозможи на терористичките групи ширум светот да комуницираат на еден брз начин и да се координираат ефективно;
- Новите технологии значително ги намалија трошоците за остварување на комуникација;

[165] Преземено од http://news.bbc.co.uk/214527.stm.

- Со интегрирањето на компјутерската технологија во комуникацијата, значително се зголеми разновидноста и сложеноста на информациите што се споделуваат;[166]
- Просторните и временските бариери се занемарливи.

Затоа со право за денешните терористи и нивните акции ги употребуваат термините *„e-jihad"* и *„ googl-teroristi"*.

6) Планирање и координирање на активностите

Планирањето и координирањето на терористичките организации за своите напади, опфаќајќи целосно сценарио за тоа како треба да изгледа нападот, кои ќе бидат главните точки на напад, времето за изведување на напад, и др активности поврзани околу нападот се вршат во самиот врв на организацијата, со потесното раководство и најблиските соработници. Самиот план за напад како што споменав претходно опфаќа до детали разработен секој дел околу целта која што ќе предмет на напад преку слики, шеми, сателитски снимки снимени од интернет и сите други податоци што им се потребни, и по е-пошта или во вид на пораки дистрибуирани на останатите членови на организацијата т.е само на оние ќелии кои ќе бидат директни извршители.

Со самото раководство околу планот и целта на нападот, комуницира еден, водачот на ќелијата и другите лица до самиот денна нападот може и да не знаат што и каде треба да се изврши заради безбедносни причини да бидат откриени и фатени, да не знаат од каде доаѓаат директивите и кои се можни идни мети за дејство.

За време на нападите на 11 септември 2001 година, сите подготовки и координација со директните извршители на нападот се вршени преку интернет, за што ни говорат илјадници шифрирани пораки пронајдени при одземените лап-топи и на веб-страниците на Ал-Каеда постирани точно со тие датуми и сегменти од нападите што треба да следат (заштитени со пасворди).

Но, понекогаш инструкциите се испорачуваат преку наједноставни шифрирани пораки од типот на онаа на Мохамед Ата, кој како последна порака им ја пратил на останатите осумнаесет терористи, одговорни за нападите на 11 септември: "Семестарот започнува за три недели. Добивме 19 потврдни одговори за студии на правниот факултет, факултетот за урбано планирање, факултетот за применети уметности и факултетот за инжењерство", при што различните факултети најверојатно била шифрата за зградите – мети на напад, [167]пораките најчесто биле испраќани од јавни места за да сочува анонимноста на испраќачот.

Планирањето е процес кој му претходи на координирањето, и кое може да потрае и по неколку години, се додека н се склопи целиот мозаик и се

---

[166]Weimann, G., How Modern Terrorism uses the Internet. Special Report 116, United States Institute of Peace March, 2004, стр. 9, преземено од http://www.usip.org/publications/wwwterrornet-how-modern-terrorism-uses-internet,

[167]Weimann, G., How Modern Terrorism uses the Internet, Special Report 116, United State Institute of Peace March, 2004, стр.10, преземено од http://www.usip.org/publications/wwwterrornet-how-modern-terrorism-uses-internet ,

опфати прецизно и до детали се онаа што треба да се изведе, брзо, прикриено и ефикасно, бидејќи терористите своите акции ги изведуваат со 100 % подготвеност и успешна реализиција. Тоа е така, бидејќи во текот на извршувањето на акцијата се појави и најмал сомнеж или нешто непредвидено, веднаш се прекинува со извршувањето на акцијата за да не дојде до евентуално нивно откривање, и ризикот да се сведе на нула.

Комуникацијата и координирањето помеѓу самите членови на организацијата т.е електронската комуникација се врши преку е-маил пошта, разни форуми, соби за разговор, испраќање на чат пораки преки социјалните мрежи и сл, секако таквите пораки се пропратени со лозинки или се шифрирани. Ваквиот начин им овозможува брза, лесна и ефтина т.е безплатна комуникација затоа и масовно се користат како средство за комуникација.

Сите пораки што ќе се испратат не мора да бидат шифрирани бедејќи таквите пораки повеќе им привлекуваат внимание на безбедносните сили, се испрачќаат и пораки од типот „ќе се сретнеме во 15 часот во метрото" што воопшто нема да ги детектира безбедносните сили дека се работи за нешто сомнително, и нема воопшто некоја детална информација што можат да ја искористат.

Најчест и најбезбеден начин на комуникација помеѓу терористичките групи се врши во отворени виртуелни поштенски сандачиња, кои им пристигнуваат на 2 или 3 корисника со корисничко име и лозинка откако ќе ја отворат поштата. Читање на поштата се врши исклучиво во самиот интернет простор (webmail), значи комуникацијата се одвива помеѓу тие лица и не се користи за испраќање на други адреси, туку си разменуваат пораки на начин што пораките ги стават во фолдер означен како „скици" или ("drafts"), а сите користат иста корисничко име и пасворд на иста електронска пошта, и само тие можат да ги отворат пораките.[168]

Но, интернетот може да послужи и како медиум преку кој ќе им се одврати вниманието на надлежните органи од вистинските сценарија за терористички напад. Заканите, искажани на веб-страниците и форумите, можат да имаат за цел да ги наведат на погрешна трага властите, особено откако на најголемиот број на терористички групи им се познати начините на кои безбедносните служби ги прибираат и анализираат информациите. Терористите знаат дека се јавува загриженост кај безбедносните служби кога ќе забележат зголемени активности преку интернет, па можат да се обидат преку дискусии за лажни напади да го привлечат нивното внимание и да добијат шанса да го набљудуваат начинот на кој што властите реагираат на таквите закани.

По нападите на 11 септември, безбедносните сили на САД, како и другите западно европски сили Еуропил и Интерпол, формираат свои специјално обучено безбедносни сили кои ќе можат да се справат и да им влезат во траг на терористичките организации, и откривање како и попречување на плановите за извршување на своите сајбер-терористички акции или било какви акции што во последно време терористите ги

[168] Википедија -Злоупотреба на интернетот за потребите на тероризмот стр. 421

извршуваат комбинирано со сајбер подготовка (со помош на Yahoo I Googl), а директна физичка акција.

8.3.Користење на интернетот од страна на терористичките организации

Терористичките организации, до пред, брзиот развој на интернетот и информационата технологија, беа насочени кон еден друг начин на војување, обука, комуникација, напади и сл. Но, како напредуваше технологијата и тие не заостанаа по тоа прашање, така да ако другите на неа гледаа како придобивка за развој и за полесна бизнис политика и комуникација, терористите ја искористија за развој на еден нов начин на искажување на своите незадоволства, насочувајќи го како оружје кон воени и цивилни цели, поединци и влади за свои цели и потреби.

Како што истакнав во претходните поглавја, брзиот проток на информации, лесниот пристап, достапноста до сите, им отвори нови погледи и на терористите да почнат интернетот да го користат за регрутација, собирање на средства, ширење на пропаганда, водење психолошка војна, па дури и сајбер – напади. Денес, скоро сите активни терористички организации, имаат свои веб-страници, а некои од нив имаат и по повеќе од една веб-страница и тоа на повеќе јазици.

Повеќето терористички организации се транснационални, т.е се закана од глобален карактер се со помош на интернетот за кој нема географски граници.

- Од **Азија:**
  - ✓ Ал-Каеда (al Qaeda),[169]
  - ✓ Јапонската Црвена Армија (the Japanese Red Army (JRA)[170]),
  - ✓ Ослободителните тигри на Тамил Илам (the Liberation Tigres of Tamil Eelam (LTTE)[171]),
  - ✓ Јапонската Врховна вистина (Aum Shinrikyo),[172]
- Од **Средниот Исток:**
  - ✓ Хамас–Исламистичко движење за отпор (Hamas–the Islamic Resistance Movement),

---

[169] Ал-Каеда нема официјална веб-страница? Alneda.com, е само една од веб-страниците за кои се претпоставуваше дека се администрирани од страна на Ал-Каеда. Денес со клик на Alneda.com се појавува следното: Hacked, Tracked, and NOW Owned by the USA., http://alneda.com/,

[170] Интересно, Јапонската Црвена Армија, има мноштво подржувачи и на социјалната мрежа Facebook, http://www.facebook.com/group.php?gid=14825924343 6&v=wall ,

[171] Официјалната веб-страница на LTTE, http://www.eelam.com/ltte ,

[172] Официјална веб-страница http://english.aleph.to/ ,

- ✓ Хезболах – Господовата партија (Lebanese Hezbollah – Party od God),[173]
- ✓ Палестински Исламски Џихад (the Palestinian Islamic Jihad),
- ✓ Народниот фронт за ослободување на Палестина (the Popular Front for the Liberatio of Palestine (PFLP)),
- ✓ Курдската работничка партија (Kurdish Worker's Party (PKK)) и др.[174]

➢ Од **Европа:**

- ✓ Ирската републиканска армија ИРА (Irish Republican Army, IRA)
- ✓ Баскиско движење ЕТА (the Basque ETA movement)
- ✓ Корзиканската армија (Armata Corsa, the Corsican Army),

➢ Од **Латинска Америка:**

- ✓ Светлосен пат (Shining Path (Sendero Luminoso)),
- ✓ Колумбиската национална ослободителна армија (the Columbian National Liberation Army (ELN-Columbia)),
- ✓ Вооружените револуционерни сили на Колумбија (the Armed Revolutionary Forces of Columbia (FARC))

Терористичките организации не дека го запоставија стариот традиционален начин за извршување на терористички напади, туку само го збогатија и направија уште потежок за откривање, и спречување за негово извршување.

8.3.1. Ал-Каеда

Ал-Каеда е глобална мултинационална исламистичка организација основана од Осама Бин Ладен, Абдула Азам и неколку други милитанти во периодот помеѓу, крајот на 1988 и почетокот на 1989 година, за потребите во Афганистан и борба против тогашниот Сојуз на Советски Социјалистички Републики (СССР)[175]. Таа функционира како терористичка организација и се состои од паравојска и радикално вехабистичко муслиманско движење, каде владее строго шеријатскиот закон, повикот за џихад и исламистичките идеали на глобално ниво.[176]Прогласена е за терористичка организација од ОН, НАТО, Европската Унија, САД, Русија, Индија и разни други земји.

---

[173] Официјалната веб-страница на Хезболах, http://www.moqawama.org/ ,

[174] Повеќе во United State institute of Peace, Special Report 116, March, 2004, стр. 3, достапно на http://www.usip.org ,

[175]Al-Qaeda's origins and links. BBC News. July 20, 2004.

[176]"Middle East, Wahhabi opponent killed in Iran" BBC News. June 26, 2007.

Осама Бин Ладен[177] со својата терористичка организација, ги помина националните граници и почна да војува и напаѓа насекаде во светот. Особено по нападот на Кулите Близначки во 2001 година, стана терористичка организација број еден во светот, од која почнаа да се плашат и најголемите сили како Америка, која зазема став дека со терористите не треба да се преговара, туку дека тоа е зло на денешнината кое треба да се искорени, и дека сите што го крijат или му помагаат на Бин Ладен или на било која друга терористичка организација на било кој начин и тие ќе бидат прогласени за терористи.

Повеќе автори дејствувањето на Ал Каеда го оквалификуваа како глобален тероризам (во светски рамки) – супер тероризам кој го промени целиот светски поредок и начинот на војување. Истражувачите на Оксфордската истражувачка група сметаат дека не станува збор за организација, туку многу повеќе од своевиден конзорциум, мрежа на мрежа на истомисленици, кои симбилички се поистоветуваат со Осама бин Ладен, дејствуваат независно и не ретко за локални цели.[178]

Ал Каеда ја рашири својата мрежа низ целиот свет, така што во едни држави се регрутираат Џихадисти, во друга се врши подготовка и план за нападите, од трета се изведуваат нападите, сето тоа помогнато со помош на интернетот, со кој беше ширена пропаганда и поттикнувани борците да се борат против неверниците и западниот режим на САД. Достапната литература говори дека многу од членовите на Ал-каеда се добро едуцирани, и со огромни познавања од инжињерски и други технички области.[179]

Голем дел од воените експерти во редовите на Ал Каеда, инжењери, електроничари, алхемичари и друго, се школувани на врвните Универзитети по САД, и тоа со државни стипендии, што покажува дека релацијата на Бин Ладен со САД им се во тесна врска, односно тие индиректни и биле помагани од западот, се додека Бин Ладен не се сврте против своите ментори.

За точниот број на приврзаниците на Ал –Каеда не се знае бидејќи се смета дека тие имаат свои ќелии и следбеници во 70 земји ширум светот, спрема некои проценки на Американските стручњаци се смета дека Ал-Каеда има околу 6-7 милиони следбеници, од кои 120.000 се спремни да земат оружје во рака.[180]

Присуството на Ал-Каеда на интернет стана се повидливо од јануари 2002 година, кога групата започна со искористување на неколку, а особено на две веб-страници за испраќање на својата порака.

Ал – Каеда беше постојано присутна на интернет со неколку веб – сајтови, кои ги користеше за повеќе цели на организацијата, но никогаш не беше забележан сајбер – терористички напад токму организиран и спроведен од оваа организација.

---

[177] Осама Бин Ладен е роден 1957 година во Ријад, Саудиска Арабија како 17-то од 52 деца. Неговиот таткосе доселил од Јемен во Саудиска Арабија 1930-тите години. Таму стекнал богатство и меѓу другото контролира една од најголемите индустриски и финансиски корпорации на Блискиот Исток.

[178] Билјана Ванковска, Меѓународна безбедност, критички пристап, Бомат Графикс – Скопје, 2011,стр.212

[179] Spring, T., Al Qaedas Tech Traps, PC World, September 1, 2004, достапно на http://www.pcworld.com/news/article/0,aid,117658,00.asp ,

[180] *Ivona Pastor Perisa:Organizacijski oblici suvremenih teroristikih organizacija.* стр. 149

Како едни од поблиски интернет и тв-станици на Ал- Каеда се сметаат Al-Neda и Al-Jazeera, Jehad.net,As-Sahab и др, за кои организацијата јавно никогаш не потврди дека се нејзини. Ал- Каеда се сврте кон интернет за величење на терористите самоубијци пуштајќи видео клипови на нивните веб -страници како Azzam.com, како и герилските кампови за обука, жртвите на странските војници, светото дело на бомбашите самоубијци, обезглавени тела, слики како и повикување на Џихад и постојано вртење на сликите на првите отсечени глави кои беа ставени на интернат на Пол Џонсон, Ким Сонце-Ил и Даниел Перт, од кои па наваму почна психолошката пропаганда за делата на Ал-Каеда.[181]

На веб-страниците на Al-Neda и Al-Ansar меѓу деугото беа објавени:[182]

- Аудио и видео клипови од Осама Бин Ладен, и говорникот на Ал-каеда, Сулејман Абу Гаит и други.
- Проценки и објаснувања на минатите наоади на Ал-Каеда, идните планови и совети кон другите како да дејствуваат (изготвени од страна на исламски научници и свештеници). Тука биле вклучени серија на написи во кои се тврдело дека самоубиствените бомбашки напади врз Американците, се оправдани според Исламските закони.
- Записи за воените цели на Ал-каеда, и проценки за тоа како остварувањето на таквите цели ќе биде од корист за муслиманската ummah.[183]
-

Scheuer (2008) верува дека Бин Ладен по настаните од 11 септември 2001 година, намерно одржуваше низок профил и тоа поради две причини:

- Прво, за да се избегне САД и сојузниците да ја откријат неговата позиција
- Второ, затоа што тој знае дека со неговото позлекување 'под земја' и тишината ќе предизвика уште поголем страв кај Западната јавност.

На интернет страниците кои беа под контрола на Ал-Каеда, можеа да се најдат сајтови за финансиска подршка, адреси за пријавување на доброволци, коментари на истомисленици, прирачници за војување, како да се направи експлозивна направа, па дури сите свои подржавачи од Арапскиот свет, па и ширум светот ги повика на Џихад (света војна против неверниците), против сите што не се муслимани.

Интернетот уште повеќе ја зацврсти позицијата на Ал-Каеда како

---

[181]Scheuer, M., (January, 2008), Bin Laden Identifies Saudi Arabia as the enemy of Mujahideen unity. Terrorism focus.

[182]Scheuer, M., *Imperial Hubris:Why the West is Losing the War on Terror*, Brassey's Inc., 2004, стр. 79

[183]Ummah, е заедница од луѓе. Терминот се користи за заедницата на Верниците или муслиманите од целиот свет, бидејќи тие се браќа и сестри во Исламот. Објаснувањето е преземено од Исламскиот речник, достапен на http://www.islamic-dictionary.com/index.php?word=ummah ,

најопасна и најраспространета терористичка организација, која сега можеше да ги координира своите напади, да напаѓа истовремено во две или три одделни места или држави, да се стекнува со финансиски средства, да наведува авиони, психолошки да делува ширум светот пуштајќи снимки на интернет и по телевизии како им ги сечат главите на странските војници, репортери и др, со што веќе стана глобална закана за светот.

Медиумската рака на Ал-Каеда, беше значително скратена во септември 2008 година, кога беа затворени неколку од нејзините клучни веб-страници. Еден месец подоцна, само еден форум на Ал-Каеда 'al-Hesbah' почна повторно да функционира.[184]

Ал-Каеда во своите редови регрутира и експерти од информационата технологија, кои даваа логистичка подршка на се што можеше преку интернет да се организира и координира, како и ширење на пропаганда, но сведоци сме дека директен сајбер-терористички напад немаше, што не значи дека организацијата не планира таков напад или напад паралелно со физички напад.[185]

Да го земем какоконкретен пример нападот на 11 септември 2001 година и да претпоставиме едно сценарио во кое Ал-Каеда не само што спроведува физички напад, туку ефектите од физичкиот ги зајакнува и со паралелен сајбер-терористички напад.

- Ако на пример, терористите ја имаа способноста и можноста да навлезат во сообраќајниот контролен систем на Њујорк, и истиот да го онеспособат или замрзнат, ина тој начин да предизвикаат уште поголем хаос во сообраќајот на улиците, со што уште повеќе ќе го отежнат пробивањето на спасувачките екипи до местото на настанот.

- Ако веднаш после падот на кулите, ги онеспособеа и системите за електрична енергија и на тој начин го отсечеа градот од напојување со електрична енергија.

- Ако веднаш потоа ги онеспособеа телекомуникациските системи и мрежи.

Ваквото сценарио веќе би значело потполен пекол, хаос, што воопшто не се исклучува можноста и тоа да се случи или нешто слично, како што воопшто не се очекуваше со цивилни авиони да бидат нападнати и срушени Кулите Близначки.

Пронајдените пораки после нападот потврдија дека целата координација се вршела преку интернет што значи дека тие во своите редови

---

[184]Knickmeyer, E., "Al-Qaeda Web Forums Abruptly Taken Offline, " *Washington Post*. Oktober, 2008. Преземено од http://www.washingtonpost.com/wp-dyn/content/article/2008/10/17/AR2008101703367.htm

[185]Devost, G.,M., Pollard A., N., Taking Cyberterrorism Seriously, Failing to Adapt to Emerging Threat Could Have Dire Cosequences, The Terrorism Research Center, TRC Analysis- June 27, 2002, стр.2, преземено од http://www.terorism.com ,

имаат оперативци со огромни познавања и вештини, високо софистицирано знаење од областа на информатичката технологија, координирање и секако финансиски средства за да се спроведе таков координиран напад на повеќе нивоа.[186]

Ал-Каеда освен од донациите од своите симпатизери ширум светот, уплаќајќи на нивните жиро сметки, се финансира и со помош на црни канали, таа е најголемиот производител на афион во Авганистан, продажба на оружје, грабнување на богати личности бизнисмени и сл, остваруваат профит вреден неколку милијарди евра кои ги користат за обука и изведување на напади ширум светот.Затоа и претставува глобална закана по светската безбедност, на која САД и објави војна, а некои сметаат дека Ал-Каеда е креација на САД во борба против СССР за време на инвазијата во Авганистан.[187]

8.3.2. Хезболах (Lebanese Hezbollah – Party of God)

За изведување на своите терористички подвизи, со користење на интернет и телекомуникациска опрема не заостануваше и партијата од бога, задоена со една верска омраза, која пропагира и со своите акции тоа го докажува да се уништи се што е од друга вера, бидејќи нивната вера е најдобра, а се друго се неверници и за тоа треба да платат.

Уште пред десетина години, во извештај на ЦИА, Хезболах беше идентификувана како една од терористичките организации кои поседуваат и намера и желба да развијат одредени сајбер-вештини, односно да развијат modus operandi за спроведување на ефективен сајбер-терористички напад.[188]

Интересно е тоа што терористите кои се бораат против модернизацијата и истата ја сметаат како зло, бранејќи ги притоа традиционалните вредности и религиозните принципи, не го избегнуваат регрутирањето односно искористувањето на новата технологија за водење на нивните свети војни и за остварување на нивните цели. Така на пример, лидерите на Хезболах носат традиционална облека и својот живот го живеат раководелќи се по Исламските обичаи. Но, како и многу други групи, тие се потпираат на помладите членови на нивната организација кои се обучени и запознаени со модерните комуникациски технологии.[189]

Иста како Ал-Каеда и другите терористички организации и Хезболах на ист начин, регрутира писмен кадар кои ќе можат да ги задоволуваат потребите на организацијата, подготовка на планови, прирачници за тренинг и обука, кои преку електронска пошта ги испраќа на своите оперативци и соработници. Сето тоа е потврдено и пронајдено во компјутерите и лап-топи

---

[186]Bottler, J., Threat 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, стр. 11

[187]Cook Robin (July 8, 2005), The struggle against terrorism. Cannot be won by military means.The Guardian.

[188] McCullagh, D., 'CIA Warns of Net Terror Threat.'*C/Net* 29 October 2002, преземено од http://news.com.com/2100-1023-963771.html?tag=cd.mh.,

[189]Conway, M.,Cybercortical Warfare: The Case of Hizbollah.org. Paper prepared for presentation at the European Consortium for Political Research(ECPR) Joint of Workshops, Edinburgh, UK, 28 March-2 April, 2003, стр. 10

што им се одземени при апсења и претреси.

Врховното раководство на Хезболах, кое донесува одлуки е поделено помеѓу Мецлисал Шура (Советодавното собрание), кое се состои од 12 високи свештенички членови со одговорност за тактички одлуки и надзор на целокупната Хезболах активност во Либан и Мецлисал Шураал-Карар (одлучувачки собрание), предводена од шеикот Мухамед Хусеин Фадлалах, и се состои од единаесет други свештеници кои се одговорни за сите стратешки прашања. Во рамките на Мецлисал Шура, постојат седум специјализирани комитети кои се занимаваат со идеолошките, финансиски, воени и политички, судски, информативни и социјални прашања.[190]

Хезболах вели дека главни извори на приходи им се од донации од муслиманите.[191]Хезболах добива значителна сума на финансии, обука, оружје, експлозиви, политичка, дипломатска и организациска помош од Иран и Сирија.[192] Според извештаите во февруари 2010 година Хезболах добиле 400 милиони долари само од Иран како подршка.[193]Освен од донации Хезболах се финансира и од Шиитската дијаспора во Африка, САД, Аргентина, Парагвај и Бразил, а исто така има и црни фондови од нелегална продажба на цигари и дрога.

Хезболах уште од 90–тите години користи тв и радио – станици со помош на кои врши пропаганда, регрутира свои членови и прибира средства ширум светот. Со помош на сателитската тв – станицата Ал-Манар, Хезболах праќа пораки до своите следбеници ширум светот, и води психолошка војна против сите непријатели од другата вера. Телевизијата на Хезболах Ал-Манар емитува програма направена да ги инспирира самоубиствените напади во Газа, Западниот Брег и Ирак.[194]

Автономноста на комуникациите, е едно од основните залагања на Хезболах. За прв пат он-лајн се појавија во 1996 година, кога веб-страницата Hizbollah.org, стана официјална веб-страница на групата, притоа достапна и на англиски и на арапски јазик.

Хезболах има повеќе веб-страници од официјален карактер, (и сите се достапни и на англиски и на арапски јазик) и тоа:

- Al Manar – тв станица која се емитува уште од 1991 од Бејрут.
- http://www.nasrollah.net, официјалната веб-страница на лидерот на групата Sayyed Hassan Nasrallah и е достапна на француски јазик.

---

[190]Ranstorp, *Hizb'Allah in Lebanon, 1997, p 45*

[191]Lebanese Wary of a Rising Hezbollah.Washington Post. December 20, 2004. Retrieved August 8, 2006

[192]" In the Party of good: Are terrorists in Labanonpreparing for a targer war? By Jeffrey Goldberg. The new Yorker. October 14, 2002.

[193]Harel, Amos:Stern, Yoav (August, 2006)" Iranian official admits Tehran supplied missiles to Hezbollah.

[194]"Terrorist Television Hezbolah has a World Widw reach" National Review on line. December 22, 2004

- http://www.moqawama.org, или позната како 'Асоцијација за подршка на Исламистичкиот отпор' на која се опишуваат нападите на групата врз Израелски цели, [195]

Нивната тергетирана публика се глобално земено и граѓаните на Израел, но и светската јавност.[196]

Нивната психолошка војна која е постојано *on-line,* ги потресе Израелците во 1999 година кога беа пласирани слики на загинатите Израелски специјалци во Либан, и според нив во ниту еден ковчег немало цел труп на еден војник, туку сандаците биле полни со разни делови на тела од повеќе војници. Со овој чин предизвикаа големо незадоволство и конфронтација помеѓу семејствата на загинатите и владата на Израел.

Хезболах како терористичка организација доста успешно ги користи придобивките на интернетот за своите потреби и ширење на пропаганда. Освен Израел како таргетирана држава нивните сајбер-активности са насочени и кон САД така што се забележани повеќе обиди од страниците на Хезболах за упад во нивните владини и воени системи, но за среќа во тоа не успеале, но можеби еднаш и тоа ќе им успее.

Секако зборовите се многу поефтини од човечките животи. На јавноста не и се влева страв од терор кога терористот само зборува, таа е преплашена кога ќе ги види наговите акции и последиците и жртвите од истите. Ако терористите се убедени дека имаат случај, тие ќе сакаат истиот да го презентираат во јавноста, ќе сакаат да бидат слушнати, а демократските општества не би требало да се плашат од ова.Секако дека тероризмот подразбира употреба на насилство за ефект, "зборува со акција", наместо со зборови.

Хезболах и покрај тоа што е претставува терористичка организација, која повеќе години наназад го нарушува светскиот мир, не бирајќи средства и начини за тоа таа, и покрај тоа што се наоѓа на американската црна листа, Хезболах е легитимна политичка партија со широка база на подршка во Либан. Исто така, на 2 мај 2002 година, Европскиот совет (односно тогашните 15 влади на ЕУ) ја ажурира листата на терористички организации како резултат на настаните од 9-11 и во согласност со Резолуцијата на Советот за безбедност на ОН 1373. Додавањето на нови групи доведе листата на ЕУ да биде поблиска до онаа на американскиот Стејт Департмент. Но, Хезболах не се појави ниту на оригиналната ЕУ листа, ниту во ажурираната верзија.

Сепак, во Европа аналитичарите предвидуваат дека означувањето на Хезболах како терористичка организација, ќе има значително влијание, и симболични и практично, во ослабување на организацијата.[197]

---

[195] Исто и http://hizbalah.org/,

[196]Conway, M., Cybercortical Warfare: The Case of Hizbolaah.org, Paper prepared for presentation at the European Cosortium for Political Research (ECPR) Joint Sessions of Workshops, Edinburg, UK, 28 March-2 April, 2003, стр. 11

[197]Jacobson, M., "Adding Hezbollah to the EU Terrorist List", Testimony before the House Committee on Foreign Affairs, June 20, 2007, стр. 3, преземено од http://www.ajc.org/site/apps/nl/content2.asp?c=ijiti2phkoG&b=1323269&ct=4490703#_ftn6 .

8.3.3. Aum Shinryko (Јапонската Врховна вистина)

Аум Шинрикјо (Aum Shinryko) е јапонски култ кој е основан во 1984 година од страна на Шоко Асахара во Токио, првин како клуб за јога и медитација, подоцна во 1989 година, е прогласен за религиозна организација која во 2005 година брои 40.000 членови ширум светот, а 9.000 само во Јапонија.[198]

Овој култ спаѓа во групата на верски секти кои заговараат омраза, нетрпеливост, нетолерантност и дискриминација според расна, полова и верска основа. Ритуалите им се препознатливи по силувања, убиства, самоубиства, дрога и друг вид на криминал.

Јапонскиот култ Аум Шинрикјо ни е позната и по тоа што во 1995 год испушти хемиски средства во токиското метро. Ефектите од овој хемиски терористички напад беа 12 мртви, и неколку илјади повредени[199], што ни зборува за каква организација и се работи и дека тие се спремни се да направат. Особено беше постигнат психолошкиот ефект порадфи употребата на оружје за масовно уништување, кое за прв пат беше употребено за терористички цели.

И оваа култна јапонска група не остана не забележана по тоа што поттикнуваше на убиства, самоубиства, продажба на дрога, прибирање средства преку интернет, па дури на една нивна локација под една планиона бил пронајден и хеликоптер, неколку тона Сарин доволен да усмрти 4 милиони луѓе, повеќе милиони долари и др. што ни кажува за добрата организираност, и комуникација на нивните членови.

Работејќи како подизведувачи за други фирми и на различни софтвери и програми, членовите на култот имале пристап до податоци од софтвери од најмалку 80 фирми и корпорации, како и од повеќе владини агенции. со што значително ја отежнале можноста на фирмите и организациите да знаат кој всушност стои зад изработката на нивниот софтвер. Постои реална закана дека, при склучување на тие договори и изработување на таквите софтвери, припадниците на Аум Шинрикјо (Aum Shinryko) софтверите ги иницирале со најразлични вируси и црви, или во нив намерно оставиле пукнатини и грешки, за да преку нив бидат во можност да го контролираат функционирањето на софтверите.

Така да воопшто не е исклучена можноста дека култот располага со доста податоци од разни програми и софтвери, со високо стручен информациски потенцијал, дека воопшто не им е грижа за тоа кој ќе биде повреден, и како, да го изненади светот и со сајбер – терористички напади.[200]

8.3.4. Ирската републиканска армија (ИРА)

Ирската републиканска армија (ИРА), не е директен корисник на ниту еден веб-сајт или пак директно го користи интернетот за организирање, регрутација, изведување на напади, постирање на слики од истите или сл.

---

[198]Shupe, Anson, D (1998), wolvesWithin The Fold: Religious Leadership New Religious Oxford Rutgers press, p. 162

[199] Котовчевски, М., Национална безбедност, Бомат Графикс – Скопје, 2011, стр. 428.

[200]Bottler, J., Threat 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, стр.8

Сето тое е со умисла, за да не се поврзува ИРА со терористичките напади , или пак се оквалификува за терористичка организација.

Присуството на оваа група на интернет, е всушност индиректно, воглавно преку нејзиното политичко крило Sinn Fein. На веб-страницата на Sinn Fein, [201] постои линк до он-лајн верзијата на Републиканските вести (An Poblacht / Republican News[202]), неделно списание кое подолго време се залага за крај на британското владеење во Северна Ирска.

Од страна на САД, беа преземени најостри мерки против ИРА еден месец по нападите на 11 септември, кога ФБИ затвори веб-страница која беше обвинета за подржување на Вистинската ИРА (Real IRA), - фракција на ИРА.

Со новиот закон донесен во САД од страна Претседателот Џорџ Буш (George Bush)на ФБИ и на ЦИА им се дава за право да запленуваат имот и средства, пред да обезбедат цврсти докази за одредено лице или компанија помага, подржува или на било кој друг начин презема активности кои можат да бидат квалифицирани како тероризам или одржуваат врски со терористи од било кој вид.[203]Така да на Вистинска ИРА (Real IRA) – фракција на ИРА и се забранува било каква активност, прибирање на средства и фондови во САД, и секој кој е поддржувач на истата може да биде казнет и затворен.

Цензурирани се и повеќе веб-страници од страна на универзитетски сервери. Овој феномен се повторува постојано на интернет кога се обидувате да пристапите на сајтови поврзани со терористички или герилски групи, и е доказ дека повеќето од универзитетите и бесплатни хост-сервери вршат скенирање и периодично бараат информации, за кои имаат "обврски" да ги избришат или да ги елиминираат носечките веб-страници. На пример датотеката линк The Irish Republican Army: Heroes Unifying a Nation, беше отстранет од интернет, а беше хостиран на бесплатен сервер http://www.angelfire.com, а доколку кликнеме на таа страница, таму сеуште има содржини кои се однесуваат на фактите и историјата на Ирска, [204]не само оваа и други веб – страници се цензурирани или избришани бидејќи ги поврзуваат со каузата за осамостојување на Ирска, и стоп за Британското владеење врз неа.

Дека и ИРА ја користи информацискатa инфраструктура за сајбер-терористички акции, укажува фактот на упатените закани од ИРА во1997 год, кога Англиската јавностбеше шокирана од заканите дека покрај бомби, атентати и други облици на терористички акти ќе почне да користи и електронски напади на стопански и владини компјутерски системи.

---

[201] Официјалната веб-страна Sinn Fein, http://www.sinnfein.ie,
[202]Irish republican News, достапно на http://209.68.13.153/aprn/index.html
[203]Middleton , J., *FBI shuts down 'IRA' webside*, октомври, 2001, преземено од http://www.v3.co.uk/v3-uk/news/1961115/fbi-shuts-ira-website ,
[204]http://www.angelfire.com/ca/irelandhistory/1998.html#one ,

9.Сајбер–тероризам, како глобална закана по безбедноста во светот

9.1.Поим за сајбер – тероризам

По завршување на Студената војна, временскиот период кој следеше го добил името Пост-индустриска ера, но се попознат и покорстен термин стана и терминот информатичка ера, и навистина доколку во предвид го земеме квантитетот на информациите кои денес во секоја секунда се пренесуваат ширум светот, и растот на компјутерските мрежи во последнава декада овој термин воопшто нее претеран.

Компјутерите и интернетот не само што станаа битен дел од секојдневниот живот, тие станаа есенцијален дел, без кој современото развиено општество не може да се замисли да функционира. Секоја година се повеќе и повеќе луѓе, приватни претпријатија, влади, интернационални организации, нуклеарни централи, разузнавачки организации и др. го користат интернетот и останатите придобивки на информатичката технологија.

Но освен придобивки, информатичката ера со себе носи секакви ризици и загуби. Со оглед на тоа што денес, скоро се тргнувајќи од телекомуникациите, радиото, телевизијата, преносот на електрична енергија, системите за греење, банкарските трансакции, сообраќалната контрола и јавната администрација базира своја функција токму на ваква технологија, од која стана зависно целокупното општество. Многу лесно, орудието наречено Информатичка технологија, би можело од слуга на човекот, да се претвори во негов господар. А ваквата зголемена зависност на општеството од компјутерите и информатичката технологија, од друга страна значи и негова зголемена ранливост, било од физички, а пред се од т.н сајбер-напад, односно една голема електронска Ахилова пета. Непријателска нација или група, би можела да ги искористи овие ранливости и да навлезе во слабо заштитените и обезбедените компјутерски мрежи и да предизвика нарушување па дури и уништување на виталните инфраструктури.

Оттука можеме да кажеме дека без разлика дали станува збор за развиена земја, земја во развој, или некоја друга земја во транзиција, многу лесно може да дојде до општ хаос кој предизвикан од објективни или субјективни фактори, секако продуцира голем број на деструкции и нанесува огромни загуби за државата и директно удира по националната безбедност па дури и на глобалната безбедност во целина.

Честопати голем број од неовластени навлегувања или пробивање на системите се извршени од најразлични побуди, и за најразлични цели, и тоа од досада, заради забава, или како најчесто што знаат да кажат сторителите за да се докажат. Но, за жал терористите и терористичките организации ги користат овие придобивки за свои сопствени цели и кои во сопствена режија создаваат такви лица сајбер-терористи кои ги користат за сајбер-терористички акции ширум светот од кои ни најразвиените држави со најбезбедносни системи не се заштитени, и се на мета на сајбер-терористите.

За да укажеме на што точно се мисли кога велиме сајбер-тероризам, ќе разгледаме сценарија за потенцијални сајбер-терористички акти, кои би

можеле да бидат изведени од сајбер-терористите.

1. *Сајбер – терористот, навлегувајќи во компјутерскиот систем за контрола на воздушниот или железничкиот сообраќај, ќе предизвика директен судир на два цивилни воздухоплови, или на ист начин ќе предизвика судар на два воза.*

2. *Сајбер – терористот, по електронски пат, со неовластено навлегување во компјутерските системи на одредена фармацевтска компанија, може да ги промени формулите за изработка на одреден лек, а загубата на човечки животи како последица на тоа би била катастрофална.*[205]

3. *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 одредена хемиска супстанца штетна за човековиот организам, и на тој начин ќе предизвика болести или смрт кај припадниците на одредена нација, конзументи на таквата храна.*

4. *Сајбер – терористот ќе навлезе во мрежата на сообраќајниот сигнален систем на еден град при што ќе направи хаос и ќе го парализира целиот град само со помешување на работењето на семафорите и ќе предизвика колапс.*

5. *Сајбер – терористот може да одлучи по електронски пат да го промени притисокот во цевките на гасот, со што ќе предизвика оштетувања на вентилите и ќе доведе до експлозија на цели населби или предградија. Истото се однесува и на можностите за напад врз електричната мрежа.*[206]

6. *Сајбер – терористот ќе го наруши финансиското работењето одредена држава и тоа на банките, интернационалните трансакции и работењето на берзите во светот или во одредена земја, со цел да го поремети економскиот систем на земјата и вовлекување во криза, која ќе резултира со колапс на власта.*

7. *Сајбер – терористот, по електронски пат може да навлезе во контролните системи на некоја нуклеарна централа. Доколку успее*

---

[205]Botller, 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, стр. 10

[206]Collin, C., B., the Future of Cyber-Terrorism: Where the Physical and Virtual Worlds Converge, 11th Annual International Symposium on Criminal Justice Issues, Institute for Security and Intelligence, преземено од http://afgen.com/terrorism1.html,

да го наруши нормалното функционирање на системите за ладење, може да предизвика прегревање и топење на реакторското јадро. Ефектите од таквото топење, се познати од хаваријата на нуклеарната централа во Чернобил во 1986 година.

Со ваквите сајбер – терористички напади самите системи на државите ќе бидат совладани т.е целата држава ќе биде во хаос, паника, страв со што и целите на терористите ќе бидат задоволени односно ќе испаднат победници и го остварале тоа што им било цел или мета на сајбер-терористичкиот напад. Освен тоа, оние кои се задолжени да ја заштитуваат земјата и нацијата, не се предупредени т.е се неспремни или недоволно опремени и специјализирани за успешно справување и одбрана од ваков тип на напад, бидејќи речиси е неможно фаќањето и лишувањето од слобода на сајбер-терористот одговорен за нападот, бидејќи истиот се наоѓа на другата страна на светот.

9.2. Дефинирање на Сајбер – тероризмот

Сајбер-тероризмот е релативно нов термин и под истиот се подразбира незаконска употреба на сила или насилство врз лица или имот, со цел да се заплаши или присили одредена влада или цивилно население, заради остварување на политички или општествени цели.преку експлоатација на информатичко-компјутерските системи.[207]

Во однос на дефинирање на сајбер-тероризмот пред да истакнам и други дефиниции од други автори сакам да кажам дека сеуште не постои една воопшто прифатена дефиниција, туку различни автори различно го дефинираат.

Кога станува збор за елементите на сајбер-тероризмот, исто така постојат недореченост и различно погледи около нив од различни автори. Така на пример може да се каже дека постојат четири основни елементи : методи, алати, мотивација и цел.

Методи на напад:

Постојат три методи на напад на сајбер тероризмот

- *Физички напад* – напад против комуникациски објекти и/или далеководи. Може да се постигне со употреба на конвенционално оружје со цел да се уништи или озбилно оштетат нивните компјутери и терминали;
- *Електронски напад* – напад кој се постигнува со употреба на висока електромагнетна енергија или електромагнетен импулс кој иницира преоптеретување на струјно коло на сметачот или на микроталесниот пренос;

[207] "Overview of Cyber-terrorism," преземено од http://www.cybercrimes.net/Terrorism/overview/page1.html

- *Напад на компјутерската мрежа* – се постигнува обично со употреба на злонамерен код како би се искористила слабоста на туѓиот софтвер и манипулација со него.

Алати:

- Крадење на идентитет;
- Убацување на вируси;
- Употреба на штетни софтвери (engl.malware);
- Уништување или манипулација со податоци;

Мотивација за нападите:

- Политички промени;
- Социјални промени;
- Економски променич
- Од верска природа и др.

Цел на напад:

- Владини организации;
- Персонални компјутери.

Заедничко за сите нив е дека сајбер-терористичките напади се умислени т.е добро испланирани, бидејќи подразбираат планирање, и примена на софтвер за извршување на нападите.

Според **НАТО** (2008) **сајбер- тероризмот** е сајбер напад со помош на користење или искористување на компјутер или комуникациски мрежи да предизвика доволно уништување, да генерира страв или да го застрашуваат општеството во идеолошка цел.[208]

Друга пак дефиниција од Американскиот оддел за национална безбедност гласи : „кривично дело сторено преку компјутери резултира со насилство, смрт и/или уништување и создавање на терор со цел на присилување на влада да ја промени својата политика."[209]

Карактеристично што сакам да го истакнам за сајбер-тероризмот т.е сајбер војувањето, а што е многу карактеристично т.е многу ранливо за големите сили и држави е тоа што група или поединец може да направи штети од огромни размери па дури и да ги присили владите да прогласат воена состојба, а не знаат со кого војуваат, каде се наоѓа и кои се неговите идни планови и цели.

Затоа сајбер-тероризмот почнаа да го практикуваат и стана омилен кај терористите бидејќи нема класичен стил на војување, нема жртви од една страна само еден обучен терорист од полето на информатичките науки е доволно да си ги исполнат целите и да внесат страв кај населението. Затоа се почесто после одреден терористички чин откако ќе се спроведе истрага се увидува дека токму сторителите на таквите акции се врвни инжинери,

---

[208]NATO, 2008 Cyber defence Concept MCO 571.Brussels, Belgium.

[209]Wilson, C.,(2003).Computer Attack and Cyber terrorism: Vulnerabilities and Policy Issues for Congress.CRS.web.

доктори, информатичари, пилоти и др кои завршиле на најврвните светски универзитети , а често се стипендирани и од државите во кои што живеат.

Сајбер-тероризмот е конвергенција помеѓу сајбер просторот и терористичките активности, на пример: политичко мотивирани хакирање, кое има за цел да предизвика сериозна штета како и загуба на човечки животи или сериозни економски последици.[210]

ФБИ, го дефинира сајбер-тероризмот како умислени политички мотивирани напади врз информациите, компјутерските системи, компјутерските програми и податоци, што резултираат со насилство против цели кои не се воени, од страна на суб-национални групи или тајни агенти.[211]

Според Lewis, **сајбер-тероризмот**подразбира користење на компјутерските мрежи како алатка за да се уништат или онеспособат критични витални национални инфраструктури (како енергија, транспорт, владини операции), или заради заплашувањена владата или цивилното население.[212]

Сепак, како една од најцитираните дефиниции на поимот сајбер-тероризам е онаа на Denning дека **„Сајбер-тероризмот** е конвергенцијата од тероризмот и сајбер просторот. Генерално земено, станува збор за незаконски напади или закани од напади против компјутери, мрежи и информации складирани 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 сајбер-тероризам, истиот треба да предизвика насилство врз луѓе или имот, или барем да предизвика доволно штета со тоа што ќе генерира страв. Нападите кои резултираат со смрт, телесни повреди, експлозии, авионски несреќи, загадување на водата, или тешки економски загуби, би биле конкретен пример.[213]

Од повеќето дефиниции од различни автори можеме да направиме дистинкција и да заклучиме дека сите злодела направени со помош на компјутер т.е преку интернет како на пример: кражба на информации од кредитни картички, детска порнографија, навредлива содржина, спам пораки, закани од едно до друго лице, не можат да се сметаат за сајбер-тероризам. Движечката сила зад сајбер-тероризмот е првенствено политичка и/или религиозна основа.

Од погоре наведените дефиниции можеме да видиме сличности во дефинирањето, но има и разлики. Според согледувањата, оваа комплексна појава т.е ***Сајбер-тероризмот претставува умислена примена на***

---

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

[211]Pollitt, M., M., "A Cyberterrorism Fact or Fancy?", Proceedings of the 20th National Information Systems Security Conference, 1997, стр. 285-289, како и The terrorism research center http://www.terrorism.com, исто види http://searchsecurity.techtarget.com/sDefenition/0..sid14_gci771061,00.html,

[212]Lewis, A., J., Assessing the risks of Cyber Terrorism, Cyber War and Other Cyber Threat, Center for Strategic and International Studies, Washington DC, December, 2002, стр.1, преземено од http://csis.org/publication/assessing-risks-cyber-terrorism-cyber-war-and-other-cyber-threat,

[213]Denning, E., D., "Cyberterrorism", Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services, US House of Representatives, May 2000, преземено од http://www.cs.georgetown.edu/~denning/infosec/syberter.ror.html

штетни активности и/или напади или закана извршени со помош на информациско-компјутерските системи и мрежи, со намера за постигнување на понатамошни политички, социјални, идеолошки, религиозни, економски и слични цели или заплашување на луѓето од такви напади, за остварување на наведените цели.

Анализирајќи ја подетално дефиницијата можеме да ги издвоиме основните елементи:

1) ***Умислената примена*** – однапред планирање и подготовка за извршување на некој штетен напад или акт;
2) ***Штетни активности*** – активности со кои се нарушува нормалното функционирање на ИК системи и мрежи (од оштетување до онеспособување и уништување);
3) ***Информатичко-компјутерски системи и мрежи*** – се објект на напад на сајбер-терористите;
4) ***Заплашувањето*** – влевање страв кај некоја личност, популација или сеење страв во целата држава за да се принуди превземање/непревземање ништо од нивна страна;
5) ***Остварување на наведените цели*** – постигнување на политички, социјални, идеолошки, религиозни и слични цели.

При преземање на одредени терористички акции сајбер-тероризмот не секогаш мора да биде главен удар врз одредена цел туку терористите ги користат и другите нивни методи така да сајбер-тероризмот може да биде и добра логистика при извршување на терористичките акции како на пример: прекин на комуникации, прекин на електрична енергија, сообраќаен хаос, давање лажна тревога или тревога на друга локација за да се овлече вниманието на друга страна на службите за безбедност и др. па може да се корист за:

1) Да ја направи ранлива целта пред спроведување на физички напад,
2) Помош при планирањето на други терористички активности, или
3) Да произведе повеќе страв и збунетост при истовременото спроведување на други терористички акти.[214]

Кога се работи за сајбер-тероризмот, како што напоменав претходно не се имуни т.е не се заштитени ниту најголемите сили со најаки одбрамбени системи и разузнавачки и др. безбедносни системи како што се САД, Британија, Русија и Кина токму поради начинот на извршување на сајбер-терористичките напади каде што терористот е на едната страна на планетата, а целта на друга и само со едно притискање на копче на тастатурата се случуваат несакани настани кои резултираат со жртви и страв.

Токму поради тоа треба големите сили да имаат поголема соработка

[214]Berinato, S., The truth about cyber-terrorism, CIO Magazine, Vol.15, No. 11, March 2002, достапно на http://www.cio.com/article/30933/CYBERSECURITY The Truth About Cyberterrorism,

кога се работи за глобален тероризам и тие ставови околу дефинирањето и начинот на справување со тероризмот во глобала па и сајбер тероризмот треба да се изедначат и да се унифицираат што до ден денес нее така.

Стратегијата за сајбер-безбедност на Британија која е издадена во ноември 2011, назначува дека „ ќе работиме интернационално за да развиеме меѓународни принципи или правила на патот за однесување во сајбер-просторот (Влада на Велика Британија, 2012)–јазик не различен на овој користен од Русија и Кина кога предложија„меѓународен код на однесување" за информатичка безбедност (Обединети нации 2011 година). Но како што е документирано претходно (Гиллес 2012 година; Томас, 2011 година) Руската и Кинеската доктрина и пишување нагласуваат многу различен сет на сигурносни предизвици од оние кои нормално ги засегаат САД и британија наспроти Русија и Кина.

Дури и пред адресурање на несогласувањата во ставовите на перцепцијата, постои побазичен проблем на отсуство на заедничка терминологија помеѓу главните играчи во сајбер-просторот. Дефинирањето на ваквите поими како сајбер конфликт, сајбер војна, сајбер напад, сајбер оружје и сл. Кое го користат САД и Британија, КИна и Русија не го прифаќаат, дури ни каде што постојат официјални или генерално признаени дефиниции на секој односен јазик.

Иницијативата на Западниот институт конфузно го етикетираше билатералниот однос Русија – САД, виде начин за излез од ќорсокак со внесување на заеднички труд меѓу Американски и Руски експерти да најдат концензусни дефиниции околу три групи на области во терминологијата на сајбер-сигурноста.

Овој пофален напор на прв поглед изгледаше дека прави значителен прогрес во поставување на основата на меѓусебно разбирање. За жал, овој прогрес покажа дека е илузорен од кога договорените дефиниции на секој јазик не се слагааедна со друга, оставајќи ја секоја страна со впечаток дека е постигнат консензус, но всушност тој останува далеку како никогаш.

На пример на англиски јазик, дефиниција за сајбер војување гласи: Сајбер војување се сајбер напади што се авторизирани од државници, против сајбер инфраструктура кои се дел од воена кампања.

На Руски верзијата гласи: Воени акции во сајбер просторот се сајбер напади изведени од држави, група на држави или организирани политички групи, против сајбер инфраструктури кои се дел од воена кампања.[215]

Разликите меѓу навидум хармонизирани дефиниции и нивни импликации јасно е дека бара понатамошно елаборирање. Разликата меѓу владина кампања и воена кампања ккога се дефинира војување е доволно проблематична, но споменувањето на организирани политички групи, присутно во едниот јазик, но не и во другиот ќе создадат сериозни потешкотии ако се направи обид да се одреди дали он-лајн активностите на Руски групи кои се под покровителство на државата како НАШИ всушност конституираат необјавена сајбер војна.

Сепак треба да се усогласат ставовите и да се води една поорганизирана

[215] 2013 5th international Coference on Cyber Conflict K. Podins, J.Stanissen, M. Maybaum (Eds.) 2013 @ NATO CCD COE Publications, Tallinn стр. 416.

и заедничка борба на сите држави против тероризмот, бидејќи терористите таа неусогласеност и контра ставови ги користат за свои потреби и цели.

9.3. Закани од сајбер-тероризам

За поголеми размери и поголем замав на сајбер тероризмот можеме да го сметаме почетокот на 90 – тите години со забрзаниот развој и употреба на интернетот, како и развојот на информатичкото општество и вгнездување во секој сегмент од човековиот живот. Таквиот брз технолошки развој направи бум во сите сфери на општественото живеење, и им го олесни животот на луѓето, но од друга страна тука се и ризиците кои ги носи со себе зависноста од високата технологија.

Можеби на почетокот му се даде и преголемо значење на поимот сајбер-тероризам за кој пак постои неусогласеност на ставовите помеѓу големите стручњаци бидејќи хакирање на владина веб-страна, електронски кражби на податоци на компании, пуштање на вируси во системите и др. им се лепеа етикети на сомнителни случаи на сајбер тероризам, односно поради лошата информираност т.е дезинформираност од обичен компјутерски престап или криминал се пренесува на луѓето од страна на медиумите, како тероризам што уште повеќе влијае за влевање страв кај населението.

Затоа, при разгледување на Сајбер-тероризмот мора да се користи еден мултидимензионален пристап, затоа што како прво да направиме разлика за да се оквалификува некој напад како сајбер-тероризам мора да има голема материјална штета, да влее страв и цивилни жртви, да има политичка заднина и тука е и мотивот, а ако нема политичка заднина мора да се најде и мотив за што би дошло до некој напад и што е целта. Но, и не треба да се опуштиме и да го набљудуваме само како термин и дека не претставува закана за безбедноста бидејќи до сега сајбер-терористички напад од поголема деструктивна природа и нема како уништување на постројки, напад на нуклеарни централи, на електро централи, па јавни објекти на системи за транспорт и други круцијални компоненти на националната инфраструктура. Сајбер нападите се вообичаени, но истите не се вршени од страна на терористи и немале за цел предизвикување на штети од толкави размери, со што би се оквалификувале како сајбер-терористички напади.

По прашањето: дали заканата од сајбер-терористички напади е креација на големите сили?, за да можат светот да го држат во паника, во страв, да се биде постојано во војна со противник што воопшто не го гледаме, па дури не знаеме ни дали сето тоа е можно да се изведе до тој степен. Дали системите што носат печат строго доверливо или државна тајна, толку лесно можат да се изманипулираат и украдат или сето тоа е пренагласено. Експертите повторно имаат поделени мислења. Едните одговарат негативно и нив ќе ги наречеме 'песимисти', а другите потврдно – 'оптимисти'.

Оптимистите сметаат дека сето тоа е пренагласено, а песимистите постојано прикажуваат црни сценарија, разор, хаос и многу жртви.

Оптимистите можеби имаат повеќе право,бидејќи веќе комјутерската технологија повеќе од две децении е навлезена во сите институции и успешно се извршуваат работните задачи. Во случај на грешки во работењето или упад

во системот тие се така дизајнирани да бидат отпорни или веднаш да сигнализираат нешто сомнително. Секако дека тие не се оставени сами на себе туку има обучен персонал кој 24 часа ги набљудува и контролира системите, кои не само од сајбер – напад, туку може да дојде до дефект, природна непогода или слично, што не значи дека и немало таков случај, па се навреме откриено и поправено, што ни укажува дека тие луѓе веќе имаат искуство, и не можат така лесно да бидат измамени. Прашањето е дали нивното искуство и знаење е доволно да се спречи еден сајбер-терористички напад?– останува да видиме до каде се спремни и способни да одат тие болни умови.

Но што правиме во случај песимистите да се во право, доколку навистина едно кликање со глувче може да тргне од картата на светот цел град и однесе илјадници жртви и причини милионска штета, дали тогаш ќе биде доцна за калкулации и само со пребројување на жртвите ќе биде доволно, тогаш тие што со неверување и непреземање на ништо ќе сносат ли вина дека им овозможиле на терористите лесен пристап и добар плен.

Многу компјутерски експерти од областа на безбедноста, не веруваат дека е можно по пат на користење на интернетот да се предизвика смрт од поголеми размери. Според Weimann (2004), флексибилноста и отпорноста на компјутерските системи кон напади, е резултат на значителна инвестиција на време, пари и експертиза. Особено кога станува збор за државните компјутерски системи.[216]

Она што загрижува, се секако системите кои се контролирани од страна на приватниот сектор, како на пример системите за пренос на електрична енергија, гас, нафта, системите за комуникација и превоз и сл. Кои се многу поранливи и послабо заштитени за разлика од воените и државните системи. за кои системи државите т.е владите вложуваат големи средства за заштита, за шифрирање, постојано следење од страна на експерти сето тоа за да бидат подобро заштитени и побезбедни.

Во однос на проценката на заканата од сајбер-тероризам, експертите се согласни дека треба да се даде одговор на две прашања:

- Дали постојат актери кои се доволно способни и мотивирани за извршување на таков сајбер – терористички напад?, и
- Дали постојат ранливи цели кои се можна мета на сајбер–терористички напад?

Одговорот на првото прашање е **да**!, така што треба да нагласиме дека тука како целна група се веќе вработените експерти во самите компании кои располагаат со соодветните техники и вештини за управување со конкретните системи, а малкумина други потешко би се снашле веднаш да навлезат во системот без претходно негово познавање или проучување. Но, секако дека останува отворена можноста терористичките групи да регрутираат вработени, или поранешни вработени лица таргетираните компании или системи. Останува само прашањето, колкава би била штетата доколку навистина

[216]Weimann, G.,Cyberterrorism, How Real is The Threat?, Special Report 119, United States Instutute of Paece, December, 2004, стр. 9, преземено од http://www.usip.org/publications/cyberterrorism-how-real-threat,

терористите регрутираат вакви лица, со оглед на тоа дека, вработените во компаниите кои раководат со електричната енергија, со браните, со нафтените и постројките за гас, со комуникациските системи се добро обучени за справување со вонредни ситуации во случаи на поплави, пожари, урагани, торнада и др непогоди. Тие исто така се упатени и обучени и за справување и решавање на проблеми предизвикани од човечки фактор.

Истиот одговор може да се даде и на второто прашање. Системите кои се користат за големите индустрии, за владините и воените објекти и постројки, секако дека се најсовремени и со најдобра заштита, но факт е дека тие по својата природа се доста сложени, па оттаму и кај нив може да има пропусти односно слабости кои би можеле да се искористат. Како што образложив во првото прашање дека, доколку терористите не успејат од надвор сами да ги пробијат системите и да извршат упад во програмите, би можеле да вербуваат луѓе од внатре - т.н 'инсајдери'кои своето незадоволство или пак за пари, ќе навлезат во системот и за сметка на некоја терористичка група ќе предизвикаат значителна штета или хаварија.

Како причини кои одат во прилог на тврдењето дека моменталната закана од сајбер-терористички закани е претерана, се наведуваат следните:

- Како *прво*, сајбер-тероризмот и сајбер нападите се нешто ново, па на јавноста мошне брзо и го привлекува вниманието.

- *Второ*, мас-медиумите со своето еуфорично и преувеличено известување за настаните поврзани со тероризам им прават голема услуга на терористите кои со најмала или закана од помал тип со помош на мас-медиумите добиваат внимание како што само можат да посакуваат.

- *Третата* причина се токму политичарите, кои постојано ја потенцираат и најчесто преувеличуваат опасноста од сајбер-терористички напади, како би укажале на тоа дека владите кои го застапуваат народот воопшто немаат изградено стратегија за борба против оваа закана.

- Незнаењето е *четвртиот* фактор, а се однесува на профитирање на одредени групи на луѓе кои го искористуваат овој фактор. Имено, многу компании кои се занимаваат со развој на технологијата, се обидуваат да привлечат што е можно повеќе државни грантови за истражување во областа на компјутерската безбедност, што би продонела за зајакнување на националната безбедност. На нив им одговара јавноста да верува дека заканата од сајбер-терористички напади по националната безбедност е многу сериозна.

- *Петтиот* фактор, е токму немањето на една унифицирана и општо прифатена дефиниција за поимот сајбер-тероризам, што ја збунува јавноста и дава повод за креирање на најразлични митови за сајбер-тероризмот.

Досега не сме сведоци на некој поголем и посериозен сајбер – терористички напад но што со заканите за во иднина? Развојот на технологијата со неверојатна брзина и се побројните експерти од областа на компјутерската технологија им одат во прилог на терористите да ги искористат како алатка.

Сајбер – тероризмот како најмлада гранка во терористичките тактики на војување, сеуште го нема доживеано својот максимум, туку тој е во развивање и неговото време допрва следи. Денешните терористи, сеуште во најголем дел го применуваат старниот традиционален начин на терористички напади, со пушки во рацете и бомби околу појасите, но нивните поколенија кои допрва следат, информационата технологија од ден на ден се повеќе се равива, не е чудо со помош на глушец и тастатура пред нив да ја водат војната против цели држави на другата страна на светот. За жал таквите се предвидувањата на експертите и сите се свесни дека кај терористичките организации овој метод е се поатрактивен.[217]

Со зголемување на антитерористичките единици и нивното се поуспешно справување со терористичките акции, не значи дека терористите се повеке ќе се преориентираат кон неконвенционално оружје, односно кон преземање на сајбер-терорстички акции. Останува предизвикот да се процени што треба да се стори во врска со оваа закана по безбедноста од сајбер-терористички напади, без притоа да се преувеличува нејзиното значење, како и без да се манипулира со стравот кој произлегува од истата. Авторите кои ја третираат оваа проблематика, се согласни во тоа дека барем за сега, киднапирањето на возила и авиони, камионите бомби и биолошкото оружје се многу поголема закана по човештвото, отколку сајбер-тероризмот.

Терористите бараат начини за спроведување на напади од далечина, со што би ги намалиле шансите за откривање и фаќање при обидите да предизвикаат напад или само паника и страв кај таргетираната популација. Сајбер-тероризмот ги исполнува овие барања, и иако можеби заканата од сајбер-тероризмот е преувеличувана и манипулирана, постоењето на истата ниту можеме, ниту смееме да го одрекуваме или игнорираме.[218]

Иако можеби сајбер тероризмот не е моменталниот најупотребуван начин на терористите, тој останува реална и растечка закана за земјите во светот.

---

[217]Weimann, G., Cyberterrorism, How Real is the Threat?, Special report 119, United States Institute of Peace, December, 2004, стр.11, преземено од http://www.usip.org/publications/cyberterrorism-how-real-threat

[218]Ellsmore, N., Raghu A., Cyber Terrorism – Are We There Yet?, Stratsec, May 2010, стр. 11, преземено од www.stratsec.net,

9.4. Криминална активност и профил на сајбер терористот

Без разлика за каков вид на сајбер-терористички напад или активност се работи мора да нагласиме дека станува збор за криминална активност за која доколку бидат откриени сторителите кривично ќе си одговараат според законите на државата каде е извршено кривичното дело.

Кога говориме за сајбер-тероризмот веднаш знаеме дека главно и основно оружје му е компјутерорт, без кој неможе да се изврши нападот. Постојат безброј начини на кои што терористот може да го искористи компјутерот како алатка за извршување на напад како на пр: компјутерска шпиунажа и саботажа, уништување или манипулација со податоци, хакирање, изнада, уцена, кражба на идентитет, компјутерски вируси, идр. Кој од овие дела ќе ги направи терористот зависи од целта што сака да ја постигне во моментот, или пораката што сака да ја испрати до некого.

За да пак некој сноси кривична одговорност за било кое или напад треба да се открие **Кој** – го извршил делото, **Каде** – е извршено делото и **Кога** – е извршено делото, и секако други активности во текот на истрагата кои ќе покажат конкретно како е извршен некој напад, која е логитиката, кој е мотивот за напад и др.

Значи сајбер-тероризмот нема само за цел заплашување на луѓето туку се вршат директни напади со цел оштетување на компјутери и искористување на слабостите во системот на таков начин што ќе оствари што поголема штета и негативно влијание врз секојдневниот живот на што поголем број на луѓе. Постојат повеќе начини и активности што сајбер-терористот може да ги преземе по упадот на одреден информационен систем и да изврши сајбер-терористички напад:

- Прибирање на информации, односно нивно копирање со цел собирање на значајни разузнавачки податоци за целта;
- Менување на податоци. По упадот во системот податоците може да се бришат, додаваат, менуваат и сл;
- Прекинување на текот на информациите, односно негирање на услугите;
- Вметнување на податоци во командно-контролниот систем, и раководење со системот, при што може да му се издаде команда и за уништување.[219]

Со самото навлегување во посакуваниот систем, односно пробивање на пасвордите и заштитните станици, најголемиот дел е завршен, останува само директната команда за видот на нападот. Зошто велам најголемиот дел, пример: при промана на координати на авион во тек на лет, со самиот упад во системот можат да му бидат сменети координатите, но можеби авионот има заштитен систем со кој во тек на лет не се дозволува промена на координати.

Покрај тоа, постојат различни цели со чиј што напад може да се компромитираат и владини компјутери, како и големите бази на податоци

[219] Ibid, стр. 15-17

полни со приватни информации за поединци, авиокомпании, банки итн.[220]

Како најчести мети, односно најатрактивни можни дестинации за напад од страна на сајбер-терористите, експертите ги посочуваат полициските станици, владини објекти, воени објекти, брани и водоводни системи, комуникациите, енегетските постројки и нафтата, сообраќајната мрежа (особено авионскиот и железничкиот сообраќај), банките и трансакциските сметки, интернетот и др. и се изнаоѓаат начини на ваквите критични инфраструктури да се зголеми заштитата, така што би биле помалку ранливи од сајбер-терористички напади, или пак воопшто да не можат да се пробијат. Така како можни мерки кои се преземаат се: повеќе пасворди за една операција и менување на пасвордите почесто, поголема крипто заштита, снимањето и копирање на програмите на повеќе места, подобри антивирусни програми, појаки софтвери, поголема контрола на вработениот персонал да не можат да бидат врбувани како инсајдери.

Освен тоа што, за извршување на еден напад на сајбер-терористот не му е потребна војска како кај традиционалниот тероризам, ниту кампови за обука, ниту еден тон експлозив, туку минимални средства т.е само еден компјутер, е причината кон прибегнување и се поголемата инвазија и примена на сајбер-тероризмот како атрактивна опција за терористите, но исто така како незанемарлив е фактот дека според безграничноста на сајбер-просторот што го нуди кој е агеографски, и според местот и брзината на пренос на информации, според покриеноста на мрежата на целата планета, најчесто нападите се вршат од една земја во друга, од една страна на светот на друга, со тоа шансите да се открие сторителот се многу мали, па затоа за сајбер-тероризам до сега никој не е осуден, а и многу се мали шансите да се открие вистинскиот сторител.

Исто така што е доста битно да се спомене, и што го прави компјутерот и интернетот незаменлив и ексклузивен е тоа што информацијата се пренесува од виртуелен во реален свет, од виртуелен во виртуелен свет, или од реален во виртуелен при што е многу тешко да се следи и да се има потполна контрола врз неа.

Во однос на местот на извршување можеме да зборуваме за:[221]

- Физичко место – физичко опкружување каде што постојат физички докази[222] за кривично дело или инцидент[223] и тоа:
  - Примарно физичко место – на пример просторија со компјутер од кој осомниченият напаѓач го извршил нападот

---

[220]Stagnetto-Sarmiento, C., Critical Infrastructures and Cyber terrorism, Oglala Lakota College, USA SEPTEMBER 16, 2010

[221]Pollit, M. M., Report on Digital Evidence, (Izvestaj FBI CART, DC Washington, USA), 13th Interpol Forensic Science Symposium, Lyon, France, 16-19. 10. 2001, стр. 89

[222] Примери за физички доказ кај компјутерскиот криминал се компјутерот, хард дискот, ЦД-РОМ и сл, кои содржат дигитални докази за извршено кривично дело од областа на компјутерскиот криминал.

[223] Под компјутерски инцидент се подразбира било која серија на настани кои се разликуваат од логованите стандардни настани во компјутерскиот систем т.н events, и бараат интервенција од страна на посебен тим за истрага на компјутерско-безбедносни инциденти.

- Секундарно физичко место – на пример просторија со посредниот компјутер преку кој напаѓачот го извршил нападот врз компјутерскиот систем – жртва.

➢ Дигитално место на извршување –виртуелно опкружување кое се сосотои од хардвер и сосфтвер каде постојат траги и потенцијални дигитални докази[224]за разјаснување и докажување на настанот како кривично дело или како инцидент.

И големите сили веќе гледаат на сајбер-тероризмот како на глобална закана од светски рамки , на кој времето допрва следи. Најголема предност на сајбер-тероризмот е моментот на изненадување. Времето на напад е избрано од страна на противникот и тоа најчестесто се реализира за време на критични периоди или специфични настани, нападите се прикриени, а местото на од каде ќе се изврши нападот најчесто и никогаш нема да биде откриено, или доколку биде откриено тоа ќе биде илјадници километри подалеку од местото на целта, што значи дека шансите за фаќање на сторителот се минимални.

9.4.1. Профил на сторителот на сајбер – терористички напад

Како понова гранка на тероризмот, сајбер – тероризмот првите чекори т.е начин на дејствување го учи од постариот модел на терористи и најчесто употребуван во пракса терористи – самоубијци.

Профилите на терористите за време на студената војна според Чарлс Расел и Бауман Милер (Russell, Charles A., And Bowman H.Miller, 1979)[225]се поопширно елаборирани во нивните студии поврзани со тероризмот.

Тие се обидуваат да насликаат социјален портрет или профил на модерен и урбан терорист, што се базира врз компилација и анализа на повеќе од 350 индивидуални терористички кадри и лидери на аргентинските, бразилските, германските, иранските, ирските, јапонските, палестинските, турските и др. терористички организации активни во периодот од 1966 до 1976 година(првата декада на современата терористичка ера).

Според нив терористите, главно се самци, мажи на возраст од 22-24 години кои имаат некакво повисоко образование, ако не и универзитетска диплома.

Жените терористи, (со определени исклучоци)се повеќе преокупирани со давање подршка отколку со оперативни улоги. Повеќето од нив имаат анархистичко или марксистичко гледање на светот и се регрутирани додека биле на универзитет.

---

[224] Под дигитален доказ се подразбира дигитален податок кој може да потврди дека е извршен компјутерски криминал, и кој може да ги доведе во врска настанот и сторителот. Примери за дигитален доказ се дигитални податоци во меморијата, во хард-дискот, или на мобилниот телефон кој укажува на настапот до, и извршените активности на испитуваниот компјутер.

[225]Russell. Charles A., and Bowman H.Miller."Profile of a Terrorist", Terrorizm:An International Journal, 1, No.1 1977, 17-34

Иако, денес, нивниот модел е застарен, со невалиден методолошки пристап и неверодостоен, сепак може да се искористи како основен водич за изведување некои воопштувања во врска со типичните лични карактеристики на терористите, во комбинација со други информации.

Едгарс О'Баланс (*Edgar* O'Ballance, 1979)[226]ги посочува следните најбитни карактеристики на „успешниот" терорист: посветеност, вклучувајќи го атрибутот на апсолутна послушност кон лидерот на движењето; лична храброст, немање чувство на жал или сожалување или грижа на совест, дури и кога жртвите се невини мажи, жени или деца; прилично висок степен на интелегенција, бидејќи терористот мора да собира и анализира информации, да замислува и имплементира сложени планови и да ги избегнува полициските и безбедносните сили; прилично висок степен на "софистицираност" со цел да може да лета во прва класа на авионите, да престојува во хотели од висока класа и незабележано-ненаметливо да се замеша во меѓународниот џет-сет (елита), да биде од солидна образовна установа и да има прилично општи познавања (универзитетска диплома е речиси задолжителна), вклучувалќи и зборување на англиски јазик и уште еден од другите светски јазици.

Според сознанијата на Расел и Милер, околу 2/3 од членовите на терорстичките групи имаат определена форма на универзитетско образование.

Занимањата на терористичките регрути доста се разликуваат и нема ниедно посебно занимање кое „продуцира" терористи, освен од редот на невработените и студентите.Универзитетските центри насекаде во „терористичките зони" беа расадници-плодна почва за регрутирање нови терористи. На високообразованите регрити, нормално, им беа давани водечки места на ниво на ќелија или на национално ниво.

Занимањето на терористичките водачичесто беа од рангот на лекари, банкари, адвокати, инженери, новинари, универзитетски професори и владини службеници.

Многу од нив, кои биле во состојба да останат анонимни најверојатно продолжуваат да ги извршуваат своите легитимни професии. Тие се јавуваат во улога на терористи само тогаш кога ќе се добијат инструкции да спроведат определена терористичка мисија.

Поради тоа тие се способни да употребуваат разновидно оружје, превозни средства (вклучувајќи и авиони) и најсовремена опрема за комуникации и информатичка технологија.

За да биде сликата за терористите уште појасна, ќе потенцираме една листа од девет психолошки карактеристики, првенствено карактеристични и заеднички за десничарските терористи, кои во определена поголема или помала мерка може да се проектираат и за некои други категории терористи:

Нивниот „психолошки профил" е „збогатен" со следните карактеристики:

- Амбивалентност со власта;
- Сиромашна и дефектна внатрешност;

---

[226]O'BALANCE, Edgar, "The Language of Violence: The blood Politics of Terrorizm", San Rafael, California: Presidio Press, 1979.

- Приврзаност и следење на конвенционалните модели на однесување;
- Емоционална издвоеност од последиците од нивното дејствување;
- Нарушување во сексуалниот идентитет со функционална несигурност;
- Суеверие, магија и стереотипно размислување;
- Етеро и самоуништување;
- Ниско ниво на образовни референци;
- Перципирање на оружјето како фетиш и субкултура за следење (прифаќање) определени форми на насилство.[227]

Продукт на овие психолошки карактеристики е „личноста на авторитарен екстремист". За таа цел, голем број теоретичари сметаат дека во десно ориентираниот тероризам индивидуите се психопатолошки личности без идеологија, односно нивната идеологија е празна: идеологијата е надвор од реалноста и терористите истовремено се и повеќе нормални и пофанатични.

Од тука согледувајќи ги профилите на терористите, нивните психофизички, идеолошки и интелектуални способности ќе кажеме дека се работи за луѓе кои се спремни се да направат за својата организација не жалејќи го ни сопствениот живот, а посебно што се интелектуалци па дури и универзитетски професори, никој не се сомнева во нив, од една страна и држејќи такви позиции се столбови за регрутирање и обука на идните истомисленици.

Кога се работи пак за профил на сајбер-терористи ќе потенцирам дека важат сите досегашни согледувања само ќе додадам дека секој терорист не може да биде сајбер-терорист туку треба да има посебни знаења од информатичко-комуникациската технологија, добар програмер па затоа и се регрутираат луѓе со такви капацитети т.е од универзитети за информатички и комуникациски науки каде не им се потребни ни експлозиви, ниту поголема група на луѓе со бомби и автомати туку само еден сајбер-терорист и еден компјутер со кој може да им се зададе тежок удар на владите и на безбедносните сили.

Актерите кои се јавуваат во улога на директни извршители на различни активности во информатичко-комуникацискиот систем, можат да бидат индивидуалци, групи, па дури и државни актери. Индивидуите можат да бидат извршители на одредени сајбер-терористички акции за своја сметка без никакви побуди кои најчесто се врши од предизвик, љубопитност, покажување на храброст и вештини, исто така групи или терористички организации се најголемите можни сторители на ваков вид на криминал, најчесто од политички побуди за промена на власта или за некои други свои уредувања (верски, идеолошки, соијални итн), а не е исклучена и можноста за атак во сајбер-просторот на една држава против друга што има за цел загрозувањена националната безбедност, пример: нападот на системите на

[227] Котовчевски, Митко „Борба против тероризмот" – Скопје, Македонска цивилизација, 2004, стр. 37.

сите витални институции на Естонија 2007 и загрозување на националната безбедност). Постојат голем број на актери во сајбер-просторот, кои можат да се послужат со сајбер-терор:

- *Актери спонзорирани од страна на држави* – одредени држави отворено превземаат одбрамбени но и напаѓачки информатички операции, а ваквите активности вклучуваат: доктрини, едукација, тренинг, организации, ресурси, лаборатории и персонал;[228]

- *Актери кои не се спонзорирани од страна на држави* –има држави кои воопшто не преземаат вакви или слични напади, но има и држави кои за нивна сметка други се јавуваат извршители на сајбер-напади, но тие ги поркнуваат таквите врски со други терористички организации;

- *Суб–државни актери* – во оваа категорија влегуваат сите можни облици на загрозување на безбедноста на граѓаните а не се подржани односно директно не зависат од државни интереси како на примерразни терористички групи, религиозни групи и политички партии. Најголема опасност за можни терористички и сајбер-терористички напади;

- *Хакери*–извршуваат најразлични видови на компјутерски криминал, за своја сметка, а можат да бидат и врбувани од други;

- *Инсајдери*–'актери од внатре'–станува збор за лица кои се подолг временски период вработени и кои се добро запознаени со информационите системи, и кои се главни кандидати за "најмување" од страна на напаѓачите. Како одлични потенцијални регрути, се покажуваат оние вработени кои имаат слични сваќања или погледи во врска со каузата на терористичките групи.[229]

Сите горенаведени се во улога на потенцијални извршители на терористички напади, некои за материјална корист, други од идеолошки побуди или пак друга корист, но сепак без разлика од какви побуди се работи тие се жртвите кои го имаат оној краен завршен ефект позади кои се кријат големите умови т.е организациите кои ги врбувале или за сметка на нечии влади.

---

[228]Kulesza, J., State responsibility for acts of cyber-terrorism, GigaNet Symposium, Vilnius, September 13, 2010

[229]Ashley, B., K., Anatomy of Cyberterrorism: Is America vulnerable? Air war College, Maxwell AFB, AL, Feb 2003, стр.10-11

9.4.1.1.Профилирање на сајбер – терористот

Кои се сајбер-терористите, Каде и Зошто дејствуваат, кои се нивните мотиви и цели? Невидливиот непријател вооружен единствено со лап-топ, конектиран на глобалната компјутерска мрежа, вооружен со огромно човечко знаење трансформирано во дигитален код, кој одлучува со огромна деструктивна енергија и огнена желба да ги оствари своите мрачни цели, впловува во напад со тешко препознатлив правец, но со единствена цел: електронски атак врз државната информациска мрежа од огромно стратегиско значење за несметано функционирање на сите витални општествени функции.[230]

Сајбер-терористите се добро обучени информациско-комуникациски експерти кои со неовластеното навлегување во компјутерските системи вршат напади на институциите на ситемот на целта, која им е таргетирана со цел да предизвикаат штета, уништување, напад, да заплашат, да изнудат и сл. Себеси се гледаат и доживуваат не само како невини за било каков криминал, туку до одреден степен, на својата активност гледаат како на нешто праведно, нешто со што им се спротивставуваат на мрачните режими на нивните влади. Тие се убедени дека со своите активности и не предизвикуваат никакви штети, туку напротив прават добри дела.

Сајбер-терористите не треба да ги споредуваме со другите лица на терористи, кои се обучуваат и по неколку години по импровизирани кампови , задоени со крв од мали нозе, кои имаат за цел да убијат, масакрираат, дигнат во воздух и уништат што поголем дел од целта, затоа што сајбер-терористот како врвен познавач на компјутерската проблематика или талент може и да не знае дека со упад и пробивање на заштитните системи на некоја централа или болница, директно извршува сајбер-терористички напад, за нечија сметка и цел, иако тој е директен извршител.

Така да, како луѓе што најчесто им задаваат удар, и ги напаѓаат виталните институциски системи се јавуваат хакерите на кои како предизвик им е, да се пробие заштитата на одреден информатички систем и да се навлезе во него, со тоа што колку е заштитата посилна, толку е предизвикот поголем.[231] Најчесто ваквите напади на почетокот хакерите ги прават за докажување, од предизвик, од забава, но подоцна таа забава намерно или ненамерно предизвикана претставува општествен проблем.

Типови на хакери како можни извршители на криминал од ваков вид најчесто се :

- *Хакери од старата школа* – професионалци со долгогодишно искуство;
- *Инсајдери* – лица кои се вработени, експерти од областа на својата дејност, но се разочарани од управувањето или функционирањето на организацијата, или поранешни вработени, кои знаат за безбедносните пропусти.

---

[230] Котовчевски, М., Современ тероризам, Македонска цивилизација-Скопје, 2003, стр. 251.

[231] Како најчести мети за вакви напади се воените и разузнавачките компјутерски системи, и системите на други државни институции.

- *Професионални криминалци и сајбер*-терористи –тука спаѓаат поранешните разузнавачи и школувани сајбер-терористи, кои се добро запознаени и обучени да изведат акција од ваков вид.

Меѓутоа, токму хакерите т.е познавачите односно талентите за компјутери се целна група на терористите за регрутирање во своите редови и извршување на зададените задачи за кои во поголем број случаи самите извршители на задачите и незнаат за какви цели ги извршуваат задачите и кои се крајните резултати односно жртви.

Не секој хакер што е приврзан до некоја терористичка организација мора да биде вклучен во секоја акција, што ја спремаат терористите или па не мора да значи доколку се има план за напад на одредена постројка да се делува од надвор, туку како пооптимална и подобра опција ќе биде да се врбува човек од внатре 'инсајдер', кој е запознаен со работата на системот, со шифрите, и само треба да се одреди време на извршување т.е не следи никаква претходна подготовка со месеци или со години па да дојде до откривање на планираниот напад или поголем финансиски трошок за организацијата.

Таквата транзиција од хакери во сајбер-терористи е мотивирана од финансиски придобивки или углед, но најчесто ваквата промена односно транзицијасе случува како што кажав без самите да знаат и ги продаваат своите информации, анонимно преку тајни мрежи.[232]

Терористите постојано преку своите тајни мрежи или веб-страници врбуваат свежи мозоци кои се во тренд со времето и технологијата, а особено добро ќе им дојде и школувани кадри на некој од престижните универзитети кои паралелно извршувајќи си ги своите должности, од различни побуди или интереси ги продаваат своите знаења и вештини, најчесто од политички побуди да се наштети на некоја влада, со цел да се смени политиката што ја водат или раководството, но и финансискиот фактор е исто така битна алка во системот, што сајбер-терористот подоцна воопшто не го интерирсира исходот од таквите зло-намери.

Заедничко во филозофијата и на едните и на другите е нивната определба кон примена на асиметрични средства за постигнување на нивните цели.

За терористичките организации преземањето на активности од типот на сајбер-тероризам и врбување на сајбер-терористи им е од особено значење, бидејќи како што кажав не бара големи средства, не треба поголем период за обука, па затоа во последно време се повеќе се посветува внимание на сајбер-тероризмот и претставува атрактивна опција на терористите, не занемарлив е и фактот што исто така многу им одговара е асиметричноста во војувањето, со добро опремен и обучен сајбер-терорист можеш да војуваш и преговараш со цела држава.

Сајбер-терористот е, и секогаш ќе биде еден чекор пред оние задолжени за негово откривање и спречување. Не постоењето начин да се контролира интернетот и информациите за новите методи и алатки за напад кои се шират

---

[232]Francis, B., Know Thy Hacker, Infoworld, January 28, 2005, достапно на http://www.infoworld.com/d/security-central/know-thy-hacker-534.

меѓу хакерите ширум светот им го овозможува тоа. Иако можеме да ги корегираме повеќето слабости во компјутерските системи, едноставно не е можно да се елиминираат сите.[233]

Освен финансиските средства, или моќта како мотиви за пристапување во терористички организации, во најголем дел се јавуваат политичките, економските, социјалните како и верските побуди кои се многу поопасни од оние со финансиски побуди, бидејќи тие се опиени со таквата идеологија, па и со цена на живот не отстапуваат од тој идеал.

Мотивите за сајбер-напад, вариpаат и се движат од сеење на страв или паника, заплашување, принудување, освета, влијание, моќ, одмазда, рушење на довербата на јавноста во властите, ширење на одредена идеологија (политичка или религиозна) или истовремено постигнување на повеќе ефекти.

Тоа се истите мотиви со кои се користат и традиционалните терористи што вршат физички напад, но во сајбер-светот останува и дилемата дасе открие кој го врши нападот (индивидуалец, група, државата), и да се разбере зошто. Најчесто, финансиските удари, откупот, нарушување и намалување на воената моќ, стравот, паниката, публицитетот и медиумското влијание, намалување на довербата во критичните инфраструктури, психолошкиот терор, огромната материјална штета или загуба на човечки животи, се очигледните цели кон кои се стремат терористите.[234]

Во литературата се среќаваат повеќе примери за тоа, што придонесува и ги поттикнува луѓето да пристапат и да преземаат сајбер-терористички акции:

1. Кога оние кои се на власт, немаат слух;
2. Економски, социјални и други неправди;
3. Кога не постои друг излез;
4. Промена на политичкото уредување;
5. Атак на една држава против друга (и државите можат да бидат терористи)
6. Кога владата на една земја сака да оствари влијание врз владата на друга.

Но, не е доволно да гледаме само на факторите на опкружувањето односно средината како на фактори кои придонесуваат поединци да гледаат на тероризмот како на ефективен метод за постигнување на нивните цели.

Секако дека постојат и голем број други фактори кои се среќаваат односно се користат како мотивација на сајбер-терористите - неправда извршена од страна на државата, репресија од страна на властите, несоодветен одговор од страна на власта кон одредена тема, угнетување на одредена група луѓе итн.

Но, во никој случај не треба да се допушти ниту да се толерира

---

[233]Jachowicz, L., How to prevent and fight international and domestic CYBERTERRORISM AND CYBERHOOLIGANIZAM, Collegium Civitas, Foreign Policy of the Unitet State of America, Warshaw, January 2003, стр. 2

[234]Ashley, B., K., Anatomy of Cyberterrorism: Is America vulnerable? Air war College, Maxwell AFB, AL, Feb 2003, стр. 22

насилство или остварување на свое право на одредени народи или групи луѓе по пат на тероризам, без разлика од кој вид се работи, а нормално дека во светот има милиони незадоволни луѓе кои живеат под владин режим без право на глас, угнетувани без загарантирани основни човекови слободи, или пак друга држава загрозена од некоја трета, па сепак овие земји не се здружиле со терористите.

Дел од експертите сметаат дека сајбер-тероризмот, по начинот и природата на своето дејствување е помалку опасен од традиционалниот начин на војување, со тоа што дејствува од виртуелен во реален свет, па така што помалку била опасноста од него.

Тоа е мислење само на дел од експертите, според мене како што традиционалните облици на тероризам се сметаат за тежок облик на криминал, и загрозување на националната безбедноста, така и на тероризмот во сајбер просторот треба да се гледа на помалку тежок облик на криминал, бидејќи сменета е само средината на делување (од физичка во виртуелна), но последиците и ефектите се видливи во реалниот свет.

Со оглед на тоа дека во литетатурата постојат многу малку податоци кои го карактеризираат присуството или однесувањето на сајбер-терористите, останува прашањето дали сајбер-терористот е вистински или само теоретски тип на непријател. Ние ќе тргнеме од ставот дека сајбер-терористот е многу реална потенцијална закана по модерните информатички системи. Затоа ќе се обидеме да го моделираме непријателот наречен сајбер-терорист, тргнувајќи од следните претпоставки:[235]

- *Ресурси*

Сајбер-терористите како основно средство т.е. алатка за работа го имаат компјутерот, кој што колку е подобро опремен толку ќе овозможи подобар и побрз пристап до сите информации кои им се потребни :

- ✓ Изработувачи на софтвер, мрежни програми и сл, за изработка на сопствени алатки за напад.
- ✓ Консултантски услуги и други комерцијални јавно достапни експертизи,
- ✓ Сите јавно достапни информации – на телевизија, новини, интернет,
- ✓ Комерцијално достапни технологии како хардвер, софтвер и сл мрежи.

Што се однесува до финансиски средства како ресурс тие им се ограничени, но од друга страна, тие се способни да прибават огромно финансиски средства, кои ќе ги потрошат за спроведување на зацртаната мисија.

---

[235]Schudel, G., Wood, B., Modeling Behavior of the Cyber-Terrorist, Information Assurance Program Integration Team GTE/BBN Tehnologies, Washington, стр. 2

➢ *Ниво на софистицираност*

Сајбер-терористот според нивото на софистицираност (знаење, обука, вештина, брзина), се наоѓа некаде на рамниште на добро обучен хакер, инсајдер или високо образовен кадар од информацискатa проблематика кој во редовите на терористите ќе послужи како добар сајбер-терорист.

➢ *Разузнавање*

Се претпоставува дека сајбер-терористот може да дојде до потребните информациите за системот цел и тоа:

- ✓ Преку јавните гласила телевизија, интернет, новини и сл,
- ✓ Слаба заштита на информациите кои не са јавни,
- ✓ До информациите кои се контролирани и заштитени, може да се дојде по пат на изнуда или поткуп.

➢ *Специфични таргет – цели*

При изборот на целта, се бара начин како да се изврши зададената задача без непотребно напаѓање на целиот систем, туку точно конкретен систем или сегмент од него, за да не се губат непотребно време и средства и ставање во ризик. Пр: (нема потреба да се учи полетување со авион ако се планира да се преземе во воздух).

➢ *Избегнување на ризик*

Сајбер-терористот ќе се одлучи за реализација на нападот, само тогаш кога ќе оцени дека тоа е погодно време за негово спроведување, се што ќе се преземе на своја рака или недоволно осмислено ги зголемува шансите за негово откривање и ќе ги загрози другите соработници.

Нападите на сајбер-терористите се брзи, добро прикриени, па дури се вршат и надвор од државата да би се анулирала можноста за нивно, откривање. Доколку се појави и најмал ризик при спроведување на нападот, нападот нема да се реализира.

9.4.2. Криминалистичко – виктимолошки карактеристики

Самото дело предизвикано со некој терористички акт, доколку има за цел предизвикување општа опасност, голема материјална штета, загрозување на безбедноста на луѓето и посегнување по нивниот живот, придобивање на материјална корист и др. претставува кривично дело.

За да биде прогласен некој акт како кривично дело треба да има сторител, жртва и деликт. Сајбер-терористот со преземање на некоја активност против друго лице или институција се јавува како сторител на тоа дело, а како жртви се јавуваат корисниците на информационо телекомуникациските системи (ИКТ), т.е инфраструктурните објекти кои се од витално значење за опстанокот и развојот на секое современо општество.

Така да на опасност од вакви напади се изложени сите корисници на информатичкатакомпјутерска инфраструктура, од обичните граѓани до организациите, владините институции и безбедносни системи – до општествата како целина предупредуваат експертите.[236]

Како и традиционалниот тип на терористички акции, така и сајбер-тероризмот не е насочен само кон одредена единка која би се нашла како непосредна случајна жртва, туку е насочен кон предизвикување на чувство на страв и несигурност кон поширока група на луѓе, која е таргетирана при одреден напад.

При изборот на жртви и објекти за напад терористите подолго време собираат разузнавачки податоци и добро осмислуваат која категорија на луѓе да биде опфатена при одреден напад, ништо не се презима и остава на случајност што е една од најзначајните карактеристики на тероризмот воопшто, со што се стекнува впечаток дека и не постојат објекти и жртви кои не би можеле да бидат мета на терористички напад.

Општо земено, терористичките мети би можеле да ги поделиме на :

- Напади врз луѓе:
  - Претседатели на држави, дипломати, политичари, воени лица, успешни научници, случајни групи на луѓе (луѓе во метроа, патници во авиони, автобуси, луѓе на плоштади и др јавни места).
- Напади врз објекти:
  - Амбасади, училишта, владини згради, полициски станици, научни објекти и институции, фабрики, туристички објекти, постројки и др.[237]

Кога се зборува конкретно за сајбер-терористички напади, веднаш се знае дека тие се насочени кон информациско-комуникациските системи односно нападот е извршен со помош на нив, а се насочени кон критичните инфраструктури.

Нападите обично се насочени кон цивилни цели бидејќи во споредба со воените цели се послабо заштитени, и со таков напад се создава поголема несигурност и паника кај населението, бидејќи нема дом, што нема барем по еден компјутер и нема институција што на било кој начин не врши пренос на информации со помош на него. Поткрепено пак со што поголема еуфорија во мас-медиумите уште повеќе им оди во прилог на терористите, но не значи дека воените објекти се изменети и дека во иднина нема да биде нападната некоја воена база или лансирна рампа.

---

[236] Преземено од: Компјутерскиот тероризам нова закана, Радио Слободна Европа достапно на http://www.makdenes.org/content/article/24390898.html

[237] Кеча, Р., ТЕРОРИЗАМ – Глобална безбедносна пријетња – Европски дефендологија центар за научна, политичка, економска, социјална, безбједносна, социолошка и криминолошка истраживања, Бања Лука, 2012, стр. 3

9.5 Сајбер-тероризмот како атрактивна опција за терористите

Бидејќи за извршување на одредена акција не се потребни голема група на луѓе, без никакво оружје, без посебни тренинг центри и непотребни жртви од страна на терористите, а во исто време низок степен од ризик на откривање сајбер-тероризмот се повеќе и повеќе е по атрактивна опција за терористите:

1) Сајбер-тероризмот, по својата природа е без голем ризик за откривање (поанонимен метод), за разлика од класичните терористички методи. Како и сите останати корисниците на интернетот, и сајбер-терористите се логираат на одредени веб-страници, но со лажни кориснички имиња, со што го прават многу тешко откривањето и следењето на нивните вистински идентитети од страна на безбедносните служби. А бидејќи во сајбер-просторот не постојат физички и просторни бариери, што значи дека на интернет секој со секого може да се поврзе и да разговара без посебни проверки на идентитетот.

2) Милиони можни комбинации за напади и цели. Сајбер-терористот како цели може да ги земе информационите системи и мрежи на болници, банки, влади, авио компании, поединци, и сл при што ќе бараат слабости и ранливости во тие системи, со цел да ги нападнат и уништат.

3) Станува збор за метод, кој е многу поефтин за разлика од традиционалните терористички методи. Се што му треба на еден сајбер-терорист е компјутер, интернет конекција и доволно познавање на информатичката технологија. На овие терористите не им се потребни бомби и автомати, туку наместо нив ќе бомбардираат со компјутерски вируси.[238]

4) Голема предност на сајбер-тероризмот е што терористичките акти можат да се вршат од еден на друг крај на светот, и да бидат управувани од далечина, што е од голема корист за терористите. Така да ризикот за нивно откривање и фаќање е многу минимален.

5) Сајбер-тероризмот, со мултимедијалниот пристап и големиот број на корисници ширум светот (милијарда луѓе) постигнува голем ефект, генерира страв, психолошки делува и повлекува медиумско покривање што им е и прва цел на терористите.

---

[238] Jeong-Tae, K., Tchanghee., Status and Requirements of Counter-Cyberterrorism, World Academy of Science, Engineering and Technology, 6, 2005, стр. 31

6) Најголем проблем претставува откривање на сторителите на сајбер-терористичките напади, кој според безграничноста и непостоењето на никакви бариери и (просторни и временски), претставува невидлив непријател, а и доколку се детектира тој веќе одамна заминал од местото на извршување. Во најголем број случаи остануваат неоткриени и неказнети, што им влева уште поголема самодоверба и мотив.

Целиот проток на информации буквално во општеството на денешнината оди преку телекомункацискиот систем, така да доколку терористите успеат успешно да спроведат сајбер-напад врз институциите на системот, целата држава ќе биде во колапс, а со тоа ќе падне и способноста на државата да се бори со криминалот и со тероризмот.

Оштетувањето или онеспособувањето на таквите мрежи, значи не еден, туку многу повеќе поени на сметката на терористичките организации.

Тоа беа предностите на сајбер-тероризмот во однос на другите видови на тероризам и затоа се повеќе терористите се стремат кон овој вид на тероризам.

Меѓутоа сигурно има и свои недостатоци така што доколку не би имало кај би му бил крај на светот, ако е толку лесно во пракса се тоа да се изведе без никакви препреки и потешкотии.

Како недостатоци би ги навел:

- Потребна е опрема за изведување на нападот (компјутер и интернет конекција), регрутирање и обука на нови терористи со познавање од областа на информатиката, потребно е одредено време за обезбедување пристап и информации, посложени за сервис и одржување, потежок пристап до владини и воени лозинки (поради почеста промена на корисничко име на истите од страна на владините служби), помал емоционален ефект, можност за следење и прекинување.

Само да истакнам дека сајбер-тероризмот не само што е алтернативна можност за терористите за во иднина, туку веќе со своите огромно предности, така што во однос на нив недостатоците дури се занемарливи, сајбер-тероризмот на голема врата влегува како глобална закана на 21- от век во светот, особено за генерациите што следат, кои растат со компјутерите и од мали нозе ги совладуваат компјутерските вештини.

9.6. Case study – сајбер напад врз информациско-комуникациската инфраструктура на Естонија

Естонскиот случај претставува еден од најголемите кои некогаш се случиле во историјата. Овој случај вклучува серија на сајбер напади кои започнале на 27-ми април 2007 година. Во тој период, Естонија е рангирана како 23-та земја во светот на е-спремност, каде 61% од популацијата има on-line пристап до своите банкарски сметки, а 95% од банкарските трансакции се водат по електронски пат.[239]

Во април 2007 година, се извршени напади врз информациско-комуникациските системи на Естонскиот парламент, во банките, владата, медиумите, всушност, во сите значајни државни институции при што предизвикале дестабилизација на државната безбедност,[240] кои од страна на мноштво експерти беа окарактеризирани како пример за сајбер-тероризам.

Нападот се случил во време на затегнати односи, после една дипломатска расправија помеѓу Естонија и Русија за дислоцирање на споменик на непознат Русин, кој загинал во борбата против нацистите, кога новинарите од Естонија во медиумските извештаи ја обвиниле Руската влада за отпочнување на нападот,[241]поточно во април кога и започнале серија на компјутерски напади врз неколку естонски веб-страници, вклучувајќи ги сајтот на Владата на Естонија, неколку министерства и на владеачката Реформска партија.

Нападот отпочнал со преблокирање на Естонските владините веб-страници кои вообичаено имале околу 1000 посети дневно, одеднаш започнале да примаат по 2000 посети секоја секунда. Ова според официјалните изјави на Естонските власти, предизвикало замрзнување и пад на веб-страниците по неколку часови, понекогаш и подолго. Но, некои од експертите, тврдат дека ваквите напади против Естонија се по малку чудни, бидејќи траеле многу подолго од вообичаеното.[242]По бранот на напади врз виталните институции на Естонија, НАТО и САД испратиле свои компјутерски експерти за да и помогнат на земјата да закрепне од нападите, какао и да ги утврдат можните мотиви и сторителите на овој сајбер-напад.

Бидејќи Русија и Естонија во тој период имаа заладени односи и недоразбирања и околу некои други прашања, Естонската влада ја посочи Русија како можен сторител на сајбер-нападите или пак како нарачател на транснационални сајбер криминалци за користење на нивни услуги.

По спроведените истраги ниту НАТО, ниту експертите на Европската комисија не успеале да докажат и да најдат докази за вмешаност на руските службеници во тие напади, туку дека се производ на спонтан гнев од слаб сојуз на повеќе поединечни напаѓачи, а на таквиот заклучок укажале техничките податоци, според кои изворите на напад биле распространети

---

[239]Buckland, S., B., Schreier, F., Winkler, H., T., Demokratsko upravljanje izazovi sajber bezbednosti, Forum za bezbednost I demokratiju, Beograd, Srbija, 2010, стр. 26

[240] Надица Мирчевска, научен труд сајбер-тероризам – современ облик на тероризмот колку Република македонија е ранлива од сајбер тероризам

[241]Cyber terrorism: The World's First Internet War?: Stefan Nicola, August 8, 2007, http://www.govtech.com/dc/articles/12966,

[242]Marsan, C., Examining the Reality of Cyberwar inWake of Estonian Attacks, Network World, August 27, 2007, vol. 24, no. 33, стр. 24

ширум светот, а не сконцентрирани на неколку локации. Со ова се елиминираше вмешаноста на Руската влада во нападите врз Естонија, што го потврди и Министерот за одбрана на Естонија Џек Авиксо.[243]

Овој настан ни покажува за постоечкиот проблем кој се јавува при, и после секој сајбер-напад, а тоа е прецизната идентификација на напаѓачот, преку откривање дали се работи за напад спонзориран од некоја држава, или е независна активност на неколкумина меѓусебно поврзани институции.

Ваквиот вид на напад сепак не претставува напад од тој вид да има огромни последици и загуби, голема материјална штета или човечки жртви. Но тоа е првиот напад од такви размери да се бликираат сите витални институциина државата, со што целиот систем, па и државата се во колапс. Многу пострашен исход би имал нападот кој би се состоел од навлегување во естонските компјутери и бази на податоци на здравствени или криминални евиденции, исчезнување на банкарски сметки и сл.[244]

9.6.1.Грузискиот конфликт 2008[245]

Како прв комбиниран напад на сајбер-напад и воена офанзива се бележи нападот врз Грузија.DDoS - напади[246]од мали размери (напади со дистрибуиран прекин на услугите) врз грузиската интернет инфраструктура, биле регистрирани во јуни, скоро два месеци пред петодневната војна помеѓу Русија и Грузија, по прашањето за Јужна Осетија.

Војната не само со директно учество на фронт на двете завојувани страни, туку првин претходеше сајбер-напад на владините сајтови и на некои други позначајни комуникациски портали и медии слични на оние во Естонија 2007 година, само со помал интензитет. Повторно беше посочена Руската влада за вмешаност и во овој напад. Според некои интернет експерти за безбедност ваквиот сајбер-напад беше очекуван, бидејќи Русија, заедно со Кина и Бразил, се лидери во интернет криминалот.[247]

На 20 јули, фондацијата Shadowserver, група чувари на интернет, приметиле повеќе DDoS напади насочени кон официјалната веб-страница на Грузијскиот претседател Михаил Сакашвили, кои резултирале со пад на веб-страницата повеќе од 24 часа. Утврдено било дека нападот бил координиран преку Американски сервери, факт кој ја нагласува безграничната природа на оваа закана.

Според New York Times нападите врз Грузиската комуникациска мрежа кулминирале на 8-ми август 2008 година, првиот ден од војувањето, кога биле регистрирани напади на веб-страниците на владата и медиумите. Како се

---

[243]Estonia has no evidence of Kremlin invlment in cyber attacks, Ria Novosti, 2008, http://en.rian.ru/world/20070906/76959190.html,

[244]Lewis, J., Cyber Attacks Explained, June 15, 2007, преземено од http://www.csis.org/tech/070615 cyber attacks.pdf,

[245]Buckland, S., B., Schreier, F., Winkler, H., T., Demokratsko upravljanje izazovi sajber bezbednosti, Forum za bezbednost I demokratiju, Beograd, Srbija, 2010, стр. 28

[246] Повеќе за ваквите напади во "Explaining Distributed Denial of Service Attacks to Campus Leaders," May 3, 2005, http://www.uoregon.edu/~joe/ddos-exec/ddos-exec.pdf,

[247]*Нова димензија на војни: Битките се преселија од Кавказ до Интернет(on-line), ihnet. Cz.*

заоструваl конфликтот, така ескалирале и on-line нападите кои руските хактивисти ги вршеле над веб-страниците на претседателот, парламентот, министерството за одбрана и надворешни работи, грузиска народна банка и новински агенции. Канцеларијата на Полскиот претседател нуди помош со свои експерти за опоравање од сајбер-нападот и отргнување на блокадата.[248]

Владата на Грузија сепак, не чекала ситуацијата да ескалира и да дојде до поголеми блокади на системот, туку веднаш побарала помош од другите земји, кои испратиле свои експерти за справување со сајбер-нападот и зајакнување на својата сајбер-одбрана.

Експертот за дигитална активност на Белорусија, Евгениј Морозов посочува дека координацијата на нападите била воглавно спроведена преку on-line хакерскиот форум StopGeorgia.ru, основан само неколку часа откако руските воени сили извршиле инвазија на Јужна Осетија. На овој форум имало константно ажурирана листа на веб-страници – мети, охрабрувајќи ги посетителите да ја преземат бесплатната програма со помош на која можат веднаш да се приклучат на сајбер-нападите.

Грузија од сајбер-нападите претрпе мала штета бидејќи грузиската економија и клучна инфраструктура сеуште не биле интегрирани во е-општество. Сеедно, кампањата водена од страна на националистичките хактивисти, поттикнати на акција со помош на рускиот on-line хакерски форум, ефикасно ја пореметила дистрибуцијата на информации на Владата на Грузија, во клучните моменти на нападот.

9.6.2. Примери за позначајни сајбер – инциденти

Постојат доволно докази на располагање дека терористичките организации активно користат сајбер-простор за спроведување на своите напади. Терористите интернетот освен за напади го користат и за комуникација на едни со други, регрутирање на членови, прибирањена на податоци, подигање пари легално и илегално, илегално добивање на пасоши и визи и дистрибуција на пропаганди. Во литературата се забележуваат само оние позначајни, односно инциденти кои се успешно спроведени напади врз владини агенции, хај-тек компании, банки и сл, кои резултитале со поголема штета.

- *2003 година* – програмски црв Slammer, вметнат е во енергетскиот систем на САД, при што ја успорил контролата на системот што резултирало со тоа осум држави, две Канадски провинции и неколку милиони луѓе да останат без електрична енергија.

- *Ноември, 2006 година* – обид на група хакери да навлезат во мрежите на Воениот колец во САД, кој резултирал со двонеделен прекин на мрежата, додека да се отстранат дефектите.

[248] Cenne Polskye wsparcie DLA GEO (ОНЛАЈН)

- *Пролет, 2007 година* – банки, владини агенции, парламент во Естонија нападнат е како што тврдат Естонците од страна на Русија. Естонија беше во потполн колапс, без интернет и комуникации и се бележи за прв IT рат помеѓу две држави.

- *Август, 2007 година* – германските тајни служби пријавиле сајбер-напади од Кина на неколку германски министерства и владата, со цел да се откријат доверливи информации. При што канцеларката Ангела Меркел отворено потражила од кинеските дипломати за време на нивна посета на Германија со тоа да се прекине.

- *Септември, 2007 година* – Израелци ги нарушиле мрежите на системите за воена одбрана на Сирија (со мала колатерална штета на сопствените домашни мрежи), за време на бомбардирање на наводната Сириска нуклеарна постројка.

- *Септември, 2008 година* – група на хакери кои се нарекуваа "Greek Security Team" предизвикаа глобална паника, упадајќи во системот на CERN (Европски центар за нуклеарни истражувања) толку длабоко да се наоѓале многу блиску до превземање на контрола над еден од детекторите на LHC-а, најголем за акцелерирањена честици. Претставници на CERN, изјавиле дека никаква материјална штета не е причинета, но е незгодно сознанието дека детекторите и целата скапоцена машинерија се подложни на дигитални загрозувања.

- *Август, 2008 година* – напад на веб-порталите на Грузискиот претседател, владата, министерството за одбрана и медиумите, 2 месеци пред воен напад на Русија кон Грузија. Прв комбиниран напад првин со сајбер атак, а подоцна и воен удар.

- *Лето, 2008 година* – базите на податоци на Демократската и Републиканската партија на САД, кои содржеле податоци за претседателските кампањи биле хакирани од страна на непознати странски хакери.

- *Јануари, 2009 година* – хакери ја нападнале интернет инфраструктурата на Израел, при воената офанзива во појасот Газа. Нападот, насочен кон владини веб-страници, бил извршен од страна на најмалку 4 милиони компјутери. Според

Израелските власти, нападот бил нарачан од страна на Хамас или Хезболах,, а извршен од криминална организација од поранешниот Советски Сојуз.

- *Февруари, 2009 година* – Француските воени воздухоплови биле приземјени како резултат на тоа што воените бази на податоци биле заразени со вирусот наречен "confickr", а се претпоставува дека до заразување дошло при користење на заразен USB-уред.

- *Јуни, 2010 година* – голема фама во јавноста привлече Staksnet (*Stuhnet)* – специјално направен малициозен програм со кој се заразени Simensovite SCADA уреди кои ги контролираат нафтоводите, електриката, нуклеарни и други индустриски постројки во Иран, инфицирајќи најмалку 30.000 компјутери ширум земјата. Спрема проценките на експертите, Staksnet е најсофистициран малициозни програм до тогаш направен, и претставува комбинација кој од четири различни страни го напаѓа Windous – оперативниот програм.

- *Март, 2010 година* – НАТО и ЕУ предупредуваат дека бројот на сајбер-напади кон нивните мрежи и системи е значително зголемен во последните 12 месеци, а Русија и Кина се меѓу најактивните напаѓачи.

- *Март, 2011 година* – хакери навлегле во компјутерските системи на Француската влада, со цел да бараат осетливи информации за престојниот самит на G-20 групата.[249]

Со овие примери се докажува се поголемата присутност на сајбер-тероризмот, како опција која се повеќе е прифатена од страна на терористите, која со мали средства се постигнуваат големи резултати, што можеме да видиме и од самите примери што ги наведов. Сакам исто така да посочам дека ниту големите сили не се поштедени од ваквиот вид на терористички напад и војување, туку напротив сајбер-тероризмот особено е насочена против големите сили, каде таа асиметрија на војување ја користат помалите организации или држава за искажување на своите незадоволства, од угнетувањата на западниот свет.

Од наведените примери исто така гледаме дека скоро во сите сајбер-напади во позадина на тој напад стои некоја држава, што значи дека сајбер-тероризмот веќе е прифатен и подржуван од големите сили, што може да се сврсти и во редовите на државен тероризам. Како еден одличен пример на

[249]Lewis, A., J., Cyber Events Since 2006, Significant Cyber Incidents Since 2006, Oct 10, 2011, преземено од http://www.csis.org/publication/cyber-events-2006.

сајбер – напад ќе го споменам нападот врз Естонија која неколку месеци не можеше да се оправи од сјбер-нападот, при што имаше колапс на целиот систем, а што ќе се случеше доколку и воено беше нападната истовремено, без никаква комуникација и целосна блокада на информационите системи ќе беше лесен плен за освојувачите.

Затоа сајбер-тероризмот не беше потценет и големите сили на него гледаат на закана од глобално ниво, чие време допрва доаѓа.

10.Мерки за делување против сајбер-тероризмот

10.1.Општо за мерките за делување против сајбер-тероризмот

Од досега презентираното се уверивме дека интернетот и глобалната информатичка ера покрај своите предности кои им користат на луѓето и го олеснуваат животот, имаат и недостатоци и слабости што со себе носи ризици и слабости. Тој нуди информации и инеракција, што во поголемиот број на случаи се базира на доверба, при што лесно може да се увиди веројатноста од компромитирање и злоупотреба.

Историски гледано, владите го применуваат реактивниот пристаппри изнаоѓањето на решенија за ранливоста и нападите врз сајбер-безбедноста. Таквиот пристап им дава можност на сајбер-терористите за непречено тестирање на своите можности бидејќи заштитните структури немаат превентивен пристап, туку откако ќе се случи напад, се прават анализи и доколку е можно се поправаат 'дупките' и пропустите. Но, не треба да се продолжи со разгледување на индивидуалните случаи на напад, како поединечни, без притоа да се разгледува поголемиот проблем како целина. Ако времето на сајбер-тероризмот е дојдено, дојдено е и времето да се бориме против истот зло, со сите средства што стојат на располагање.

Ефикасноста со справувањето на со криминалот од ваков вид сериозно ќе се доведе во прашање, доколку не се преземат соодветни мерки. Студиите и останатите материјали содржани во рамките на меѓународните организации и асоцијации, како и одговорните национални институции предвидуваат реализација на мерки во рамките на постојаните консултански процеси. Така на пример во рамките на COMCRIME е предвидено:

- Формирање на посебни единици на специјализирана полиција на национално ниво;
- Воспоставување соработка помеѓу правосудните органи, индустријата, организацијата на потрошувачи и телата за заштита на податоци;
- „охрабрување" во создавање на специјализирани продукти кои служат за зголемување на сигурноста на компјутерските системи и мрежи.[250]

Сепак, воспоставувањето на специјализирани единици за откривање, праќење и фаќење претставува вистински чекор во борбата против сајбер-тероризмот. Како пример за работа на такви тела претставува врската помеѓу големите сили и тоа: САД, Велика Британија, Германија, Норвешка, Австрија, Холандија и Ирска во рамките на таканаречената ***Daphne*** програмата и поврзаните провајдери во Европскиот форум. овие програми биле подржани од повеќе експерти и под покровителство на УНЕСКО се состанале во Париз во 1999 година, и дек од договорот бил за воспоставување на конкретна мрежа симболички наречена „електронска кула на стражари",, која би имала потесна соработка со Европол и Интерпол.

Воспоставување на соработката помеѓу правосудните органи, индустријата

[250] Југослав Ачковски и Методија Дојчиновски – скрипта за сигурност на компјутерски системи, компјутерски криминал и компјутерски тероризам, Скопје 2012, стр. 35

и приватните организации и асоцијации посебно е потенцирана во 1997 година, кога во Вашингтон е одржан состанок на министрите за правда и внатрешни работи од земјите членки на Г8, и кога се утврдени 10 точки на Акционен план за борба против сајбер-криминалот меѓу кои посебно место е посветено на соработка во индустрискиот сектор кој произведува и развива компоненти од глобалните мрежи, кај кои треба да применети техничките стандарди за сигурност.

Поефикасна заштита на своите информациско-комуникациски системи и развивање на пософистицирани и пообучени кадри за сајбер-заштита се превентивни мерки кон треба да ги преземат сите земји во борба против сајбер-тероризмот, како и поттикнување на големите и мали фирми кои се занимаваат со тоа,т.е ранливите категории на можни институции за напад истото да го преземат.

Како и да е, јасно е дека, признавањето дека сајбер-тероризмот постои, реална сакана е по безбедноста на луѓето и потребно е изнаоѓање на решение за заштита од тоа зло.[251] Потполно елиминирање на ризиците од сајбер-тероризмот не е можно, но можно и реално е минимизирањето на ризиците.[252] Како безбедносен одговор, владите можат да дејствуваат реактивно и проактивно.

Особено што е значајна и што сакам да го истакнам е различниот пристап на големите сили, првин кон самото дефинирање на тероризмот за кој сеуште не е изнајдена дефиниција, и во разни држави различно се третира, за некои некој напад е терористички за други не е, истото се случува и со сајбер-тероризмот кој многу брзо се разви како многу моќно оружје на терористите, но од претходното наведените примери се уверивме дека и самите држави го применуваат кон загрузување на интегритетот и националната безбедност на други држави.

10.2.Реактивно дејствување

Реактивно дејствување е токму пристапот на поголем број на држави за преземање на заштитни мерки на заштита на информациско-комуникациските системи откако ќе бидат нападнати, па се преземаат мерки колку може да се спаси и да се повратат функциите на истите.

Токму и затоа прв за разгледување го земав реактивниот пристап кој всушност претставува одговор на сајбер-нападот каде првиот потез го има сајбер-терористот, но со таквиот пристап сајбер-терористот е чекор пред безбедносните сили, и додека се открие и поведе истрага тој мирно спие и веќе ги сокрил и уништил можните траги и докази кои со нивно пронаоѓање би се искористиле против него.

Што побрзо и поефикасно дејствување и сумирање на штетата тоа подобро за државата бидејќи овозможува:

---

[251]Pladna, B., Cyber Terrorism and Information Security, East Carolina University, стр. 14, преземено од http://www.InfoSecWriters.com,

[252]Вулетич, Д., Претње сајбер тероризма у Републици Србији и безбедносни одговори на њих, Република Србија, Министерство одбране, институт за стратегијска истраживања, ЖУРНАЛ ЗА БЕЗБЕДНОСНЕ СТУДИЈЕ, Октобар, 001/2008, стр. 82

- Реакција и преземање на дополнителни заштитни мерки;
- Утврдување на можните причини за напад;
- Локализирање на оштетувањата;
- Побрза потрага по можниот сторител;
- Заштита на животот и безбедноста на луѓето;
- Поправка на оштетувањата.

Основните задачи на реактивното дејствување би биле ефикасна неутрализација на нападот како и што побрзо опоравување на системите и враќање во првобитна состојба. Тоа што се однесува до ситемите кои се нападнати, а исто така како реактивен одговор треба да биде и трагање по сторителот, преземање на мерки друг напад од таков вид да не се повтори, дуплирање на системите кои се од витално значење по националната безбедност, резервни копии на хардвер и софтвер на централните компјутери и др.

10.3. Проактивно дејствување

Проактивното дејствување, всушност претставува преземање на превентивни мерки т.е активирање на сите можни аларми и заштитни мерки пред нападот, односно оневозможување да дојде до нападот или негово отежнување. Доколку една држава има јака заштита на виталните информациски-комуникациски системи, постојана контрола над истите, следење и навремено алармирање за можните упади, правилен избор на кадар и обезбедување на оптимални услови за работа, современи системи за детекција на упадите, планови и упатства за извршување на задачите, законски регулативи и др. тогаш и терористите нема да можат така лесно да ги остварат своите зацртани цели.

Затоа нагласувам дека проактивното дејствување е тоа што претставува правилна и навремена заштита што треба да се преземе и озбилно да се свати од сите влади, така што со навремено проактивно дејствување и со евентуален напад последиците би биле многу помали, а со реактивното дејствување само ќе се утврдат носителите и евентуалната одговорност за пропустите.

Проактивното дејствување подразбира одвојување и вложување на значајни финансиски средства, како и обука и едукација на соодветен кадар за справување на таков вид на напад како и:

- ✓ Формирање на соодветно тело за дејствување на национално ниво. Подразбира центар за заштита на националната инфраструктура, кое ќе функционира 24/7, и ќе биде во коралација со другите одговорни тела.
- ✓ Усвојување на Национална стратегија за обезбедување на сајбер-простор. Подразбира намалување на ранливоста од сајбер-напади и минимизирање на штетата и времето потребно за опоравување од евентуалните напади, доколку се случат.

- ✓ Поголема соработка со безбедносните системи и заедничко дејствување со другите сили за безбедност на повеќе држави, особено високо развиените бидејќи сајбер-тероризмот е глобална закана.
- ✓ Тестирање и испитувањена системите, поради пронаоѓање на слабите страни и можните пропусти на системите
- ✓ Соработка помеѓу приватниот сектор и владата и размена на искуства и информации за можните закани и ризици бидејќи подеднакво ги засегаат и двете страни.
- ✓ На национално ниво, неопходно е одговорните лица да преземат мерки за заштита, да направат повеќе копии од важните фајлови, да ги чуваат доверливите документи off-line (надвор од мрежата).[253]

За успешен одговор против тероризмот, висококвалитетната разузнавачка работа е во срцето на проактивната против-терористичка стратегија за успешна инфилтрација и спротивставување на терористичките групи. На глобален план е неопходно високо координирана разузнавачка соработка на земјите сојузници и на сите заинтересирани држави кои може да бидат загрозени од терористичките напади.[254]

10.4. Преземање на мерки од страна на меѓународни организации во борба против сајбер-тероризмот

Меѓународните организации се владини организации кои се формирани со намера, непристрасно одржување на мирот и безбедноста во светот, помош на сиромашните и угнетените, спречување на водење на војни, заштита на човековите права и човековата средина и др. Сето тоа ќе го спроведат преку свои норми и правила, дефинираат нови меѓународни стандарди и задачи, рашируваат нови модели на општествено организирање ширум светот.[255]

Секојдневно сме сведоци насекаде во светот каде има некоја криза, зараза, војна, загрузување и кршење на меѓународното и хуманото право, присутност на некоја меѓународна организација, која се обидува да помогне, да се изнајде мирно решение. Не само тоа тие се длабоко инволвирани и во внатрешните политики на суверените држави, и тоа по прашања кои исклучиво се во домен на државна надлежност, како на пример асистенција во делот на пишување устави, закони, судски, воени и полициски реформи.

Но, како што кажав на почеток тоа се владини организации кои зависат од државните финансии за нивно функционирање, доминираат односно се

---

[253] Вулетич, Д., Претње сајбер тероризма у Републици Србији и безбедносни одговори на њих, Република Србија, Министерство одбране, институт за стратегијска истраживања, ЖУРНАЛ ЗА БЕЗБЕДНОСНЕ СТУДИЈЕ, Октобар, 001/2008, стр. 83

[254] Котовчевски, М., Борба против тероризмот, Македонска цивилизација – Скопје, 2004, стр. 141

[255] Michael N. Barnett and Martha Finnemore, *Rules for the world: international organizations in global politics*, Cornell: Cornell University Press, 2004

претставени во нивните највисоки управувачки тела, и со државен договор се определува кој ќе биде носител на највисоката извршна функција, тогаш е јасно зошто голем број аналитичари ги сметаат МО само за средство во рацете на државите.[256]

Значајно е да се истакне дека и големите сили како САД сфатија дека борбата против терористите е тешка и дека треба будно и постојано да се следи сузбива, и дека ниту една држава, па ни тие не се имуни и неможат така лесно да се заштитат од нивните напади. Што се однесува пак до сајбер-тероризмот, тој им претставува уште поголема потешкотија и главоболка, бидејќи војуваат против непријател кој не се гледа, не му се потребни армии, ниту бомби, туку напаѓа од другата страна на планетата.

За да се заштитат, тие преземаа низа чекори во текот на годините како на пр. менување на законите, политиката и технологијата за заштита на информациите и спречување на сајбер-тероризмот.[257]

Се утврдуваа мерки и стандарди за заштита од сајбер-тероризмот на меѓународно ниво помеѓу приватни фирми и влади, меѓународни организации, воени организациии се повеќе признаваат дека само заеднички може да се заштитат и колку можат повеќе го сузбијат сајбер-тероризмот.

И САД како најбезбедна држава во светот со најразвиена разузнавачка служба не остана имуна на нападите од тероризмот. Атентатите од Њујорк и Вашингтон покажуваат дека во иднина воените конфликти нама да мораат да се ограничуваат единствено во регионот на Европа, Блискиот Исток, Азија и Африка туку можно е поголемиот дел да бидат сконцентрирани токму на теририторијата на Северна Америка. Тоа го потврдуваме и со уривањето на кулите близначки на 11 септември 2001 година. Таквите сценарија не може да се прецизира дали се поттикнати од друга држава или се спремаат одвнатре, но најчесто тоа се меѓународни терористички организации кои планираат и дејствуваат ширум светот.

На светската сцена доминираат голем број на меѓународни организации кои со своите законски прописи и нормативи придонесуваат да се зачува светскиот мир, други се задолжени за унапредување на економскиот развој и помош на неразвиените земји, трети се однесуваат на здравствената заштита и сл. Меѓу кои како најзначајни ќе ги споменам: ООН, ОБСЕ, НАТО, ЕУ, ММФ, СЗО, СТО и др.

Како најзначајни за проблематиката што јас ја разработувам се: НАТО, ОБСЕ, ООН, Советот на европа и др., кои во најголема мера допринесоа да се увидат глобалните заканите кои ги носи сајбер-тероризмот, и преземаа мерки со своите повелби за негово сузбивање и доколку е можно минимизирање или потполно уништување (секако доколку во тоа не се мешаат големите сили кои работат зад грб одредени прљави работи).

10.4.1. НАТО

Северно-Атланската Алијанса на чело со САД сметаат дека најголема

---

[256] Билјана Ванковска, Меѓународна безбедност- критички пристап, Бомат графикс-Скопје, 2011, стр. 145

[257] Schjolberg, S., ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, преземено од http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html,

закана за националната безбедност во светот е тероризмот, и доста цврсто се инволвирани во борбата против него.

Според НАТО (2008) сајбер-тероризам е сајбер-напад со помош на користење или искористување компјутер или комуникациски мрежи, за да се предизвика уништувањем да генерира страв или да го застрашуваат општеството за идеолошка цел.[258]

Особено е важно да се истакне дека НАТО[259] презеде крупни и одлучни чекори за борба против тероризмот, и нетолерирање на тероризмот по никоја основа. Како прво се согласи за заедничка политика на сајбер-одбрана во јануари 2008 година, која беше усвоена на самитот во Букурешт на 3 април. Политиката се состои од посветеност на заштита на критичните информациски системи и зајакнување на националната и меѓународната соработка. Во рамките на НАТО од тогаш, започна да функционира и Кооперативен центар за сајбер одбрана и подршка во Талин (Естонија).

Во периодот од 17-19 јуни, 2009 година се одржа и тридневна конференција за сајбер-војување, на која биле опфатени следните теми:

- ✓ Користење на интернет од страна на терористички организации и можностите за сајбер-напади;
- ✓ Истражувањето на сајбер-шпиунските мрежи;
- ✓ И дали суверенитетот може да се адаптира кон предизвиците во сајбер-безбедноста.[260]

Уште на самитот во Прага, во 2002 година, НАТО лидерите признаа дека постои опасност по критичните инфраструктури од сајбер-терористички напади, и потребата од имплементација на НАТО во програмата за сајбер-одбрана. Формирана е агенција за комуникациско-информациони системи и услуги на НАТО (The NATO Communication and Information Systems Service Agency (NCSA).[261]

Северно Атланскиот Сојуз- (НАТО) претставува досега најсилна воена алијанса создадена после втората светска војна па до ден денес, која зазема важно место во зачувување на светскиот мир, почитување на хуманитарното право, женевска конвенција и др, но под директно покровителство и команда на САД, сведоци сме дека НАТО алијансата дејствува селективно, бранејќи ги интересите особено на САД, која веќе како меѓународна организација го изгуби својот рејтинг (особено по бомбардирањето на СР.Југославија), каде и без одобрение на Советот за безбедност, НАТО алијансата дејствуваше по наредба на САД.

Што се однесува до сајбер-безбедноста до сега немало потреба од интервенција од НАТО, меѓутоа гледаме дека НАТО активно учествува на конференциите организирани на таа тема и дава свој допринос, а како ќе се

---

[258]NATO 2008, Cyber defence concepr MCO 571. Brussels, Belgium

[259] За НАТО повеќе на http://www.nato.int,

[260]Cooperative Cyber Defence Centre of Excellence, Agenda for June 17-19, 2009 CCD COE Conference on Cyber Warfare, http://www.ccdcoe.org/123.html,

[261] Повеќе за NCSA, како таа работи, кои се нејзините активности и задачи, на http://www.ncsa.nato.int/,

справи на дело со оваа закана допрва ќе видиме.

10.4.2. ООН

Различните појавни форми на тероризмот и безобзирноста во неговите форми на извршување беа поттик и Организацијата на Обединетите нации да се ангажира во правец на изнаоѓање форми и начини за дефинирање, проучување и градење на стратегија за спречување и превенирање на појавните облици на тероризмот. Во тој правец во повеќе наврати проблемот на тероризмот зазема соодветен простор во активностите на Организацијата на Обединетите Нации.

Комисијата за меѓународно право при ООН, при утврдување на инкриминациите кои се однесуваат на загрозување на мирот и безбедноста на човештвото, ги обработи инкриминациите кои се однесуваат на тероризмот. Прифаќањето на овој законик беше одложено само затоа што тероризмот како појава исто така беше опфатен во извештајот на Специјалниот комитет за дефинирање на агресијата. При неговото дефинирање, некои забележале дека актот на тероризмот може да ја промени агресијата индиректо или директно.[262] Тоа се однесува и на сајбер-тероризмот како форма на тероризмот.

Меѓутоа за да се донесе одредена одлука и директно да се атакува на тероризмот и на подржувачите на тероризмот до ден денес не видовме, бидејќи уште не е дојдено до општоприфатена дефиниција за тероризмот, така што напорите за нејзино одредување траат и до ден денес. Со тоа што нема општо прифатена дефиниција ги кочи земјите цврсто да заземат став со прецизно издефинирани ставови по кои ќе може да се гонат и сусзбиваат терористите.

Во повеќето собранија, истата ги повикува државите членки чекор по чекор да придонесуваат за попречување на настанувањето на причините за појава на меѓународен тероризам преку преземање на национални мерки, да ги ратификуваат меѓународните конвенции за поедини аспекти на меѓународниот тероризам, потоа да ја испитаат можноста за практична соработка меѓу нив во борбата против меѓународниот тероризам, како и да се стават во функција на препораките и повиците за борба против тоа зло.[263]

Во рамките на Високиот панел, терористичките закани и напади се дефинирани како закана врз вредностите кои го претставуваат темелот на Повелбата на ООН:

- Почитување на човековите права
- Владеење на правото
- Толеранција меѓу луѓето и народите и
- Мирољубивото разрешување на конфликтите.

Состојбите кои придонесуваат за појавата и опстојувањето на тероризмот се регистрираат во:

---

[262] Declaration of special Cometee for Question of definicion of aggression, 31 01-03.03.1972. Oficial document, declaration No. 19 (a/8719)

[263] Un doc. Off.34. Session, Suppl. No. 37 (A/34/37), p.36

- Безнадежноста со која се соочуваат голем број на луѓе и сиромаштијата;
- Политичката неправда;
- Непочитувањето;
- Екстремизмот и кршење на човековите права;
- Регионалните конфликти и
- Недоволниот капацитет на државите да воспостават и одржуваат ред и правда.[264]

ООН не само на полето на безбедноста, има значајна улога и во трговската размена, економската размена, меѓународниот монетарен фонд, светската здравствената организација и др, полиња на кои таа успешно го дава својот придонес. ООН исто така имаат преземено бројни активности кои директно или индиректно биле поврзани со решавањето на проблемот врзан за компјутерски и сајбер-тероризам.

10.4.3.ОБСЕ

Организацијата за безбедност и соработка во Европа (ОБСЕ), огранок на Обединетите нации, има развиено бројни контра-терористички програми за техничка помош, а една од нив е и Единицата за Акција против тероризмот (Action against terrorism Unit-ATU). ATU е "централна точка на ОБСЕ за координирање и помагање во борбата против терористичките активности", кои вклучуваат изработка за програми за помош, обука и организирање на стручни работилници на тема-борба против тероризмот.[265]

Од 2004 година, сајбер-тероризмот е една од главните области на кои ATU става акцент.

Ерик Лебедел (Eric Lebedel), амбасадород Франција, претседател на Форумот за Безбедносна соработка на ОБСЕ, го опиша дејствувањето на ОБСЕ како „проактивно" во изнаоѓањето на одговор на заканата од сајбер-тероризмот, тој призна дека "останува уште многу да се направи во борбата со оваа променлива закана што влијае врз сите димензии на безбедноста.[266]

Во Баку (Азербејџан) 2011 година се одржа дводневна конференција подржана од ОБСЕ, на тема „Фаќање во костец со сајбер-криминалот", а целта на конференцијата беше да се подигне свеста за проблемите и заканите кои што може да ги донесе сајбер-тероризмот.[267]

ОБСЕ во рамките на Обединетите Нации преземаат бројни активности за успешно справување со сајбер-тероризмот која се уште млада метода на терористите, не ја доживеала својата потполна експанзија, па што побрзо превенирање и презимање мерки за нејзино спречување, ќе има поголеми резултати во успешна одбрана. Својот удел што го зема во развивање и

---

[264]Димовски, Злате – Тероризам, Графотранс – Скопје, 2007. стр. 32

[265]*Gable, A., K.,* Cyber-Apokalypse Now: Securing the Internet Agains Cyberterrorism and Using Universal Jurisdiction as a Deterrent, VANDERBILT JOURNAL OF TRANSNATIONAL LAW, VOL. 43:57, СТР. 91-94

[266] Повеќе во: Press Release, Org.for Sec.& Co-operation in Eur., http://www.osce.org/fsc/50717,

[267] ПОВЕЌЕ ЗА КОНФЕРЕНЦИЈАТА ВО Баку на http://www.osce.org.baku/83604,

покровителство на единицата за акција против тероризмот, ни говори за определбата на ОБСЕ во успешно справување и борба против сајбер-тероризмот што допрва следи, (доколку не потпадне под влијание на големите сили, па со селективност да се дејствува против можните сајбер-терористи без разлика дали се под покровителство на терор-организации или држави).

10.4.4.Совет на Европа

Меѓу другите безбедносни прашања кои ги разгледува и донесува Советот за Безбедност кои важат за сите членки на ЕУ, како еден од најзначајните чекори е токму Конвенцијата за компјутерски криминал, која стапи на сила во 2004 година.[268]

Од страните потписнички на конвенцијата се бара:

- ✓ Да донесат суштински и процедурални закони;
- ✓ Да се криминализираат одредени дела кои влегуваат во компјутерскиот криминал, и
- ✓ Да се олесни екстрадицијата на оние обвинети за извршување на вакви злосторства.

Советот на Европа има донесено бројни студии и директиви со помош на кои се става на тапет компјутерскиот криминал и сајбер тероризмот како глобална закана на 21-век меѓу кои:

Во рамките на групата Г8 од 1997 година (кога е предложен акциониот план за борба против компјутерски криминал, а усвоен 1998 година), на предлог на експертската група за соработка на полето правда и внатрешни работи, министрите во повеќе наврати расправале за принципите на таа борба, како и за потребите за меѓународна соработка во спроведување на истраги и фаќање на извршителите, како и прифаќање на стандарди дефинирани со конвенцијата на Советот на Европа.

На Лисабонскиот состанок на Советот на Европа, 2000-тата е истакнато значењето на транзицијата во конкурентна, динамична и на знаење заснована економија, ги претставува насоките на активностите поврзани за разбирање на феноменот компјутерски криминал.

Во истата година е донесен и Предлог на Советот за правна рамка за одлучување, поврзано за нападите на информациониот систем (Proposal for a Council Framework Decision on attacks against information system).После една година, документот е дополнет со недозволен пристап во информационите системи и недозволено поречување на системите и податоците.

Во 2000 година донесена е и Директивата за електронско работење (*Directive on electronic commerce),* во која посебно внимание е посветено на проблемот на злоупотреба.[269] Исто така значаен документ донесен истата година кој треба да обезбеди сигурно информациско општество, низ безбедна

---

[268] За конвенцијата, кои земји ја имаат ратификувано и кога стапила во сила, види повеќе на: Council of Europe, Convention on Cybercrime, Chart of Signatures and Ratifications, достапно на: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG,

[269]Directive on electronic commerce http://www.edc.uoc.gr/~panas/PATRA/sieber.pdf.

информациска инфраструктура и борба против криминал поврзан за компјутерите (Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime).[270]

Советот на Европа на крајот на 1998 година отпочнува со подготовки за донесување на **Конвенција на сајбер криминал**, а во 2000 година пуштена е во процедура и јавна расорава. Конвенцијата стапи на сила во јули 2004 година, и ја пратат бројни документи донесени во рамките на советот:

- Cyber-Rights & Cyber-liberties, Advocacy Handbook for NGOs (2003);
- The Protocol to the Cybercrime Treaty(2002);
- Report Revised draft of the Protocol on Racist Speech(2002);
- Backround Materials on the Racist Speech Protocol;
- Second Protocol on Terrorism (2002);
- Racism Protocol to the Convention on Cybercrime(2003) и др.

Во јануари, 2007 година беше усвоена и Препораката за соработка со Интерпол[271], во борбата против тероризмот, со која на владите им се препорачува во борбата против тероризмот да ги користат алатките и услугите на Интерпол.

Советот на Европа јасно ги оквалификува компјутерскиот тероризам и сајбер-тероризмот како глобална закана на 21-от век и ги презеде сите мерки преку конвенции и други препораки за соработка на сите меѓународни институции меѓу себе за успешна борба против оваа зло. Советот на Европа има донесено најмногу директиви и одржано бројни конференција на кои е потенцирана заканата на светската безбедност, и оквалификуван сајбер-тероризмот како глобална закана, против кој треба превентивно и навремено да дејствува, за да може да стопира метастазирањето на оваа болест додека не е касно.

---

[270]Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, http://www.justice.gov/criminal/cybercrime/intl/EUCommunication.0101.pdf.

[271]Recommendation Rec (2007) 1 of the Committee of Ministers to member states regarding co-operation against terrorism between the Council of Europe and its member states, and the International Criminal Police Organization(ICPO-Interpol), достапно на http://www.coe.int.

10.5. Мерки што ги презема Република Македонија во борба против сајбер - тероризмот

Секоја држава за своето успешно функционирање и за заштита на своите витални функции обезбедува основни предуслови за тоа, и презима мерки за успешна заштита.

Еден од тие предуслови е и успешното функционирање на разузнавачко – безбедносниот систем, и спротивставување на сите облици на закани што претставуваат закана по безбедноста на граѓаните или институциите на системот.

За тоа успешно да се спроведе, неопходно е да се преземат следните мерки и активности:

- Донесување на закони што одговараат во областа на одбраната и безбедноста на земјата;
- Правно регулирање на обврските на сите носители на безбедноста;
- Создавање на предуслови (материјални и законски) за работа со стручните органи и служби;
- Регулирање на научни, технички, военоекономски и други облици на соработка со странски земји;
- Регулирањена начинот за заштита на објектите од посебно значење како и документите во нив;
- Правно регулирање на соработката и надлежностите на сите служби кои се занимаваат со спротивставување на дејностите на разузнавачката служба.[272]

Република Македонија нема донесено посебен закон, односно останува неинкриминирано кривичното дело Сајбер-тероризам, па оттука и нема посебно специјализирани институции и посебно обучени стручни лица во Министерствата и во безбедносните сили, кои би се занимавале со сајбер-тероризмот како посебен облик на тероризам.

Сајбер-тероризмот како облик на тероризам, во Уставот на Република Македонија[273] како највисок правен акт, не е пропишана посебна законска рамка за борба против ваков вид на криминал, туку важат истите мерки и активности кои се преземаат во борба против сите извори и облици на нарушување на безбедноста на граѓаните и загрозување на националната безбедност од тероризмот и сите негови облици и видови. Меѓутоа, секако дека постојат и државни институции, кои се одговорни за заштита на информацискатa технологија и информацискатa безбедност во целина каде спаѓа и сајбер-тероризмот.

---

[272] Котовчевски, Митко., Современи разузнавачки служби, Македонска цивилизација - Скопје, 2001, стр. 64

[273] Устав на Република Македонија, 1991, достапно на http://www.pravo.org.mk/documentDetail.php?id=538,

Тука влегуваат:

- Министерството за информатичко општество и администрација, [274]
- Министерството за внатрешни работи, [275]во чии рамки се:
  - ✓ Бирото за јавна безбедност (БЈБ),
  - ✓ Управата за безбедност и контраразузнавање (УБК),
  - ✓ Криминалистичката полиција
- Министерството за одбрана[276], во чии рамки функционира:
  - ✓ Сектор за безбедност и разузнавање
- Агенција за разузнавање[277],
- Совет за национална безбедност на Претседателот на РМ[278],
- Центар за управување со кризи, и
- Агенција за електронски комуникации.[279]

Со добра соработка и добра координација на горе споменатите институции, како и интензивирање на меѓународна соработка на оваа поле, можеме да зборуваме за борба против сајбер-тероризмот. Секако дека во успешна борба и справување со тероризмот како и сајбер-тероризмот најголем збор го има државата, која треба да изгради успешен систем за борба против ова зло, што подразбира обучени и опремени безбедносни сили за успешно справување од овој вид на закана, поголема соработка помеѓу државните институции и приватниот сектор, како и измена и дополнување на постоечкиот Кривичен законик, и инкриминација на сајбер-тероризмот во нашето законодавие, а подоцна и донесување на соодветни прописи за усогласување со меѓународните стандарди.

---

[274] Официјална веб-страница на Министерството за Информатичко општество и администрација на Република Македонија, http://www.mio.gov.mk/

[275] Официјална веб-страница на Министерството за внатрешни работи на Република Македонија, http://mvr.gov.mk/,

[276] Официјална веб-страница на Министерството за одбрана на Република Македонија http://www.morm.gov.mk/portal/,

[277] Официјална веб-страница на Агенција за разузнавање на Република Македонија http://www.ia.gov.mk/maked/ar.htm,

[278] Официјална веб-страница на Советот за национална безбедност на Претседателот на Република Македонија http://www.president.gov.mk/mk/kabinet/sovet-za-bezbednost.html,

[279] Официјалната веб-страница на Агенцијата за електронски комуникации на Република Македонија http://www.aec.mk/,

11. Заклучок

Основна цел на овој труд е прибирање на податоци и давање на научна дескрипција и објаснување на конкретната појава наречена Сајбер-тероризам.

Исто така, особено важно е да се направи разграничување на предностите и недостатоците на брзиот развој на информатичката технологија и навлегување во сите сфери на општественото живеење, придобивките и недостатоците на глобалната компјутеризација, која на голема врата овозможи појава на сајбер-тероризам, како модерен облик на тероризмот и нова глобална закана по светскиот мир и безбедноста.

Со дефинирањето на поимите сајбер-простор, сајбер-напад, сајбер-криминал, сајбер-тероризам, направивме едно спознавање на оваа проблематика од настанокот, развојот, начинот на делување, критичната инфраструктура, мотивот и целите кои им се, и на крај кои се мерки и активности се потребни да се преземат од владите на државите и големите сили за успешно сузбивање на овој вид на општествено зло.

На сајбер-тероризмот не треба да се гледа како на научна фантастика и да чекаме да видиме до каде може да отиде и кои се неговите крајни ефекти од еден сајбер-терористички напад, туку треба да се сфати како реална опасност и закана бидејќи тој е веќе меѓу нас, а терористите постојано вршат илјадници сајбер-напади, но сеуште не се отидени предалеку и светот сеуште не ги осетил разорните последици од еден вистински сајбер-напад за кој критичарите сметаат дека многу брзо ќе се случи.

Брзиот информациски развој и преминот во информатичко општество, што го овозможи информатичката револуција особено последната декада, го дигитализираа светот и го олесни животот каде многубројните скапи и спори активности, беа заменети со брзи, лесни, ефтини т.е само со кликање на едно копче на компјутер и го имаме светот на дланка, но таквите продобивки не останаа незабележани од терористите кои ги насочија за реализација и остварување на сопствените цели, а целите на сите терористи им се истите како и кај традиционалниот начин на тероризам, а тоа е потклекнување на владите и исполнување на нивните барања.

Зошто сајбер-тероризмот стана атрактивна опција за терористите, и се повеќе почна да се практикува како начин за најдобро постигнување на ефектите? Затоа што има лесен пристап, брз проток на информации, неограничена комуникација, евтин за употреба, што терористите сето тоа го искористија за своја арена и широко поле за борба против сите субјекти во светот кои не им одговараат. За изведување на еден сајбер-терористички напад, не им е потребна голема војска, тренинг кампови и скапи оружја и опрема туку само еден компјутер и професионален хакер, за да се спроведе успешен сајбер-напад, секако во добро одбрана цел од страна на терористите, токму таму каде што ќе се најде пукнатина во системот и ќе се искористи

необученоста и нестручноста на безбедносните сили. Затоа во своите редови терористите се повеќе регрутираат високо образовни кадри, добро потковани со знаење од областа на информационата технологија, со помош на која се вршат планирање, организирање, комуникација и координирање, задоени со насилничка идеологија, жедни за крв и публицитет, преземаат сајбер-напади ширум светот, на штета на општество, најчесто насочени да допрат до цивилното население, а крајниот мотив се најчесто политички промени.

На почетокот можеби и не беше сфатен како голема закана од глобални размери, но откако големите држави увидоа дека сајбер-тероризмот претставува закана на кои не се имуни ниту тие, со најјаки безбедносни системи и најдобро платени разузнавачки служби, почнаа да преземаат соодветни мерки за успешна заштита од сајбер-тероризмот, но откако ја увидоа предноста на сајбер-терористот што ја има во виртуелниот свет, кој е безграничен, анонимен, агеографски сфатија дека ќе биде многу тешко справувањето со оваа зло и изведување на сторителот пред лицето на правдата.

За да знаеме какви мерки треба да преземеме, за да се заштитиме од оваа зло треба добро да го проучиме, со кое би помогнале во подигање на свеста и на другите граѓани кои не се информирани и не знаат што е тоа сајбер-тероризам и како може да ни наштети, и како може да ја загрози дури и безбедноста на државата.

Невидливиот непријател вооружен единствено со преносен комјутер (лап-топ), конектиран на глобалната компјутерска мрежа, „вооружен" со големо компјутерско-знаење и искуство, задоен со огромна деструктивна енергија и огнена желба да ги оствари своите мрачни цели, впловува во напад со тешко препознатлив правец, но со единствена цел: електронски напад врз државната информациска мрежа од огромно стратегиско значење и упад во мрежата на виталните државни институции и нивно хакерирање или некаква злоупотреба за сопствени цели.

Тоа е злокобното лице на сајбер-терористот и сајбер тероризмот, опасна закана за националната безбедност на определени држави, смртна закана и за глобалната безбедност во наредниот период.

Целта на современите терористички организации, е токму дестабилизирањен на економијата, и економската стабилност на земјата, а со тоа и поткопување на довербата и подршката на граѓаните што ја имаат во институциите на системот, доколку не бидат правилно и навремено заштитени.

Токму затоа терористите се повеќе се ориентираат кон сајбер-терористички напади бидејќи со модернизација на општеството и функционирање на целокупниот современ живот преку интернет и електронското работење, ги отвори портите на терористите кон напад на ваквите системи со кои со едно кликање на копче на компјутер ќе нападнат или банка, или нуклеарна постројка, или ќе остават без греење или

ел.енергија цел град, ќе изменат или ќе избришат медицинска документација, ќе ги сменат состојките за изработка на некој лек со што ќе се заразат милиони луѓе и многу други можности што им ги нуди напредната информатичка-технологија, на сајбер-терористите за нивните мрачни цели. Но владите особено на високо развиените држави, ја увидеа опасноста од сајбер-терористичките напади и почнаа со проучување на овој вид на тероризам и преземање на мерки на заштита од истиот, или во најмала рака доколку би се случил да се помине со што помала штета, и што побрзо враќење во нармала.

Соочени со ова зло, Владите на различни држави (нема држава која не е цел на терористи и на сајбер-терористички напади, особено западно европските држави и САД), треба да креираат политика за успешен и ефикасен противтерористички одговор, навремена идентификација на терористичка закана и стопирање на можниот напад, а тоа е можно со добро опремени безбедносни сили, спроведување на построга казнена легислатива, појаки разузнавачки служби, меѓународна соработка и заеднички акции на мултинационално ниво, бидејќи слабиот одговор на силите на безбедност особено на големите сили уште повеќе им овозможува развој и простор за планирање и изведување на сајбер-терористички акции, чие време допрва следи, а веќе се наметна како закана за глоболната безбедност на 21-от век.

За разлика од конвенционалните напади, сајбер-терористичките напади, можат да бидат изведени по пат на далечинско управување на растојание оддалечено со илјадници километри, со што се намалува можноста за откривање и фаќање на сторителот. Секако дека терористите нема да се откажат од традиционалниот начин на поставување на бомби по метроа, по згради, киднапирања и вршење на атентати, но за тоа се потребни големи подготовки, многу големи финансиски средства, обука и поголемата можност за фаќање на истите доколку нешто тргне наопаку и разоткривање на другите инволвирани.

По долготрајно и детално истражување за потребите на овој труд може да се наиде на повеќе примери за веќе извршени сајбер-терористички напади ширум светот, кои беа наведени како пример што сајбер-терористите повеќе сакаат да нападнат, начинот на припремата, кој може и како да го изврши нападот, начинот на заштита на државата од таквите напади, и сл. Ова може да ни користи во понатамошната борба со сајбер-тероризмот, како за заштита на виталните институции така и за приватните упади во компјутерите и крадење на податоци и други доверливи документи.

Меѓутоа, иако сајбер-терористичките напади се високо ефективни, со ниски трошоци, тие можат да се реализираат од голема дистанца, го поседуваат елементот на комплетно изненадување и се реализираат многу побрзо отколку што противникот може адекватно да одговори на истите, сепак сакам да нагласам дека не е нешто од што неможеме да се заштитиме, или дека треба да потклекнеме на ваквите напади, напротив секоја држава која навреме ќе преземе мерки за заштита на системите на виталните

институции и критични точки, со добро обучени разузнавачки тимови и софистицирана опрема, нема да можат терористите толку лесно да им ги хакираат системите, туку напротив нивните напади би имале многу мало дејство што можеби нема ни да се осети во општеството или со минимални штети.

Сајбер-тероризмот како закана врз глобалната безбедност во 21-от век, постојано не демне, прашање е само време и место каде ќе го осетиме неговиот разорен моќ, и ќе ги изброиме жртвите врз недолжно цивилно население предизвикани од група луѓе, добро обучени за работа со компјутер, спремни се да направат за својата идеологија наречени сајбер-терористи.

12. Литература

Книги и монографии

- Милошевиќ, М., Систем државне безбедности, Београд, 2001
- Flemming, P., Stoht, M., Myths and realities of Cyberterrorism, Countering terrorism Through international Cooperation, Coutmayer, Italy,2000
- Котовчевски, М., Современ тероризам, Македонска цивилизација, Скопје 2003
- Milosavljevic, M., Grubor, G., Istraga kompjuterskog kriminala, Univerzitet SINGIDUNUM, Beograd, 2009
- Котовчевски, М., Национална безбедност, Бомат Графикс, Скопје 2013
- Котовчевски, М., Борба против тероризмот, Македонска цивилизација, Скопје, 2004
- Котовчевски, М., Национална Безбедност, Бомат Графикс, Скопје, 2011
- Билјана Ванковска, Меѓународна безбедност – Критички Пристап, 2011.
- Hoffman, B., Inside Terrorism (revised and Expanded Edition), New York: Columbia University Press, 2006
- Квигин, Т., Да се види Невидливото, Разузнавањето за националната безбедност во несигурно време, Магор, Скопје, 2009
- Кронин, К., О., Лудс, М., Ц., Напад на тероризмот: Елементи на грандиозна стратегија, Скопје, Нампрес, 2009
- Kuehl, D., From Cyberspace to Cyberpower: Defining the Problem, Information Resources Management College/National Defenses University
- Kurbalija, J., Uvod u upravljanje internetom, Drugo izdanje,Albatros Plus, Beograd 2011
- Laqueur, W., the New Terrorism-Fanatism and the Arms of Mass Destrustion, London, 1998
- Margetic, D., ISLAMSKI TERORIZAM NA JUGU EVROPE, Zagreb, 2006
- Bradly, K., A., Anatomy of Cyberterrorism: Is America vulnarable?, Maxwell AFB, AL, February, 2003
- Ganor, B., достапно на :http://www.ist.org.il/articles/articledetcfm?articleid=128
- Petrovic, R., S., Znanjem protiv Zloupotrebe znanja
- Thomassen, N., *Communicative Ethics in Theory and Practice*, Macmillan, 1992

- Тунески, А., Бабунски, Д., Заев, Е., Регулација и автоматизацијана ХЕП Скрипта(Прва верзија), Машински факултет Скопје, 2008
- Sshmid, A., P., De Graaf, J., *Violence as communication, Mineapolis & London: University of Minesota press, 1982*
- Николовски, М., Поврзаноста и влијанието на организираниот криминал, тероризмот и политиката, Графотекс, Скопје, 2008
- Милошевиќ, М., Систем државне безбедности, Београд, 2001
- Котовчевски, М., Современи разузнавачки Служби, Македонска Цивилизација-Скопје, 2002,
- Verton, D., Black ice> The Invisible Threat of Cyber-terrorism, McGraq-Hill/Osborne, CA, USA 2003
- Шалијан, Ж., Блин, А., Историјата на тероризмот: Од Антиката до Ал- Каеда, Табернакул, Скопје, 2009
- Југослав Ачковски, Методија Дојчиновски., Сигурност на компјутерски системи, компјутерски криминал и компјутерски тероризам.
- Димовски, З.,Тероризам, Скопје, 2007
- Paul Wilkinson: "Political Terrorism", London 1974.
- Rogriguez, A., C., CYBERTERRORISM- A rising treath in the Western hemisphere, Monograph, Washington, DC., 2006
- Спасески, Ј., Македонија-столб на безбедноста и мирот на Балканот, Скопје, 2005
- Спасески, Ј., Аслимоски, П., "Безбедност, Одбрана,мир", Охрид, 2001
- *Nacos,* B., L., Mass-Mediated Terrorism: The Central Role of the media in Terrorism and Counterterrorism, New York: Columbia University pres, 2006
- *Stancic, " Digitalizacija grage".*
- *Wilson, C (2003), Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for congress, CRS.*
- *Petrovic R.S., Kompjuterski criminal, op.cit.*
- *Petrovic R.S., Kiberterorizam, Vojno delo, god. LIII, br. 2/2001.*
- Steven Metz," Strategic Asymmetry," *Milatery Review,* July-Avgust, 1997
- 2013 5th international Coference on Cyber Conflict K. Podins, J.Stanissen, M. Maybaum (Eds.) 2013 @ NATO CCD COE Publications, Tallinn
- Russell, Charles A., and Bowman H.Miller."Profile of a Terrorist", Terrorizm:An International Journal, 1, No.1 1977,
- Shupe, Anson, D (1998), wolvesWithin The Fold: Religious Leadership New Religious Oxford Rutgers press, p. 162

- Scheuer, M., (January, 2008), Bin Laden Identifies Saudi Arabia as the enemy of Mujahideen unity. Terrorism focus.

Зборници и списанија

- Addicott, J., Terrorism Law: Materials, Cases, Comments, 6th edition (2011), Center for Terrorism law Issues for Discusion-Cyber Security, 11 March 2011 CLE
- Benoist, A., Тероризам је рат глобалног свијета, Хрватско слово, бр.344, Загреб, 2001
- Bozinovska, N., PUSH Tehnology, Wireless and mobile Tehnologies, 2002
- Cohen, A., CYBERTERRORISM: ARE WE LEGALLY READY?, THE JOURNAL OF INTERNATIONAL BUSINESS & LAW, 4/15/2010
- Dimitrova, V., *Security aspects for mobile communications, Wirelles and Mobile Tehnologies, 2002*
- Македонско сонце – интервју со Марја Ристески – инспектор по компјутерски криминал
- Derencinovic, D., Novi antiterorizam na razmedju depolitizacije dejuridizacije, Zbornik Pravnog Fakulteta u Zagrebu, 2002/3-4
- Мирческа, Н., Сајбер-тероризам, современ облик на тероризмот, Колку Република македонија е ранлива од Сајбер-тероризам, Годишник на Факултетот за безбедност, Скопје, 2010
- Тупанчевски, Н., Компјутерски криминалитет, Годишник на правниот факултет, Скопје, 1990/91
- Whine, M., Cyberspace: A New Medium for Communication, Command and Control by Extremists. *Studies in Conflict and terrorism* Vol.22. 1999
- Zirojevic, T., M., BORBA PROTIV TERORIZMA, Revija za bezbednost, strucni casopis o corupcii I organizovanom kriminali, Godina 4, br2, 2010
- Arquilla, J., Ronfeldt, D., Networks and Netwars: The Future of Terror, Crime and Militancy, RAND, 2001
- *Gable,* A., K., Cyber-Apocalypse Now: Securing the Internet Agains Cyberterrorism and Using Universal Jurisdiction a Deterrent, VANDERBILT JOURNAL OF TRANSNATIONAL LAW, Vol. 43:57
- Крајновић, П., Безбједност-Полиција-Грађани, Часопис Министарство унутрашњих послова Републике Српске, Бања Лука, Година 6, бр 1-2/10
- Marsan, C., Examining the Reality of Cyberwar in Wakeof Estonian Attacs, Network World, August 27, 2007, vol. 24, no.33

- Trends in terrorism series, Canadian center for Intellegence and Security studies, The Norman Paterson scool of Inernational Affairs, Carleton University, Volume 2, 2006
- Al-Qaeda's origins and links. BBC News. July 20, 2004.
- Lebanese Wary of a Rising Hezbollah Washington Post. December 20, 2004 Retrived August 8, 2006
- Лазарова, М., **Слободата на изразувањето во сајбер просторот,** превземено од http://www.ii.edu.mk/.../слободата%20на%изразувањето%20во%20сајбер%20просторот
- Jeffrey Goldberg the New Yorker. Oktober 14, 2002,
- Cook Robin (July 8. 2005), The struggle against terrorism. Cannot be won by military means. The Guardian.

Речници и енциклопедии

- Department of Defance Dictionary, преземено од :http://www.dtic.mil/doctrine/jel/doddict/data/01168.html,
- Википедија, планирање и организирање на сајбер-тероризам
- Encyclopedia Brittanica, dospapno na http://www.britanica.com/EBchecked/topic/303857/jihad
- Исламски речник, достапен на http://www.islamic-dictionary.com/index.php?word=ummah.
- Мала енциклопедија – ИП Просвета, Београд, 1970
- Поимник на Македонски зборови од областа на информатичката технологија, Министерство за Информатичко општество и администрација на Република Македонија
- The New Dictionary of English, Oxford English Dictionari, превземено од : http:/ /www.oed.com/
- Vujaklija, M., Leksikonstranih reci I izraza

Извештаи

- Convway, M., Cybercortical Warfare: the Case of Hizbollah. Org, Paper prepared for presentation at European Cosortium for Political Research (ECPR) Joint Sessions of Workshops, Edinburgh, UK, 28 March-2 April, 2003
- Gao Report, "Information Security: Computer Attaks at Department of Defense Pose Increasing Risks" преземено од http://www.fas.orfg/irp/gao/aim96084.htm.

- Fischer, A., E., Creating a National Framework for Cybersecurity: An Analysis of Issues and Options,CRS Report for Congress, RL 32777, February 22, 2005
- Kulesza, J., State responsibilitu for acts of cyber-terrorism, GigaNet Symposium, Vilnius, September 13, 2010
- McAfee Virtual criminology Report: organized crime and the internet, December 2006, превземено http://www.sigma.com.pl/pliki/albums/userpics/10007/VirtualCriminology Report 2006.pdf
- Nagpal, R., SYBER TERRORISM IN THE CONTEXT OF GLOBALIZATION, Paper presented at: IIWorld Congress on Informatics and Law, Madrid, spain, September 2002
- Ratledge, M., Info War: Cyber Terrorism in the 21st century, Can SCADA systems be successfully defended, or are they our 'Achilles heel'?SANS GSEC practical Version 1.4, September, 2002
- Shea, A., D., Critical infrastructure: Control Systems and the terrorist Treat, CRS Report ror Congress, RL 31534, February 21, 2003
- Weimann, G., Cyberterrorism, How Real is the Threat?, Special Report 119, United States Institute of Peace, December, 2004, преземено од http://www. Usip.org/ publications/cyberterrorism-how-real-threat
- Wilson, C., Botnets, Cybercrime and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, January, 2008
- Wilson, C., Botnets, Cybercrime and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, April, 2005
- Ranstorp, Hizbollah in Lebanon, 1997, p. 45
- Harel, Amos; Stern, Yoav (August 4, 2006) "Iranian official admits Tehran Supplied missiles to Hezbollah".
- "Terrorist Television Hezbollah has a Word Wide reach" National review On-line. December 22, 2004.
- Middle East, Wahhabi opponent killed in Iran" BBC News. June 26, 2007.

- Конвенција за компјутерски криминал од 2001 година на Совет на Европа бр.185, достапна на http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG
- Стратегијата за борба против тероризмот, види повеќе на http://europa.eu/legislation summaries/justice freedom security/fight agains terrorism/133275 en.htm
- Директива за електронско работење – Совет за безбедност достапно на : http://eur-lex.europa.eu/LexUriserv/LexUriserv.do?uri=OJ:L:2000:178:0001:0016:EN:PD

- Creating a Safer information Society by Improving the Security of Information Infratrukrutes and Combating Computer –related Crime http://www.justice.gov/criminal/cybercrime/intl/EUCommunication.0101.pd
- Cyber-Rights & Cyber-liberties, Advocacy Handbook for NGOs (2003),
- The Protocol to the Cybercrime Treaty(2002),
- Report Revised draft of the Protocol on Racist Speech(2002),
- Backround Materials on the Racist Speech Protocol,
- Second Protocol on Terrorism (2002),
- Racism Protocol to the Convention on Cybercrime(2003) .
- Повеќе за конференцијата во Баку на http://www.osce.org.baku/83604,

Интернет извори

- Агенција за електронски комуникации на Република Македонија http://www.aec.mk/
- Агенција за разузнавање на Република Македонија http://www.ia.gov.mk/maked/ar.htm
- Al Qaeda suspect reveals communication strategy, CNN News, August 4 2004, превземено од http://www.cnn.com/2004/US/08/03/terror.threat/idex.html
- Bosch, O., Defending agains cyber terrorism: preserving the legitimate economy, BUSINESS AND SECURITY, SIPRI, 2004 превземено од http://www.sipri.org
- Center for Strategic International Studies, достапно на http://www.csis.org

- Clarke, R., *Information tehnology & Cyberspace : Their Impact on Rights and liberties,* Mietta's, Melbourne, January 1996, превземено од http://www.anu.edu.au/people/Roger.Clarke/II/index.html
- Clem, A., Galwankar, S., Buck, G., health Implications of Cyber-terrorism, Prehospital and Disaster medicine, Vol.18, No. 3, 15 March 2004, превземено од http://pdm.medicine.wisc.edu
- Collier, S., J., Lakoff, A., The Vulnerability of Vital Sistems: *How "Critical Infrastructure" Become a Security Problem, 2008,*превземено од http://anthroposlab.net/wp/publivations/2008/01/collier-andlakoff.pdf
- Collier, C., B., The Future of Cyber-terrorism: Where the Physical and Virtual Worlds Converge, 11th Annual International Symposium on Criminal Justice
- Issues, Institute for Security and Intelligence, превземено од http://afgen.com/terrorism l .html
- *Marshall McLuhan Foresees The Global Village, http:// www.livinginternet.com/i/ii mcluhan.htm*
- Computer Professional For Social Responsibility, http://cpsr.org
- Достапно на веб http://www.let.leidenuniv.nl/history/ivh/chap2.htm
- History of ARPANET достапно на http://inventors.about.com/library/weekly/aa091598.htm
- Cooperative Cyber Defense Centre of Exellance Agenda for June 17-19, 2009 CCD COE Conference on Cyber Warfare, httpwww.cedcoe.org/123.html
- Counter-terrorism, Training and Resources for Law Enforcement, http://counterterrorismtraining.gov
- Crime online: Cyber crime and illegal inivattion, Research report: July 2009, превземено од http://eprints.brighton.as.uk/5800/01/Crime Online.pdf
- Cromwell, B., 'Separatist, Para Military, Military, and political organizations' достапно на http://www.sromwell-intl.com/security/netusers.html
- Duell, S., Cyberterrorism, American Siciety for industrialSecurity: San Francisko Bay Area Chapter 2001, достапнонаhttp://search.freefing/find.html?si=57336350&pid=r&n =0& charset =UTF&bcd=%C3%B7query=Cyberterrorism