УНИВЕРЗИТЕТ У НИШУ
ПРАВНИ ФАКУЛТЕТ

Компјутерски тероризам

(мастер рад)

Ментор:
Проф. др Дарко Димовски

Студент:
Васић Милош М011/16-УП

Ниш, 2018

УНИВЕРЗИТЕТ У НИШУ
ПРАВНИ ФАКУЛТЕТ

Компјутерски тероризам

(мастер рад)

Ментор:
Проф. др Дарко Димовски

Студент:
Васић Милош М011/16-УП

Ниш, 2018

САДРЖАЈ

Увод

Напади аутомобилима, отмице, подметање бомби на разним местима и манифестацијама, су оно што је до сада обележавало тероризам. Са развојем друштва, односно науке и технологије, долази се до нових могућности деловања. Сав онај ризик, где је било неопходно угрозити свој живот како би се извела терористичка акција, постепено је нестао, замењен је могућношћу вршења тероризма из фотеље своје собе.

Као што је новонастала технологија употребљена кроз добре ствари, омогућивши несметано функционисање друштва, тако је дошло и до њене злоупотребе. Могућност самосталног коришћења рачунара које је компјутерским програмима потпуно олакшало приступ и његово познавање скоро сваком лицу које је заинтересовано, довело је до тога да га свако може злоупотребити.

У почетку се злоупотреба сводила на кривична дела , с циљем прибављања одређених користи, међутим схвативши могућност, и терористичке организације су те које су се окренуле овом виду ратовања. Тог тренутка је опасност по друштво достигла свој максимум.

Тему компјутерски тероризам ћу обрадити кроз овај мастер рад, пре свега због због њене занимљивости. Конвенционални начини вршења тероризма ће свакодневно бити замењивани овом новом врстом, где постоји велики број непознаница, а као неко ко је проводио доста времена на компјутеру, и неко коме је проучавања безбедности и њеног угрожавања веома интересантно, решио сам да спојим те две ствари.

Пре свега због недостатка како домаће, тако и стране литературе, ову тему ћу обрадити кроз анализу већ постојећих тумачења и схватања, покушаћу, онда када сам у могућности да дам свој суд о томе, као и да навођењем примера из стварности, што више приближим и појасним појмове везане за компјутерски тероризам.

Циљ овог мастер рада би ми био што боље упознавање и разумевање нове опасности која прети, како мени као члану овог друштва, тако и целом друштву, али и упознавање других заинтересованих лица са овом темом, сводећи битне информације на једном месту.

Тему компјутерски тероризам планирам да обрадим на тај начин што ћу пре свега сагледати појмове који га сачињавају.

Компјутерски криминалитет је појам приближан компјутерском тероризму, разликује се пре свега у неколико карактеристика, самим тим како бих направио разлику између њих, поћи ћу од првенствено дефинисања компјутерског криминалитета, сагледавања његових карактеристика, његових врсти, као и његовог законског третирања.

Друго поглавље које је неопходно сагледати јесте поље тероризма. Компјутерски тероризам као врста тероризма, има његове катактеристике, односно све његове елементе, али како бих ипак сагледао ту разлику, односно по чему се компјутерски тероризам издваја, анализираћу тероризам, шта је оно што га изазива, сагладавање какав све тероризам постоји, као и поставка нашег законодавства у борби са њим.

Након обраде ових поглавља, долазимо до централног дела теме, односно најбитнијег, компјутерског тероризма. Због недостатка јединствене дефиниције, сагледаћу схватања различитих теоретичара, анализираћу и даћу своје виђање специфичности које га издвавају од осталих врста тероризма, као и видети који су то све начини на који се ова врста тероризма манифестује.

Видећемо да ли је Интернет стварно место које може угрозити функционисање друштва, односно да ли је стварно толико коришћен од стране терористичких организација, као и у коју сврху.

На крају ћу пробати да сагледам која је одбрана могућа, односно шта треба предузети како би се ова врста тероризма истребила, анализирањем схватања неких битних међународних организација.

Пробаћу да након свега тога извучем закључак о опасности ове појаве.

I. КОМПЈУТЕРСКИ КРИМИНАЛИТЕТ

1. Појам

Велики број фактора утиче како на настанак, тако и на развој одређених врста криминалитета. Са развојем друштва, дошло је до развоја технике и технологије што је самим тим отворило врата, за чињење нових врста кривичних дела. Константни развој, и доступност допринео је све већем коришћењу компјутера, као и њиховом глобалном повезивању, што доводи до све веће изложености нападима. Појединци, као и организоване групе, су у време компјутеризације пронашли нове начине да противправно за себе или друге приграбе новчана или друга средства.

Последице ове врсте криминалитета јесу милијарде долара, а због све веће спретности и домишљатости извршиоца, стопа откривања и решавања је веома мала, самим тим можемо причати о такозваној „тамној бројки".

Због константног унапређења овог криминалитета, законодавним органима је тешко да прецизно дефинишу овај појам, самим тим не постоји прецизна дефиниција, међутим можемо извући пар дефиниција.

„Компјутерски криминалитет представља друштвеноопасну појаву за чије се остварење учинилац користи знањима компјутерске технологије , тако што се компјутерски систем схваћен у најширем смислу (хардвер, софтвер, њихово јединство; један комппјутер или мрежа компјутера) користи као средство или као објекат криминалног напада, или и једно и друго"[1]

Према неким интернационалним организацијама, компјутерски криминалитет нема јасну дефиницију, али се може прецизније одредити тако што ће се раставити две врсте криминалитета и то:

- Напредни компјутерски криминалитет (високотехнолошки)- софистицирани напади усмерени на компјутесрки хардвер или софтвер
- Криминалитет извршен уз помоћ компјутера- традиционалне врсте криминалитета, користећи компјутер (тероризам, финансијски криминалитет)[2]

[1] Симоновић, Б. *Криминалистика*, Крагујевац, 2004, стр. 665
[2] INTERPOL- https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime приступљено 15.05.2018.

2. Карактеристике компјутерског криминалитета

Свака врста кривичног дела се разликује од осталих по одређеним карактеристикама, на основу којих и кривична дела добијају пропадност. Да ви разумели разлику компјутерског криминалитета, неопходно је сагледати пта је то што га одликује.

Компјутерски криминалитет, један од новијих врста криминалитета, разликује се од осталих врста по својим специфичностима, у које спадају:

- Једна од првих карактеристика јесте, динамика развијања овог криминалитета. Она зависи од компјутерског система, међутим због потреба друштва, овај систем је у константном развоју, што омогућује извршиоцима кривичног дела, константну примену нових знања, примену нових, развијенијих делова компјутера.
- Просторна и временска основа. Карактеристично за ову врсту криминалитета јесте да извршиоц не мора бити на месту извршења кривичног дела, шта више, извршиоц може бити на сасвим другом крају планете, једино што је њему потребно јесте приступ компјутерском систему. Кривично дело није везано за само једно место, извршиоц може извршити истовремено велики број кривичних на различитим местима, са такође велике удаљености. Осим просторне, и временски се овај облик криминалитета разликује од осталих. Специфичност је да због брзине компјутерског система, за извршење кривичног дела је довољан неки део секунде, као и да у једној секунди, може се извршити и неколико хиљада кривичних дела.
- „ Тамна бројка“- [3]веома битна карактеристика јесте и велики број неоткривених кривичних дела. Пре свега због умећа извршиоца, као и брзине напада, велики број жртава није ни свестан да је био мета оваквог напада. Осим тога , велики број људи ни не жели да пријави овакво деловање, или из разлога што мисли да је банално, или из разлога што то желе сакрити јер им може донети лош публицитет.
- Оно што је битно напоменути јесте и лош законодавни приступ овом проблему, веома мала пажња је усмерена на ову врсту криминалитета, и законодавни акти константно каскају за новијим варијантама ових кривичних дела.

[3] Израз „Тамна бројка“- разлика између извршених и званично евидентираних кривичних дела

3. Појавни облици компјутерског криминалитета

Не постоји јединствена форма у којој се ова врста криминалитета јавља. Као и сваки други криминалитет, тако и компјутерски има неколико облика у којима се може срести.

Постоји већи број подела, сваки теоретичар на различити начин и кроз разичите параметре сагледава ову врсту криминалитета, међутим подела коју ћу ја узети за примерну јесте она типологија коју је дао Кривични законик Републике Србије.

Законик ову врсту криминалитета сврстава у Кривична дела против безбедности рачунарских података, где пре свега укључује следећа дела:

1. Оштећење рачунарских података и програма
2. Рачунарска саботажа
3. Прављење и уношење рачунарских вируса
4. Рачунарска превара
5. Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података
6. Спречавање и ограничавање приступа рачунарској мрежи
7. Неовлашћено коришћење рачунара или рачунарске мреже
8. Прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података

1.1.Оштећење рачунарских података и програма[4]

Под овом врстом компјутерског кривичног дела подразумева се свако неовлашћено брисање, измена, оштећење, прикривање или на други начин чињење неупотребљивим рачунарских података или програма. Законодавац је предвидео за ово кривично дело основан и два тежа облика.

- Ко неовлашћено избрише, измени, оштети, прикрије или на други начин учини неупотребљивим рачунарски податак или програм казниће се новчаном казном или затвором до једне године.

[4] Члан 298. Кривични законик Републике Србије, *Службени Гласник* бр. 85/2005

- Први тежи облик се састоји ако је основни облик проузроковао штету у износу који прелази четристопедесет хиљада динара, а учинилац ће се казнити затвором од три месеца до три године.
- Други тежи облик се састоји ако је основни облик проузроковап штету у износу који прелази милион и петсто хиљада динара, а учинилац ће се казнити затвором од три месеца до пет година.

Допунски став се састоји да ће се уређаји и средства којима је учињено ово кривично дело, одузети, међутим ако су у својини учиниоца.

1.2.Рачунарска саботажа[5]

Ово кривично дело подразумева да свако ко унесе, уништи, измени, избрише, оштети, прикрије или на други начин учини неупотребљивим рачунарски програм или податак, уништи или оштети рачунар или други уређај за електронску обраду и пренос података са намером да онемогући или знатно омете поступ електронске обраде и преноса података који су од значаја за државне органе, јавне службе, установе, предузећа или друге субјекте.

Ово кривично дело има само основни облик, а последица извршења овог дела је казна затвора од шест месеци до пет година.

1.3.Прављење и уношење рачунарских вируса[6]

Кривични законик Републике Србије предвиђа казну за извршиоце овог дела које обухвата дела прављења рачунарског вируса у намери његовог уношења у туђи рачунар или рачунарску мрежу. Ово дело има основни и тежи облик.

- За основни облик је предвиђена новчана казна или затвор до шест месеци
- Тежи облик се састоји уколико је извршењем основнох дела проузрокована штета, а предвиђена је новчана казна или затвор до две године.

Законик предвиђа да ће средства којима је учињено кривично дело бити одузета.

[5] Члан 299. Кривични законик Републике Србије, *Службени Гласник* бр. 85/2005
[6] Члан 300. Кривични законик Републике Србије, *Службени Гласник* бр. 85/2005

1.4.Рачунарска превара[7]

Рачунарска превара предвиђа кривично гоњење за оно лице које унесе нетачан податак, пропусти уношење тачног податка или на други начин прикрије или лажно прикаже податак и тиме утиче на резултат електронске обраде и преноса података у намери да себи или другом прибави противправну имовинску корист и тиме другом проузрокује имовинску штету. Састоји се од основног облика, два тежа као и привилеговани облик.

- Основни облик овог кривичног дела предвиђа за учиниоца новчану казну или затвор до 3 године,
- Први тежи облик постоји уколико је овим кривичним делом настала штета која прелази износ од четристопедесет хиљада динара, а учинилац ће се казнити затвором од једне до осам година,
- Други тежи облик постоји уколико је овим кривичним делом настала штета која прелази износ од милион и петсто хиљада динара, а учинилац ће се казнити затвором од две до десет година,
- Привилеговани облик се састоји уколико је циљ овог дела само наношење штете другоме, а казна је новчана или затвор до шест месеци.

1.5.Неовлашћени приступ заштићеном рачунару, рачунарксој мрежи и електронској обради података[8]

Основни став овог кривичног дела се на лице које кршећи мере заштите, неовлашћено укључи рачунар или рачунарску мрежу, или неовлашћено приступи електронској обради података. Постоји основни и два тежа облика.

- Учинилац основног облика казниће се новчаном казном или затвором до шест месеци,
- Први тежи облик се састоји уколико се сними или употреби податак добијен коришћењем основног облика, а предвиђена је новчана казна или затвор до две године,

[7] Члан 301. Кривични законик Републике Србије, *Службени Гласник* бр. 85/2005
[8] Члан 302. Кривични законик Републике Србије, *Службени Гласник* бр. 85/2005

- Други тежи облик је састоји уколико је применом основног облика дошло до застоја или озбиљног поремећаја функционисања електронске обраде и преноса података или мреже, или су наступиле друге тешке последице, а учинилац ће се казнити затвором до три године.

1.6.Спречавање и ограничавање приступа јавној или рачунарској мрежи[9]

Ово кривично дело односи се на лице које неовлашћено спречава или омета приступ јавној рачунарској мрежи. Има основни и тежи облик.

- Основни облик је кажњив новчано или затвором до једне године,
- Тежи облик се састоји уколико га изврши службено лице у вршењу службе и казниће се затвором до три године.

1.7.Неовлашћено коришћење рачунара или рачунарске мреже[10]

Ово дело се односи на она лица која неовлашћено користе рачунарске услуге или рачунарску мрежу у намери да себи или другом прибави противправну имовинску корист. Предвиђена казна за ово кривично дело је новчана или затвор до три месеца. Карактеристика овог кривичног дела је да се предузима по приватној тужби.

1.8.Прављење,набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података[11]

Основни став се односи на она лица која производе, продају, набављају ради употребе, увозе, дистрибуирају и на други начин стављају на располагање:

- Уређаје и рачунарске програме пројектоване или првенствено у сврхе извршења неког кривичног дела из члана 298. До 303. Кривичног законика Републике Србије,
- Рачунарске шифре или сличне податке путем којих се може приступити рачунарском систему као целини или неком његовом делу са намером да буде употребљен у извршењу неког од кривичних дела из члана 298. До 303. Овог законика, казниће се затвором од шест месеци до три године.

[9] Члан 303. Кривични законик Републике Србије, *Службени Гласник* бр. 85/2005
[10] Члан 304. Кривични законик Републике Србије, *Службени Гласник* бр. 85/2005
[11] Члан 304а. Кривични законик Републике Србије, *Службени Гласник* бр. 85/2005

- Лице које поседује нека од средстава овог члана у намери да их употреби у сврху извршења неког од кривичних дела из члана 298. Дод 303. Овог законика, казниће се новчаном казном или затвором до једне године.

4. Законска регулатива

Осим Кривичног законика, који је одредио поделу компјутерског криминалитета, постоје још неки закони и регулативе који се баве овом тематиком, како међународне тако и закони Републике Србије:

- Резолуција ОУН из 1990[12]
- Препорука ОЕБС-а из 1985[13]
- Конвенција Савета Европе, Конвенција о високотехнолошком криминалу[14]
- Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала[15]

1.1.Законска основа Републике Србије

Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала. Овај закон је донет 2005 године, и важи за главну регулативу, која даје смернице о борби против компјутерског криминалитета.

Овим законом се одређују све активности у вези са компјутерским криминалитетом, од којих су најбитнији организација, надлежност и овлашћење посебних организационих јединица државних а све у циљу откривања, кривичног гоњења и суђења за кривична дела одређена овим законом.

---

[12] ОУН резолуција бр A/RES/45/121 http://www.un.org/documents/ga/res/45/a45r121.htm приступљено 24.06.2018

[13] OSCE препорука број P(85) https://polis.osce.org/node/4651 приступљено 24.06.20178

[14] Конвенција Савета Европе о високотехнолошком криминалу, https://www.mpravde.gov.rs/files/KONVENCIJA%20O%20VISOKOTEHNOLOSKOM%20KRIMINALU.doc приступљено 23.06.2018

[15] Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала- https://www.paragraf.rs/propisi/zakon_o_organizaciji_i_nadleznosti_drzavnih_organa_za_borbu_protiv_visokotehnoloskog_kriminala.html приступљено 22.06.2018

Међутим да би знали о чему је овај закон, пре свега морамо дефинисати појам високотехнолошког криминала, што је овај закон сам по себи дефинисао, а на следећи начин „ високотехнолошки криминал[16] представља вршење кривичних дела код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже, рачунарски подаци као и њихови производи у материјалном или електронском облику“.

Како би лакше разумели дату дефиницију, законодавац се потрудио да нам прецизније дефинише неке појмове од којих су следећи:

Рачунарски податак[17]- свако представљање чињеница, информација или концепта у облику који је подесан за њихову обраду у рачунарском систему, укључујући и одговарајући програм, на основу кога рачунарски систем обавља своју функцију.

Рачунарска мрежа[18]- скуп међусобно повезаних рачунара, односно рачунарских система који комуницирају размењујући податке.

Рачунарски програм[19]- уређен скуп наредби који служе за управљање радом рачунара, као и за решавање одређеног задатка помоћу рачунара.

1.2.Међународни третман компјутерског криминалитета

Велики број међународних организација се бави овом тематиком, међутим ја ћу сагледати став Интерпола,[20] као најглобалније антикриминалне организације.

Интерполов став у вези са овом врстом криминалитета јесте глобална борба како би се истребио, као и кривичних дела повезаних са њим.

Главне активности Интерпола:

- Истражне компјутерске радње

---

[16] Министарство Унутрашњих Послова Републике Србије http://www.mup.gov.rs/wps/portal/sr/gradjani/saveti/visokotehnoloski%20kriminal/!ut/p/z0/fY6xDoIwFEV_RQdG8woqwbFxINEQV-xCSq3waG1LqSh_bwdXne65ycnNBQY1MMNn7HhAa7iO_cry5nKo8rQk2bnYkZTQnJYF2RdZmW7hBOy_EBdwGEdGgQlrgnwHqN2z1SgasXjUERLirJDB8IR0nt8GbjAhE59liDnjZJUNsjdW20nhSnl84Pdb5qtj1QFzPPQbNHcL9W_fKdYuL7r-AIS9X0w!/

[17] Члан 112. Кривични законик Републике Србије, *Службени Гласник* бр. 85/2005

[18] Ibid.

[19] Ibid.

[20] Interpol- Internacional Police- Међународна полицијска организација

- Компјутерска анализа
- Дигитална форензика
- Иновација и претрага
- Развој активности
- Јачање на националном нивоу.

Интерпол ради на развоју дугогодишњих програма супротстављања компјутерском криминалу, како би кроз оснаживање сарадње земаља успели да сузбију криминал на међународном плану. Неки од тих програма јесу:

- ASIAN Cyber Capacity program (2016-2018)
- Cybercrime capacity building project in Latin Amerika and Caribbean
- Dark net and Cryptocurrencies working group

Неке од акција Interpol-a са којима је упозната јавност јесу:

1. Операција ACES 2015 [21] - координирана акција против онлајн клађења и инатернет превара. Државе које су учествовале у овој акцији јесу Камбоџа, Кореја, Филипини, Тајланд и Вијетнам. Резултати акције јесу више од 48 ухапшених, више од 100 комада електронских средстава заплењено, како компјутера, усб дискова и мобилмних телефона, два интернет центра су угашена након пријаве преваре уе износу веће, од 200,000 долара.
2. Операција Simda botnet 2015[22]- Активност која је успела да зарази више од 770,000 компјутера широм света. Главни центар координирања је био у Луксембургу, а акција је била усмерена против штетног програма који је прикупљао информације из компкјутера корисника, као што су банковне шифре, лични подаци.

[21] Interpol https://www.interpol.int/Crime-areas/Cybercrime/Operations/Operation-Aces приступљено 16.07.2018

[22] Interpol https://www.interpol.int/Crime-areas/Cybercrime/Operations/Simda-botnet приступљено 16.07.2018

II. ТЕРОРИЗАМ

1. Увод

Тероризам представља појаву својствену друштву. Када то кажемо не мислимо да је саставни део друштва, без кога оно не може да функционише, већ то да је кроз историју тероризам био појава која је утицала на доношење великог броја одлука које су одговорне за постојеће стање друштва.

Реч тероризам се у данашњем схватању користи од 1794 године, након пада вође Француске револуције Максимилијана Робеспјера.[23]

Појмовно одређење које ће бити универзално је немогуће донети, јер константна промена тероризма, нападање нових вредности, нови начини извршавања, нове циљне групе, не иду томе у корист, јер би једна дефиниција била преобимна.

Кроз историју је циљ проучавања великог броја научника и безбедносних фактора.

Схватање појма се мењало кроз историју, како се друштво развијало, тако је постојала могућност за њено боље разумевање.

Према запажањима неких теоретичара, „ већина површно посматра тероризам као друштвену појаву, прилагођавајући дефиницију сопственим интересима или интересима група које заступају“[24].

Терористичка деловања, изазивајући патњу друштва и желећи да својим деструктивним понашањем утичу на политичку елиту сваког друштва, која доноси битне одлуке, битно су утицале на савремено схватање безбедности. Велики изазови су захтевали нове модалитете борбе, како би друштво стало на крај оваквом изнуђивању одлука, и онемогућавању довођења становништва у опасност.

Одликујући се великим бројем карактеристика, представља једну од најкомплекснијих појава којима се друштво бави, односно које је погађају. Својом структуром и организованошћу, односно њеним проучавањем у овом раду, видећемо да она није проста организација која је пуким случајем дошла на то место које заузима, већ да је то нешто сасвим супротно.

---

[23] Mannik. E. “Terrorism: its past, present and future Prospects”, пдф https://www.ksk.edu.ee/wp-content/uploads/2011/03/KVUOA_Toimetised_12-M%C3%A4nnik.pdf приступљено 10.09.2018

[24] Стајић. Љ. *Основи система безбедност,* Нови Сад, 2008, стр 265

Међутим иако је тероризам везан за све друштвене сфере, ипак можемо га повезати са политичким деловањем, међутим иако се тако повезује, сагледаћемо који су то социо-економски и други фактори који утичу на деловање организације и приступање њој.

Сагледаћемо тероризам као појаву, односно појаву која је својствена садашњем, модерном друштву.

2. Појам

Као што је већ наведено у уводу овог поглавља, појам тероризма[25] је веома комплексно одредити, због великог броја карактеристика, дефиниције се могу доносити комбиновањем свих њих и стварањем своје слике о тој теми. Самим тим, сваки аутор може на основу својих схватања и уверења доносити своју дефиницију.

Неке од прихваћенијих дефиниција у нашој литератури јесу: „У најширем политичком смислу, тероризам је метод политичке борбе за коју је карактеристична систематска употреба насиља ради застрашивања противника и сламања његовог отпора“.[26]

„Тероризам је плански акт насиља који предузимају одређене друштвене групе с циљем очувања или освајања власти, односно тероризмом се с правом назива само онај терор, који у свом бићу садржи социјално-психолошку односно политичку компоненту“,[27] по Младену Милошевићу.

Дефиниција коју је дао Димитријевић сагледавајући елементе тероризма састоји се у томе да „Терористички акти су по правилу насилни, они су политички мотивисани, потенцијалне жртве ових аката немају никакве везе са политиком, и коначно, циљ оваквих дела је да изазову осећање страха и несигурности“.[28]

Што се тиче дефиниције која прецизније повезује теороризам са друштвом, ту дефиницију је дао Игњатовић „облик политичког криминалитета којим се путем непредвидивог насиља тежи остварити промене у друштву“.[29]

---

[25] Тероризам потиче од латинске речи La terre, што значи изазивање страха.
[26] Савић А, *Основи државне безбедности*, Београд, 1998, стр. 85
[27] Милошевић, М, *Тероризам као кривичноправна категорија*, Београд, Безбедност, број 4/1988 стр 341.
[28] Димитријевић, В, Стојановић Р, *Међународни односи*, Службени лист СРЈ, Београд 1996, стр 340-341
[29] Игњатовић. Ђ. *Криминологија*, Београд, 2007, стр 283

Што се иностраних дефиниција тиче, Department of State [30] је 1988. године сагледало да постоје чак 109 дефиниција тероризма. [31]

Дефиниција Oxford Concise Dictionary of Politics дефинише тероризам као „ термин око којег нема слагања међу владама нити у академским анализама, готово увек коришћен у погрдном смислу, најчешће да би се описали акти угрожавања живота од стране политички мотивисаних самоорганизованих група“.[32]

С обзиром на све ове дефиниције, и недостатак једне јединствене, можемо сагледати комплексност читаве области тероризма, и муку која академска заједница има са њеним сагледавањем и проучавањем.

3. Карактеристике

Разговарајући и анализирајући све дате дефиниције тероризма, оно што је неизоставни део јесте одређивање, односно проналажења једног својства који ће их све повезати. То својство јесте ПОЛИТИЧКИ ЦИЉ.

Читајући све ове дефиниције, оно што је мени „запало за око“ јесте коначни циљ, односно због чега се уопште говори, због чега постоји тероризам. Политички циљ је одговор. О њему можемо говорити у смислу, тероризам ради поделе територије, ради освајања тероторија, жеља за сменом власти, жељом за исказивања неповерења и мржње према политичким вођама.

Сагледавши све тадашње дефиниције State Departmenta, Schmid и Jongman дошли су до закључка да су 22 елемента који се најчешће у њима помињу и могу се сматрати одређеним смерницама и карактеристикама:

-употреба насиља;

- политичко насиље;

- изазивање страха или ужаса;

-претња, психолошки ефект и очекиване реакције;

-разликовање жртава и шире мете напада;

[30] Department of State- Министарство иностраних послова Сједињених Америчких Држава
[31] Bruce. G. *Definition of terrorism Social and Political effect*, 2013
[32] Mc Lean. I. Mc Millan. A. *The Concise Oxford Dictionary of Politics,* 2003 str. 81

-циљано планирано и организовано деловање, метод борбе,стратегија, тактика;

-кршење прихваћених правила;

-одсуство хуманитарних разлога;

-уцена, принуда и навођење на послушност;

-жеља за публицитетом; самовоља, безличност, насумичност, одсуство дискриминације;

-жртве цивили, не-борци, лица без везе са самом ствари;

-застрашивање ;

- невиност жртава;

-извршилац, група покрет или организација;

-симболичка природа;

- непредвидљивост појаве насиља;

- тајност и прикривеност, понављање кампања насиља;

-криминални, злочиначки карактер;

-захтеви постављени трећим странама. [33]

Још неке од карактеристика јесту да је то забрањено дело, сваки акт тероризма је дело против правног поретка и као такав је најстроже забрањен и кривично кажњив у свим законодавствима; акт обавештавања, односно акт достављања одређене поруке својим делима.

4. Узроци

Као чиниоце који доприносе остваривању ових кривичних дела можемо издвојити одређене услове, неке од њих можемо везати за средину, док су неке својствене личности особа који приступају терористичким актима.

Прве факторе можемо дефинисати као социо-економске и политичке, док што се других тиче можемо речи да су психолошки.

Социо-економски и политички узроци, огледају се у томе да лица која приступају терористичким групацијама, то чине са тежњом да промене свој живот, да га побољшају

[33] Schmid. A. Jongman. J. *Political terrorism: a new Guide to Actors, Authors,Cencepts, Data Bases, Theories and Literature,* New Jersey, 1988, str 5-6

тако што ће своје незадовољство исказати на веома бруталан начин, који га не дотиче, међутим то ћемо анализирати у психолошком делу.

Ти фактори јесу:

- Сиромаштво
- Неприпадност друштву
- Политичко незадовољство
- Нефункционисање друштва(његових институција)
- Мито и корупција

Иако сви ови фактори могу говорити да су то друштвено маргинализоване групе, неки показатељи говоре да међу припадницима терористичких организација има и образованих и успешних људи, инжињера, физичара и других научника.

Под психолошким факторима бих анализирао факторе везане за личност особе која жели да изврши терористички акт.

Међути оно што је битно напоменути, је да припадници ових групација нису обавезно и лица са психичким поремећајима. Post I Sprinzak, су спровели истраживање које је показало да лица који су били припадници Ал каиде [34]су људи без поремећаја[35].

Неки од фактора по Reich-у, јеси: [36]

- Неправда
- Понижење
- Злостављање

Особа која је жељна да изврши терористички акт је особа која поред могућности лабилнијег ума, може доћи у тај стадијум пре свега због начина живота, неправда која му је нанесена у друштву, понижење и злостављање које га је годинама пратило, кућно малтретирање, односно одрастање у нездравој породици, све то може водити поремећају личности и сва та трауматична искуства, могу утицати на особу да друштво схвати сасвим другачије од друштвено прихватљивих вредности.

[34] Ал Каида- Међународни Савез Исламских Терористичких Организација

[35] Post. J. Sprinzak. E. Denny. L. *The terrorist in their own words, Interviews with 35 incarcerated Middle Easter Terrorist, Terrorism and Political Violence*, 2003, стр -171-184

[36] Reich, W, *Understanding Terrorist behavior, the limits and opportunities of psychological Inquiry, Orgins of Terrorism, Psychologies, Ideologies, Theologies, States of Mind*, New York, 1990, стр 270

5. Класификација

Подела тероризма коју ћу узети као примарну за израду овог рада, је подела Љубомира Стајића, који тероризам класификује у следеће делове:

- Националистички тероризам
- Религиозни тероризам
- Идеолошки тероризам
- Емигрантски тероризам[37]

Националистички тероризам је она врста тероризма која се пре свега изводи у земљама које нису стабилне на политичком нивоу, односно чија се тероторија на неки начин, било путем становништва, било путем аутономије састоји од неколико делова, па до терористичких акција долази од стране националистичких организација, који оваквим деловањем желе да се изборе за политичку независност свог дела тероторије. Ове групе се зову и сепаратистичке.

Религиозни тероризам је она врста где до акција долази од стране религиозних фанатичких група, које због слепог погледа на своју веру, у циљу остваривања већих религиозних права, према одређеним групацијама, политичкој елити, или другим религиозним групама, врше терористичка дела.

Идеолошки тероризам јесте онај тероризам, где се терористички напади користе као средство за темељне политичке промене у друштву, односно смену власти.

Емигрантски теороризам је она врста где се као извршиоци терористичког чина налазе емигранти, који због свог лошег статуса, или исказивања незадовољства у земљу домаћина, желе да на овај начин издејствују промене свог положаја.

[37] Стајић. Љ. *Op. cit*. стр. 271-272

6. Република Србија у борби против тероризма

Уколико узмемо да је као основни објекат напада сваког терористичког акта држава, морали би смо да сагледамо који су то механизмо одбране држава, односно борбе против тероризма. Као пример ћу узети Републику Србију.

Република Србија, уколико гледамо скоријe историју, има велики број терористичких напада усмереног на своје становништво, и својих безбедносних снага.

Као врсту тероризма који је у нашој земљи на снази, јесте националистички тероризам, који се спроводи на Косову и Метохији. Косово и Метохија, као аутономна покрајина, била је територија са мешовитим становништвом, Српским и Албанским, до терористичких акција је дошло због сепаратистичког захтева Албанаца да се одвоје од остатка Србије.

Како би се наша држава на неки начин борила са тероризмом, донет је закон у складу са Уставом.

Ово кривично дело спада у Кривична дела против уставног уређења и безнедности Републике Србије, и налази се у члану 312. Кривичног законика.

Теоризам[38]- „Ко у намери угрожавања уставног уређења или безбедности Србије изазове експлозију, пожар или предузме другу општеопасну радњу или изврши отмицу, узимање талаца или самовољно лишавање слободе неког лица или други акт насиља или прети предузимањем какве општеопасне радње или употребом нуклеаног, хемијског, бактериолошког или другог општеопасног средства и тиме изазове осећање страха или несигурности код грађана“.

Казна која је предвиђена за ово кривично дело је од пет до петнаест година.

Осим закона, и неки органи се баве овим проблемом. Безбедносне структуре, састоје се од велике организационе пирамиде. Која се пре свега састоји из следећих делова:

- Председник Републике
- Савет за националну безбедност
- Службе безбедности

[38] Члан 304а. Кривични законик Републике Србије, *Службени Гласник* бр. 85/2005

- Министарство унутрашњих послова
- Министарство одбране

Ови субјекти, пре свега у корелацији једни са другима, поштовањем одређених процедура, сачињавањем стратегија, планова, извршењем тих истих процедура, су одговор тероризму наше државе.

III. КОМПЈУТЕРСКИ ТЕРОРИЗАМ

1. Увод

Савремени методи ратовања, који прелазе границе Компјутерског криминалитета Тероризма, које сам у овом мастер раду узео да обрадим јесте Компјутерски тероризам. Због значаја и све већег утицаја на друштво, сматрам да је једна од битнијих тема, безбедносног система, што боље разумевања ове теме, где ћу пробати да сагледавањем њених ситнијнијих делова на неки начин сагледам на што бољи начин њену природу.

2. Појам

Након покушаја да сагледамо шта је то Тероризам, и Компјутерски криминалитет, у мастер раду бих пробао да из ова два појма изведем значење њиховог споја, односно Компјутерског тероризма.

Као што смо раније видели, и за прве две теме, због њихове комплексности, не постоји једна прецизна, и опште прихваћена дефиниција, тако да се то пренело и на овај појам.

За компјутерски тероризам, као део тероризма, можемо рећи да је још комплекснији појам од тероризма, јер као што смо видели појам тероризма је неодређен у потпуности, па се то пренело и на овај подпојам.

Што се самог термина тиче, сматра се да га је први употребио Barry Collin[39], 1980-тих година.

Једна од дефиниција јесте она коју је дао ФБИ[40]-јев агент Mark Pollitt[41], у којој говори да се ради о“ предумишљајном, политички мотивисаном нападу на информације,

[39] Collin. B., *“The Future of Cyberterrorism*”, 1997, стр 15-17

компјутерске системе, компјутерске програме и податке који резултују насиљем против неодговарајућих група, од стране националних или тајних група“.

Једна од организација која има своју дефиницију компјутерског тероризма је и НАТО [42] -„ компјутерски напад, коришћењем или искоришћавањем компјутера или комуникацијског система, како би изазвали довољно уништавања,да би послигли свој идеолошки циљ, а то је застрашивање друштва“.[43]

Бивши министар одбране Сједињених Америчких Држава, John Hamre[44], је у своме обраћању конгресу 1997, схвативши значај компјутерског тероризма рекао „ суочавамо се са могућношћу електронског Перл Харбура. Биће електронског напада на државе у будућности“ . [45].

Janczewski и Colarik [46] дефинишу „ компјутерски тероризам представља умишљајни, политички мотивисани напад, од стране поднационалних група, тајних агената или појединаца усмерених на информације, информационе системе, програме или податке, који резултују насиљем према неодговарајућим групама“.

Bruce Hoffman [47] сматра да је компјутерски теоризам „намерно стварање и експолатација страха кроз насиље или претњом насиљем у циљу остварења политичког циља“.

На основу свих ових дефиниција, по аутору овог мастер рада компјутерски теоризам је употреба компјутера, од стране људи који поседују одређено знање, који би њиховим коришћењем желели да уз помоћ одређених активности изазову страх или осећај угрожености друштва, како би помоћу њега остварили одређене политичке или другим мотивима засноване жеље.

---

[40] FBI- Federal Biro of Investigation- Федерална служба безбедности Сједињених Америчких Држава
[41] Pollitt. M. “ *A Cyberterrorism Fact or Fancy*” ,1997, стр. 285-289
[42] NATO- North Atlantic Treaty Organization- Северно Атлантски војни савез
[43] Centre of Excellence Defense Against Terrorism, *Responses to Cyber Terrorism*, Amsteredam, 2008, str 119
[44] Decker. B. Triplet. C. “*Beijing`s Electronic Pearl Harbor*” , The Washington Times, 2011 https://www.washingtontimes.com/news/2011/nov/11/beijings-electronic-pearl-harbor/ приступљено 25.09.2018
[45] Перл Харбур- Војни рат између Јапана и Америке
[46] Janczewski. L, Colarik. A, “*Cyber Warfare and Cyber Terrorism*”, New York, 2008, стр 139
[47] Bruce Hoffman, „*Inside Terrorism“* ,New York, Columbia University Press, 2006, стр. 40

3. Карактеристике

Као и сваки облик криминалитета или тероризма, тако и компјутерски тероризам има неке своје карактеристике, које га прате у свим његовим облицима. Пре свега при одређивању да ли се ради о том делу, увек се траже те карактеристике које га ближе одређују.

Начини деловања, начини организације, извршења, средства којима је извршено, лица која га извршавају, као и циљеви, сви они се разликују и спецификују одређену врсту тероризма која се дешава, тако и за компјутерски криминаллитет ћу пробати да издвојим неке од њих, које су по мени ствари које га обележавају.

Почевши од карактеристика самог компјутерског тероризума у његовом најширем облику, могу пробати да издвојим следеће особине које га одражавају, закључујући на основу већег броја дефиниција:

- Умишљајно деловање
- Политички мотивисано
- Усмерено на изазивање страха и панике
- Коришћење компјутера
- Од стране група

Умишљајно[48] *деловање* подразумева да се компјутерским тероризмом неће нека особа случајно бавити, и неће проистићи као случајно задирање у одређене програме и сфере које могу угрозити функционисање друштва, већ ће се особа умишљајно дати у такво деловање, свесна свог понашања и опасности које произилазе из њега. О учиниоцима компјутерског тероризма ћу се бавити у каснијем делу.

Политички мотивисано, под овом карактеристиком бих могао приметити да као и код тероризма у свом основном облику, политика је веома битан фактор сваког друштва. Сва незадовољства, како због економског, социјалног или другог статуса долазе као

[48] Кривично дело је учињено са умишљајем када је учинилац био свестан свог дела и хтео његово извршење или када је учинилац био свестан да може да учини дело па је на то и пристао.- Члан 301. Кривични законик Републике Србије, *Службени Гласник* бр. 85/2005

последица лошег вођења политике, самим тим и терористи политичку елиту виде као одговорну за све проблеме друштва, и покушавају да било каквом акцијом промене њен ток, односно заокрет политике у оном смеру који њима одговара.

Једна од битнијих карактеристика јесте *изазивање страха и панике*. Становништво се неће потрести све до оног тренутка када се осети угрожено, односно када могу схватити да могу постати жртве. То је схваћено и од стране терористичких организација који сматрају да је то један од најбитних фактора, односно циљ који морају испунити како би њихов главни циљ могао бити остварен. Њихови напади јесу они напади који ће друштву показати да иако се осећа безбедно, постоје одређени пропусти који ту безбедност може довести у питање. Оног тренутка када се друштво почне осећати угрожено, тог тренутка се јавља сумња у политику своје земље и поставља се питање „ да ли је политика моје земље исправна“, као и „ да ли сам безбедан“, што може навести друшво на одређене акте, који некада иду у корист терористичким организацијама. Један од првих примера када се постављало питање компјутерског тероризма, као и угрожености становништва, јесу компјутерски напади да амбасаде Шри Ланке од стране терористичке групе Тамилски Тигрови[49], када је стигло преко 800 е-маил-ова дневно у периоду од 2 недеље са садржином „Ми смо Интернет Црни тигрови и ово радимо да уништимо вашу комуникацију“.[50], што је довело до несигурности особља амбасада, што се сматра једним од првих терористичких напада помоћу компјутера.

Последња карактеристика коју бих издвојио јесте од *стране терористичких група*. Терористички напад је могуће извршити и самостално, међутим у пракси се види да је ског свака акција извршена под покровитељством одређене организације, Без обзира да ли је организација учествовала у извршењу или не, већина појединаца који ово раде, раде то у име одређене групе, следећи њихову идеологију и подржавајући њихове ставове, самим тим их можемо стврстати као њихове чланове.

[49] Тамилски тигрови-Терористичка организација у Шри Ланки
[50] Denning.D,”*Activism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*”, Georgetown University,2000, pdf http://www.iwar.org.uk/cyberterror/resources/denning.htm

4. Подела компјутерског тероризма

Желећи да што више појаснимо ову појаву, поред дефинисања и издвајања његових карактеристика, неопходно је и направити неке разлике унутар самог компјутерског криминалитеа. Сваки облик компјутерског тероризма садржи одређене специфичности, које га разликују, макар и минимално од других. Сваки од ових облика на различите начине угрожава систем и друштво.

Компјутерски тероризам можемо поделити на основиу неколико критеријума, и то:

- На основу лица који га врше: појединац или група
- Према врсти акције: Хибридни(пропаганда, прикупљање чланова, прикупљање средстава, прикупљање података, комуникација, тренинг и планирање терористичких акција), прави компјутерски тероризам(деструктивни и омаловажавајући)[51]
- Према циљевима: не циљани, циљани[52]
- Према форми појављивања: психички, синтатички и семантички [53]

Подела према *лицима* који га врше: На основу броја лица, односно да ли лица делују самостално или у сарадњи са другим лицима, имамо:

1. Појединац- следећи своје идеолошке, политичке, националистичке и религиозне ставове, односно због могућношћу одређене болести, жели да изазове патњу и страх друштва.
2. Група- пре свега организација која нема неки прости план, већ плански организовано деловање и неки већи циљ који жели да оствари.

Према Michael-u Vatis[54], постоје четири врсте потенцијалних извршилаца:

1. Припадници терористичких група- замењујући конвенционално оружје новим, компјутерским нападима,

---

[51] Zerzi. M. "*The treat of cyber terrorism and recommendarion for coyntermeasures*", C.A. Perspectives on Tunisia No. 04-2017

[52] Littlefield. R. "*Cyber Terrorism: understanding and preventing acts of terror within our cyber space*",2017 https://littlefield.co/cyber-terrorism-understanding-and-preventing-acts-of-terror-within-our-cyber-space-26ae6d53cfbb приступљено 10.09.2018

[53] S. Baldi, E. Gelbstein, J. Kurbalija "*Hacktivism, cybrr-terrorism and cyberwar*", Diplofoundation, Malta, 2003

[54] Vatis. M. , „*Cyber attacs during The War On Terrorism*", Hanover,2001 http://www.ists.dartmouth.edu/docs/cyber_a1.pdf

2. Симпатизери терористичких група- самостални активисти који пре свега то раде из убеђења, односно пратећи идеологију терористичке групе за коју сматра да је у праву,
3. Нације или државе- подржавајући циљеве одређених терористичких група, пре свега у другој држави,
4. Лица која то раде због узбуђења.

Подела према *врсти активности*: У зависности какав се компјутерски тероризам предузима, односно које се активности предузимају како би се остварио, можемо говорити о:

1. Хибридно:
   - Пропаганда- Интернет платформе терористичке организације користе за ширење својих ставова, као и могућношћу да се она искористи на ај начин да би њихове ставове видео цео свет.
   - Прикупљање чланова- помоћу пропаганде, односно чињењем доступним својих идеја, ово је један од начина на који организације врбују нове чланове у своје редове који ће учинити да бројчано јача организација има јаче нападе.
   - Прикупљање средстава- као и прикупљање чланова, и прикупљање средстава делује на истом принципу, чињењем доступним идеологије своје групе, одређени симпатизери не желећи да улазе толико далеко да би били извршиоци акција, једноставно донирајући одређена средства групи, потпомажу њено постојање и функционисање.
   - Прикупљање података- на тај начин што су на интернету доступне скоро све информације, њиховим пажљивим прикупљањем и анализирањем може се доћи до тога која је инфраструктура најрањивија или је друштво најосетљивије на одређену ствар, која може послужити код планирања акција.
   - Комуникација- један од начина комуникаиције јесте преко одређених интернет платформи, односно софтверских програма који омогућују шифровано дописивање одређених лица, без могућношћу приступа нежељених лица.

- Тренинг и планирање- могућност тренинга јесте могућ преко такозваног Мрачног интернета[55], где се могу достављати упутства, оносно све информације везане за активност организације и подучавање о истом, као и сва договарања.

Пример: Сагледавши литературу, може се доћи до закључка да је ова врста тероризма најзаступљенија, у томе се огледа и константна активност терористичких организација. Пропаганда, регрутација, прикупљање средстава, најзаступљенији су облик тероризма.

Једни од најзаступљенијих у овим активностима јесу Хезболах и ИСИС[56]. Што се Хезболаха тиче, још 1998. године је имао три интернет адресе, www.moqawama.org, за оправдања напада на Израел, www.Hiybullah.com , централна канцеларија, и www.almana.com.lb , адреса за информисање. [57]

Што се ИСИС-а тиче, можемо рећи да су се они у потпуности окренули интернет ратовању. Са новијом експанзијом насиља, оно што су припадници ове групе кренули да раде јесте постављање на интернету видео клипова са садржинама претњи, захтевима, па и убијањима заробљеника. За ове видео клипове можемо рећи да су потпуно успели у својој намери, цео свет је згрожен оваквим поступцима, уливен је страх становништву, што је и примаран циљ овакве врсте тероризма.

2. Директни напади- извршење акција, тј. напада на циљеве, и који могу бити:
   - Деструктивни- Предузимање напада на компјутерске системе, са циљем њиховог уништавања и њиховом дестабилизацијом.
   - Омаловажавајући- подразумева нападе на сајтове битних инфраструктура, чинећи да се систем осети угрожен и понижен немогућношћу да се заштити.

Пример: Један од најпознатијих напада јесте Stuxnet напад 2010. изведен помоћу вируса. Сумња се да је све почело кроз преносни драјв неког од радника, када је у систем

[55] Дарк нет- Кримогени део Интернета
[56] ИСИС- Исламска држава Ирака и Сирије
[57] Veerasamy. N. "*Motivation for Terrorism*", South Africa, 2010
https://www.researchgate.net/publication/46175365_Motivation_for_cyberterrorism приступљено 15.09.2018

убачен вирус. Развијајући се и размножавајући, дошло је до тога да је црв успео да уђе у Natanz нуклеарну установу у Ирану. Нуклеарна установа се сматра критичном инфраструктуром сваког друштва који је поседује, самим тим се не може наслутити шта би се могло десити да је систем преузет од стране неког члана терористичке организације. До откривања црва је дошло тек онда када је било неких нелогичности у функционисању процеса, при чему је ангажована фирма из Белорусије која је анализом система открила уљеза. Иако нису изашли са званичним саопштењем, сумња се да је црв уништио 984 уранијумске центрифуге. Налагодавци нису до данас познати, међутим због противљења Сједињених Америчких Држава и Израела, Иранском нуклеарном програму, сумња се да су они ти.[58]

Према *циљевима* напада: Разлика се може сагледати и на основу тога шта је циљ напада, да ли је одабран насумично или према строго одређеним критеријумима:

1. Не-циљани:
   - Фишинг- акција која се састоји углавном као превара, односно насумично слање лажних е-маил-ова како би се преваром прикупиле информације као што су лозинке, корисничка имена, банковни рачуни итд.
   - Лажни сајтови- креирање лажних сајтова који су као копија сајтова одређених компанија, организација, служби, где би уласком на њих кориснички компјутер био заражен и имао би се приступ његовим подацима.
   - Скенирање- случајно скенирање одређених сајтова како би се детектовали пропусти у бебедносном систему ради њиховог каснијег напада.

2. Циљани напади:
   - Циљани Фишинг- за разлику од обичног Фишинга, овде се ради о намерном слању, односно циљаној превари одређене особе како би се прикупиле њене информације.

[58] Holloway. M. „*Stuxnet Warm Attack on Iranian Nuclear Facilities"*, Standford Universiti, CA,2015, http://large.stanford.edu/courses/2015/ph241/holloway1/ приступљено 03.10.2018

- ДДОС[59] напад- ради се о намерном пренатрпавању захтева на орећени сајт или е-маил како би се он искључио до даљњег због немогућности обрађивања свих захтева.
- Дан 0- напад на софтвер и његово искоришћавање до тренутка док власник не открије ту рањивост.

Пример: Један од већих терористичких напада, десио се ове године. ДДОС напад је извршен на банкарски систем Холандије.
Напад је кренуо током викенда, и завршен је у понедељак 29. Јануара. Састојао се у ДДОС нападу на три Холандске банке, ABN AMRO, ING и RABOBANK, напад се састојао у истовременом нападу, пренатрпавајући захтевима банке, чиме је дошло до угрожавања њихових система, који су били успорени, уз оборене интернет адресе.[60]

Према *форми* појављивања имамо:

1. Психички: састоји се у нападима како би се спречила свака комуникација, односно уништио мрежни, комуникациони и рачунарски систем.
2. Синтатички: напад који се састоји у самосталном фунционисању рачунарског система, без икакве могућности и информација његовог власника о томе.
3. Семантички: састоји се у предузимању акција, односно вршењу напада како би се изазвала нека реакција, односно изазвао осећај повређености неке особе.

5. Оружје компјутерског тероризма

Терористички напади бомбама, хладним оружјем, хемијским оружјем, или неки други конвенционални начини вршења терористичких дејстава, можемо ре'и да застаревају. Како се развија друштво, тако и терористичке организације прате модерне трендове, односно користе развијену технологију.

[59] ДДОС- Distributed Deniel od Service- Напад који спречава коришћења рачунара
[60] Gunderman. D. "Incident of the Week: DDOS Attack Hits 3 Banks Simultaneoysly" Cyber Security Hub, 2018 https://www.cshub.com/attacks/news/incident-of-the-week-ddos-attack-hits-3-banks приступљено 01.10.2018

Конвенционално оружје коришћено у савременом свету постаје замењено другим, модернијим, технолошки напреднијим, који уз помоћ компјутера могу имати већи и разорнији ефекат од бомби.

Што се средстава, односно оружја, у рачунарском смислу, које се примењује ради извршења компјутерског тероризма користи, можемо издвојити неке од седећих: Логичка бомба, Тројанац, Вирус, Црв.

1. Вирус- компјутерски вирус је пре свега програм који има за циљ, да попут правог вируса који зарази људски организам, зарази рачунар или рачунарски систем у коме се налази. Својствено му је да му је циљ да оштети програме, избрише фајлове, или промени одређене податке. Самостално се крећући кроз систем, може довести да рачунар буде потпуно неупотребљив. [61]

Деловање вируса се састоји у:

- Самостално посећивање одређених сајтова
- Самосталне промене почетне странице претраживача
- Самостално слање е-маилова
- Повреда хард диска
- Успоравање рада рачунара
- Покретање непознатих програма
- Самостална замена шифре.[62]

Пример: Што се вирусног напада тиче, један од скоријих напада јесте у Индији, 2017 године. Напад је извршен вирусом под именом Wannacry.

Вирус је нападао застареле Microsoft рачунарске системе, попут ХП[63]-а. Око 60% напада је извршено на компаније, док је остатак напада био концентрисан на индивидуалне кориснике. Напад вирусом се састојао у блокади система, односно онемогућавања кориснику да приступи рачунару, његовим закључавањем, до оног тренутка док не буде

[61] Weebroot https://www.webroot.com/us/en/resources/tips-articles/computer-security-threats-computer-viruses приступљено 01.10.2018

[62] Symantec employee- https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html приступљено 03.10.2018

[63] ХР- Оперативни систем

плаћена одређена свота новца. Погођени су рачунари полицијских управа, електричних дистрибуција, болница. Било је само 2 решења, или платити или изгубити податке.[64]

2. Тројански коњ- подједнако опасан као и вирус, међутим његово својство није размножавање, његов циљ је да уништи рачунарски систем у који је упао, изнутра, како би постао небрањив за нападе споља. Постоји неколико врста Тројанских коња:
   - Преузимање приступа- односно преузимање комплетног управљања рачунарским системом,
   - Слање података- уласком у систем шаље одређене информације рачунара у коме са налази кориснику који је програмирао овај вирус,
   - Уништавајући- циљ му је уништавање података рачунара у коме се налази
   - Прокси сервер- могућност коришћења свих података који долазе заједно са прокси сервер адресом на коју је пријављен корисник, лажно представљање итд.
   - ФТП(протокол за слање података)- омогућује повезивање рачунара и слање података
   - Деактивирајући- програм који прекида дејство било каквог антивирусног програма
   - ДДОС- пре свега коришћење зараженог рачунара да шаље захтеве разним серверима, који ће га пребукирати и блокирати.[65]

Пример: Осим за нападе на компаније, и приватне кориснике, постоје и компјутерски напади на државе и њене институције. Један од тих напада је био 2011. године. Извршен је Тројанским коњем.

Влада Јапана је погођена њиме, након што је један њен службеник отворио е-маил, који је дошао из Кине, која се и сматра извршиоцем. Сматра се да је пре него што су успели да се

[64] Sherpa. S. „*Cyber Attacks that Affect India in 2017*“, Gizbot, 2017 https://www.gizbot.com/internet/features/cyber-attacks-that-affected-india-in-2017/articlecontent-pf82316-046533.html Преузето 04.10.2018

[65] Beal. V. “*Trojan Horse*”, Webopedia https://www.webopedia.com/TERM/T/Trojan_horse.html Преузето 04.10.2018

ослободе штетног програма, да је он успео да узме одређене информације из система, попут корисничких имена и шифри. [66]

3. Логичка бомба- штетни компјутерски програм чији је основни циљ уништавање система у коме се налази. Програмиран је да се активира у одређеном времену или после одређених активности с циљем уништавања места у коме се налази.[67]

Пример: Још један пример напада на критичне инфраструктуре државе је напад Логичком бомбом, извршен у Јужној Кореји. Убачена бомба се састојала у уништавању целогупног система рачунара у којима се налазио. Напад је извршен 2013, а састојао се у онеспособљавању система банака и медијских кућа који је отпочео истовремено. Дошло је до гашења преноса код медија, а немогућности подизања новца, односно његовим управљањем у банкама које су погођене.[68]

4. Компјутерски црв- штетни програм чији је циљ зараза што већег броја рачунара и константно кретање кроз систем, размножавајући се на сваком могућем месту. Његов циљ јесте успоравање система или модификација података.

6. Интернет као полигон

Досадашњи начини вршења терористичких акција, разликују се од новонасталих управо због отварања нове позорнице на којима могу наступати. Са развојем технологије, дошло је до развоја нових сфера где се може применити насиље и изазвати раличито осећање код људи. Сфера која је у константном развоју, и која сваким даном отвара све више могућности за њену примену јесте Интернт.

Модернизовање терористичких организација је почело оног тренутка када су схватили да за своје циљеве није неопходно ризиковати свој живот, односно доводити

[66] Rusell.. J. "*Japanesse government hit by Chinesse Trojan Atack*:", Asia, 2011 https://thenextweb.com/asia/2011/10/25/japanese-government-hit-by-chinese-trojan-horse-attack/ приступљено 04.10.2018

[67] https://www.techopedia.com/definition/4010/logic-bomb приступљено 04.10.2018

[68] Zetter. K."*Logic Bomb Set Off Sout Korea Cyberattack*", Wired, 2013 https://www.wired.com/2013/03/logic-bomb-south-korea-attack/ Приступљено 04.10.2018

своје људе у опасност, већ улагање у њихово знање компјутерске технологије које ће им се вишеструко исплатити.

Подметање бомби, убијање, или други напади на цивиле како би се остварили лични циљеви, полако су почели да бивају замењени другим, комплекснијим али безбеднијим методама.

Коришћењем интернета као средство остваривања својих циљева, терористичке организације више нису принуђене да делују само у одређеном географском подручју, самим тим оне добијају на већем значају, јер уколико су спремне, могу се супротставити и другим групацијама, организацијама на сасвим другом крају света.

Осим проширења својих могућности, Интернет је место које знатно олакшава функционисање организације. Константна претња од откривања, праћења која може угрозити терористичку ћелију или целокупну организацију, је уз помоћ интернета сведена на минимум, јер је комуникација припадника веома олакшана, док је службама безбедности знатно теже откривање истих.

Све што је неопходно јесте знање компјутерске технологије које припадник организације мора имати како би приступом Интернету успео да оствари планове своје организације. Почевши од ширења пропаганде, регрутовање чланова, скупљање средстава, планирање, и извршење терористичких акција.

Оно што је веома привлачно терористима на Интернет мрежи јесту неке њене карактеристике који је чине идеалном за коришћење. При коришћењу сајтова, нема никакве рестрикције, цензуре која би им сметала, као и приступ тим сајтовима терористичких организација је слободан, омогућен свима.

Сагледавајући све већу употребу Интернета од стране терористичких организација бивши шеф ЦИА[69]-е за тероризам Vince Cannistraro је изјавио „Интернет комуникација је постала главна комуникација Ал Каиде [70] широм света јер је безбеднија, јефтинија и анонимнија ако сте опрезни, а ја мислим да они јесу“[71]

Што се тиче приступа Интернету и његовог коришћења, велики број терористичких организација је присутан на њему, и то са свих страна света:

[69] CIA- Central Intelligence Agency- Централна обавештајна агенција Сједињених Америчких Држава
[70] Ал Каида- Савез Исламских терористичких организација
[71] Weimann. G. “*Terror on the Internet: The New Arena, the New Challenges*” Вашингтон, 2006, стр 3-4

- Блиски исток: Хамас, Хезболах, Курдистанска радничка партија, Палестински исламски џихад;
- Азија: Ал каида, Јапанска црвена армија, Јапанска сепериорна истина, Чеченски побуњенички покрет
- Европа: Ета[72], Ира[73], Корзиканска армија
- Латинска Америка: Колумбијска национална ослободилачка партија, Сендеро Луминосо

Све оне имају и по неколико сајтова на којима се могу информисати њихови следбеници:
Хамас:
http://hamas.ps/en/
Хезболах:
https://www.moqawama.org/
http://almanar.com.lb/
Ал каида је доступна на различитим сајтовима, што самостално што у сарадњи са другим организацијама:
http://www.jihadica.com/how-do-you-become-a-member-of-al-qaeda/

Оно што је проблем, је што се ови интернет сајтови константно мењају због бежања од служби безбедности, па тако мењају своје адресе, мењају државе у којима су регистроване, као и мењајући слова алфабета у домену.
Сви ови сајтови се служе одређеном реториком, што су запазили Weimann I Weinn, Да је један од основних циљева коришћења ових сајтова оправдавање својих поступака, односно употребу насиља, као и оправдање за коришћења средства.[74]

Сагледавајући њихово оправдање на сајтовима, Tsfati, сматра да су се издвојила 3 типа ретрорике:

1. Немамо избора
2. Демонизовање супротне стране

[72] ETA- Еускади та аскатасуна- сепаратисктичка терористичка организација у Шпанији
[73] ИРА- Ирска Републичка Армија
[74] Weimann, G, Winn, C, „*The Theatre of terror*“, Longman Publication, Њујорк, 1994, стр 42

3. Теоризам је једино преостало решење.
4. Представљање групе као ненасилне[75]

Као што је и систем безбедности организован и решен да се што бољом организацијом супротстави свим врстама изазова са којима се друштво суочава, тако је и компјутерски тероризам нашао начин на који ће избегавати све препреке које му се стављају на пут. Један од начина који се користи за функционисање без сметњи јесте Дарк нет.

1.1.Дарк нет

Уколико би помислили да је сав интернет доступан свима нама, врло лако би претраживањем дошли до закључка да грешимо. Преко Интернет претраживача можемо доћи до свих информација које нас интересују, тј. Скоро свих. На основним претраживачима можемо доћи до безазлених информација којима се не може нашкодити и нанети нека штета, односно због све контроле тих обичних претраживача, веома је тешко организовати и спровести било које кривично дело.

Међутим оно што се претрагом може сазнати, да је интернет који је нама доступан, само један мали део. Велика категорија јесте Deep Web, односно дубока мрежа. Што се ње тиче, не можемо рећи да је сама по себи справљена ради извршења кривичних дела. Пре свега њена карактеристика је да је пре свега прикривена од очију нас, обичних корисника Интернета. Свака претрага преко претраживача као што су Google, Yahoo, ће се завршити приказивањем само одређених резултата претраге. Садржају Дубоке мреже се може приступити само прецизнијим уношењем тражених адреса, односно спровођењем од стране сајтова и даљом циљаном ретрагом.

Међутим терористичке организације су организованошћу и спретношћу својих чланова успеле да на неки начин прикрију своје функционисање. Умећем је формиран такозвани Dark net, Тамни интернет.

[75] Tsfati, Y, Weimann, G, „*Terror on the internet*“, Haifa university, Тел Авив, 2002,стр 324-326

Тамни интернет, или Дарк[76] нет, је део интернета потпуно недоступан обичним корисницима интернета. Карактеристично је да је потребно специфично знање како би му се приступило. Оно што је најбитније је да је немогуће контролисати га.

Дарк нет је врста интернета која се повезује са кривичним делима. Уговарање убистава, кријумчарења дроге, трговина људима, оружјем, све су то дела која се могу организовати преко ове врсте интернета.

Оно што одговара извршиоцима је анонимност. Функционише преко одређеног броја сервера који крију интернет адресе својих корисника, и скоро је немогуће открити ко се крије иза одређеног корисничког имена.

Ова анонимност је оно што погодује терористичким организацијама пре свега. Немогућност служби безбедности да открију ко је ко на Дарк нету је оно што их спречава да реагују и заштите грађане.

Функционисање организација коришћењем Дарк нета се може огледати у следећем:

- Веома је тешко открити чланове,
- Могућност формирање засебних соба за договор и планирање, којима нико ко не поседује овлашћење не може приступити,
- Врбовање чланова, који самим приступом овој мрежи, доказују да поседују одређено компјутерско знање које може помоћи организацијама у остваривању својих циљева,
- Прикупљање средстава од стране чланова, анонимним путем,

Суочавање безбедносног система са овом врстом је веома комплеско питање, јер како се суочити са оним што „не постоји“, како се борити против нечега што није видљиво?

Продирање у Дарк нет је за скоро сваку државу веома битно питање, али ће до даљњег остати немогуће.

[76] IT Klinika https://www.it-klinika.rs/blog/sta-su-deep-web-dark-web-darknet приступљено 03.10.2018

7. Објекти напада

Као објекти напада комојутерског тероризма, јављају се стандрардне критичне инфраструктуре[77] које су циљ и основног тероризма.

Под критичном инфраструктурум спадају неки од следећих објеката чије би угрожавање довело до отежаног или потпуног престанка функционисања државе:

- Здравствени систем,
- Безбедносни систем,
- Еколошки систем,
- Социјални систем,
- Нуклеарни програм,
- Банкарски систем, итд.

Самим тим, концентрација терористичких организација усмерена је на неки од ових система, или њихових делова.

Изазивање било каквих несрећа, или прекида њиховог функционисања (уништавање банкарског система, упад у нуклеарни програм, неометано кретање кроз безбедносни систем), може имати несагледиве последице по друштво.

8. Одбрана

Због све већег угрожавања држава и друштва компјутерским тероризмом, све већа је тежња како на националном, тако и међународном левелу да се развије механизам проактивног и ретроактивног деловања, с циљем спречавања односно минимизирања последица овог вида тероризма.

Због специфичности територијалне неограничености, тежња није само на државама да делују самостално, већ се мора преко међународних институција решавати ова питања. Пре свега први задатак је доношење законске регулативе у вези са компјутерским тероризмом.

[77] Критична инфраструктура представља имовину или услуге, систем или његов део, који је неопходан за одржавање кључних друштвених функција, здрравства, безбедности, економског или социјалног благостања, а чије би ометање или уништењеимало значајан утицај на функционисање државе- Нацрт закона о критичној инфраструктури- https://www.paragraf.rs/dnevne-vesti/270418/270418-vest18.html

Постоје много могућности борбе против компјутерског тероризма, увођење нових механизама, попут Firewall-а [78], развоја нових система за заштиту шифри, развоја система за распознавање корисника.

Ни за један систем заштите се не може рећи да је савршен, сваки од њих поседује одређену пукотину кроз коју ће искусни корисници проћи у систем и радити шта пожеле, уколико до тога дође, неопходно је развити систем за препознавање уљеза, односно да се у систему налази лице које нема дозволу да ту буде, као и неопходно је развијање процедура уколико дође до таквог продора. Процедура се мора састојати од прописа и активности који се морају испоштовати уколико дође до нежељене појаве.

Међутим пре овог ретроактивног деловања, морамо сагледати које су то могућности које могу бити део проактивног деловања, почевши од основне едукације службеника, развоја система заштите, унапређење коришћене технологије и програма који ојачавају заштиту.

То би се могло посматрати са становишта компанија које желе да спрече терористичке акције, међутим уколико се поставимо на ниво државе, акција државе је од непроцењивог значаја. Она би се морала састојати у константном развоју компјутерског система заштите, праћење навика, односно разумевања размишљања терористе и сагледавање које су то критичне инфраструктуре које могу бити објекат компјутерског тероризма. Такође како би се предупредиле све грешке и пропусти, неопходно је вршење вежби као прави пример напада.

Међутим све ово можемо посматрати као уопштено деловање свих субјеката безбедности, оно што је неопходно јесте деловање међународне заједнице.

Што се правног аспекта одбране тиче, и његове способности да стане проблему на пут, то трениутно није могуће. Немогућност прецизног одређивања појма, елемената компјутерског тероризма у знатној мери отежава доношење правних аката. Оно што међународно право познаје јесу пре свега препоруке Међународних организација како се државе требају поставити ка овом проблему.

На међународном плану су донешени одређени документи који дају препоруке земљама како да се поставе у борби против компјутерског тероризма.

[78] Firewall- Заштитни зид, односно програм који спречава непожељно присуство, или напад на рачунар

Извештај Радне групе Уједињених Нација за борбу против тероризма, донет је 2011, под називом „Супротстављање коришћења интернета у терористичке сврхе“. [79]

У *извештају* се наводи да су главни изазови међународне заједнице:

- доношење стратегија за борбу против компјутерског тероризма,
- увођење неке врсте цензуре, јер се на интернету могу наћи и рецепти за прављење бомби, самим тим могућност одређивања и спречавања приступа одређеним информацијама или програмима,
- обавезност активирања интернет провајдера, који ће пратити адресе својих корисника и захтевати њихово идентификовање при било којим сумњивим активностима,

Радна група је сагледавши функционисање и оапсност компјутерског криминалитета дошла до закључка да се на неке од проблема као што су интернет напади, недозвољени садржај, комуникација и финансирање мора одговарати на одређени начин:

- Интернет напади- опасна врста компјутерског тероризма, која одређеном применом може угрозити животе много људи, упадом и системе функционисања друштва. Мере које радна група предлаже су, примена одредби компјутерског криминала на терористичке акте, и доношење закона усмерених на конкретна дела компјутерског тероризма.
- Забрањени садржај- под тим се подразумева ширење пропаганде, врбовање људи. Мере које група предлаже јесте криминализација ових дела, односно цензурисање оваквог деловања, међутим ту се долази у сукоб са слободом говора, међутим препорука групе је да се не може терористичка пропаганда дефинисати као спобода говора.
- Комуникација- сагледавши могућности коришћења комуникације преко софтвера који онемогућују приступ непозваним лицима, препорука радне групе је да се успостави одређени механизам који би могао да дешифрује све тајне поруке, код којих се препозна повезаност са криминалним делима.

[79] CTITF Working Group Compendium, “ *Countering the use of the Internet for Terrorist Purposes- Legal and Technical Aspects*”, 2011http://www.un.org/en/terrorism/ctitf/pdfs/ctitf_interagency_wg_compendium_legal_technical_aspects_web.pdf приступљено 04.10.2018

- Финансирање- више није неопходно слати новчанице како би се омогућило доницање терористичких организација, довољно је један клик на комојутеру како би одређена свота новца била пребачена на њихов рачун. Препорука радне групе је доношење закона који би омогућио заплену тог новца, односно конфисковање имовине код банака.

9. НАТО

Као један од најјачих војних савеза, неоходно је поменути његову политику према компјутерском тероризму. Одбрана од компјутерског теороризма је један од основних задатака Алијансе, док наглашавајући да је највиши приоритет заштита система комуникације Алијансе.

Заштита од компјутерског тероризма је један од његових основних пројеката, којим Алијанса подстиче бољу комуникацију између земаља чланица, како би радили заједно и повећали способност одбране од напада. Алијанса такође организује вежбе за земље чланице како би сагледале своју способност одбране, а самосталне чланице могу волонтерски или на захтев НАТО-а да помогну развој система заштите Алијансе.

НАТО је схвативши опасност Компјутерског тероризма почео да организује Међународне вежбе одбране од компјутерских напада. [80]

Развивши Меморандум о разумевању одбране од компјутерских напада, у сарадњи са још 28 држава, НАТО је показао озбиљан приступ овом проблему.

Неке од активности НАТО-а:

- У Естонији се налази центар за истраживање и тренинг задужена за едукацију, учење лекција, истраживање и развој одбране од компјутерских напада,
- НАТО школа за комуникацијске и информацијске системе, у Италији.
- НАТО школа за тренинг и едукацију у вези са одбраном од компјутеских напада, развијајући стратегију, доктрикну и процедуре, у Немачкој,
- НАТО Колеџ одбране у Риму[81]

[80] https://www.ncia.nato.int/NewsRoom/Pages/19_12_2017.aspx приступљено 29.10.2018

[81] https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf приступљено 27.10.2018

10. Будућност компјутерског тероризма

Уколико би смо рекли да је развој технологије достигао максимум, грдно би се преварили. Технологија буквално сваког дана доживљава свој развој. Као што смо направили разлику између конвенционалног и комппјутерског оружја, тако ће се правити разлика између досадашњег и будућег компјутерског оружја.

Тројански коњи, вируси, ће можда у будућности бити потпуно занемарени појавом новог начина злоупотребе компјутера.

Једна од опасности на коју сам наишао кроз литературу јесу *виртуелне валуте*.

Виртуелна валута- пре свега средства која на интернету имају одређену вредност, на основу рада компјутера и наводног „копања“ информација и њиховог каснијег продавања. Карактеристика ових валута је да немају покриће у средствима у стварном свету. Оно што је доживело експанзију јесте нагло коришћење и њихов нагли скок вредности без покрића. Велики део друштва је кренуо да је користи, иако не постоји велики број информација о њима. Плаћање рачуна је негде постало свакодневно, куповина преко интернета је такође омогућена. Иако нико не зна како је она настала, како функционише, ни да ли има будућност пре свега. Самим тим са аспекта компјутерског тероризма није на одмет напоменути је. Пре свега оно што ми је при обради ове теме запало за око јесте могућност њеног искоришћавања од стране терористичких група. Нико са сигурноишћу не може рећи да она није плод терористичке организације. Које попут Логичке бомбе само чека тренутак када може бити активирана и због своје превелике употребе, светски банкарски систем потпуно уништи.

Осим ове претње, односно развоја угрожавања друштва компјутерским тероризмом, за будућност насупрот томе би могло бити везано и повећање безбедности, и развој средстава који би стали на пут како овом тако и другим врстама тероризма.

Самим тим развој неопходних стратегија, процедура, поступака је оно што моира бити циљ свих безбедносних структура, како интернационалних организација, тако и држава.

IV. ПРАВНА ВЕЗА КОМПЈУТЕРСКОГ ТЕРОРИЗМА И КРИМИНАЛИТЕТА

Као што је већ наведено у раду, не постоји јединствени правни механизам који може стати на пут компјутерском тероризму. За разлику од компјутерског криминалитета који у сваком националном законодавству има своје темеље, компјутерски тероризам се пре свега на правном плану заснива на законске чланове компјутерског криминалитета.

Дело компјутерског тероризма не може бити приписано било ком извршиоцу, већ се та дела на основу својих карактеристика сврставају у дела криминалитета, самим тим подлежу казнама предвиђеним за та дела.

Оно што је неопходно јесте међународно решење овог проблема. Јер компјутерски теоризам у највећем делу није дело које је везано за чисто једну државу. Због своје способности географске неограничености, једно дело може бити изршено са једну у другу или више држава. Самим тим доношење заједничких аката о сарадњи у вези са Компјутерским тероризмом, би требао бити циљ свих држава.

V. АНАЛИЗА СЛУЧАЈА

За студију случаја бих узео терористичку организацију Исламска Држава Ирака и Сирије- ИСИС.

За ову организацију се сматра да је најзаступљенија у вођењу компјутерског рата. Што се ИСИС-а тиче, настала је након Америчке инвазије на Ирак, као знак отпора западним агресорима, касније је изјавила подршку и ставила се под службу Ал- каиде, од које се касније, након довољног јачања одвојила. Контролише делове територија Ирака и Сирије.

Циљ ове групе је стварање Исламске државе под верским вођама, калифама[82].

Првобитне акције ове групације су биле, бомбашки напади западних сила на територији Ирака, док је касније са развојем организације, као и прикључивања образованих људи дошло до схватања да је један од могућности ратовања, пре свега интернет ратовање.

[82] Калифа- духовни поглавар муслимана, који се сматра потомком пророка Мухамеда.

За ИСИС се сматра да је најорганизованија група која се бави овом врстом ратовања. Осим напада који врше, као и прикупљања средстава преко интернета, карактеристично за њих је интернет регрутовање као и пропаганда.

Пропаганда као облик ратовања је у оквиру ове групе доживела свој врхунац. Почевши од простих ширења убеђења, претњи, и ширења страха, ова организација је отишла корак изнад свих осталих, интернет пропаганда се састојала у видео преносу малтретирања заробљеника, убистава, противника њихове вере, како они кажу. Видео клипови се могу наћи претрагом интернета:

- https://www.youtube.com/watch?v=mlGoILUv4S0- малтретирање заробљеника

Такође и велики број новинских чланака који сведоче о појединачним и масовним убиствима својих противника:

- https://www.dailystar.co.uk/news/latest-news/586411/ISIS-Mosul-Execution-Fire-Civilians-Burning-Spies-Iraq-Army-Siege-Battle-Liberation
- https://www.christianpost.com/news/isis-burns-3-women-alive-refusing-slaughter-innocent-civilians-178566/

Осим оваквог деловања, ИСИС је интернет пропагандом решио и да врбује своје следбенике:

- https://www.wsj.com/video/isis-releases-new-recruitment-video-and-more/3A84C33C-768D-4E94-B135-BCB12433FFE0.html

Интернет у свом пуном сјају користе и као корисници налога на друштвеним мрежама, тако је до скора имао своје налоге на Twitter-[83]у и то на енглеском, немачком и руском језику.

Као последицу оваквог деловања, велики број људи, који се ни не налази на територији Ирака или Сирије, постају симпатизери ИСИС-а.

Злочини извршени у име ИСИС-а:

Северна Америка:

1. Октобар,2014, Канада- прегажена 2 војника, док је један подлегао повредама, Извршилац је био Martin Rouleau- Couture, који је на интернету јасно износио ставове подршке ИСИС-у,

[83] Twitter- друштвена мрежа

2. Октобар, 2014, Канада- Michael Zehaf- Bibeau- отворио ватру на Национални ратни центар, убивши војног каплара, притом повредивши још једног чувара. ИСИС је након овога изјавио да је убица био њихов следбеник.
3. Октобар, 2014- Њујорк- Држављаних Сједињених Америчких Држава Zale Thompson напао 4 полицијска службеника. Након напада откривено да се самосталнио претраживао ИСИС на интернету, па се сматра да је акција била тиме инспирисана.
4. Јун, 2016- Флорида, Убица убио 49 особа у Ноћном клубу, убијен након три сата, док је у разговору са полицијом рекао да се заветовао ИСИС-у,

Европа:

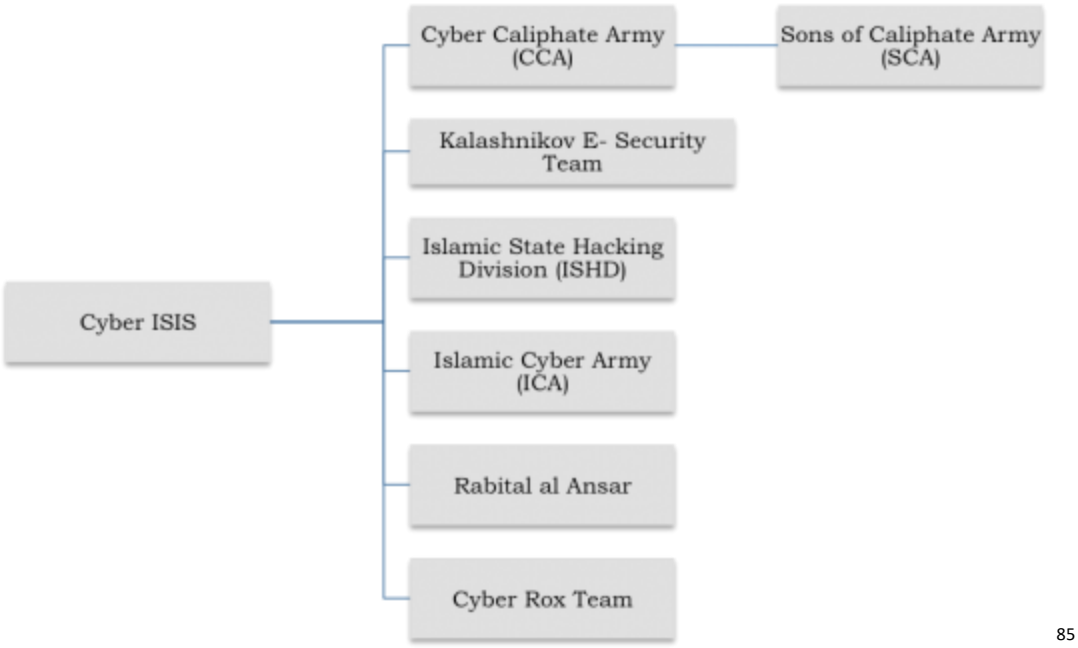
1. Јануар, 2015, Париз- Убиство 4 таоца од стране Amedy Coulibaly, који је убијен, међутим у видеу који је снимио пре злочина, рекао је да је следбеник ИСИС-а,
2. Септембар, 2015, Кавказ- ИСИС је изјавио да је њихов следбеник извршио напад на војну установу при чему је убијено неколико руских војника, неије стигла званична потврда.
3. Новембар,2015, Париз- серијом напада убијено је око 130 људи, а рањено више од 350, нападачи опасани експлозивом. Верује се да су нападачи симпатизери ИСИС-а

Што се ИСИС-а тиче, од 2014 године до данас, претпоставља се да су извршили више од 140 напада у 29 земље ван Ирака и Сирије. Претпоставља се да је убијено више од 2,000 људи, а неколико хиљада рањено.[84]

То су само неке од последица Интернет пропаганде, што се може у будућности манифествовати још горим исходом.

Што се организовања ИСИС-а тиче, на слици 1, можемо видети из којих се ћелија састоји:

[84] Lister. T. Sanchez. R. Bicxler. M. O`Key. S. Hogenmiller. M. Tawfeeq. M. " *ISIS goes global: 143 attacks in 29 countries have killed 2043*", CNN, 2018 https://edition.cnn.com/2015/12/17/world/mapping-isis-attacks-around-the-world/index.html приступљено 03.10.2018



[85]

Слика 1

Целокупан систем се према овој организацији дели на следеће делове:

- Уједињена армија калифата- састоји се од свих следбеника који користе компјутерске способности како би водиле компојутерски рат у корист Исламске Државе.
- Калашњиков тим интернет безбедности- циљ јесте објављивање података на интернет адресама, креирање сопсвених калана комуницирања[86].
- Одељење за хаковање- сврха овог одељења је продирање у системе држава, или других субјеката,
- Rabital al Ansar- ћелија задужена за шифровање порука које треба проследити кроз организацију

[85] Извор: https://poseidon01.ssrn.com/delivery.php?ID=690083116027127090074090094107004126014080037007054060088098125105090006071000127005030030106023013098105085004119080093099103106045047052093072066118118112117090008008079079111027008027069102005125017090126012127011109088010067029099002115100103075006&EXT=pdf приступљено 05.10.2018

[86] Memri Cyber and Jihad lab, " *Pros ISIS Cyber Jihadi Group Kalachnikov E-Security Team Operates On Social Media, Publishes Adresses of Federal Reserve Board od Governors*", 2016 http://cjlab.memri.org/lab-projects/monitoring-jihadi-and-hacktivist-activity/pro-isis-cyber-jihadi-group-kalachnikov-operates-on-multiple-digital-media-platforms-publishes-reported-addresses-of-federal-reserve-board-of-governors-a-review-of-their-account/ приступљено 01.10.2018

- Rox тим- активност чланова се састоји у информисању следбеника на интернет порталима о техникама избегавања праћења, упутствима о безбедном поступању, као и избегавању интернет замки безбедносних служби.

87

Како би се друштво пробало сукобити са оваквим деловањем ИСИС-а, предузето је велики број активности.

Неке од њих јесу:

- Гашење Интернет адреса за које се претпоставља да се користе за функционисање организације,
- Прављење софтвера који ће онемогућити постављање видео са насилним садржајем или позивима за регрутацију,[88]
- Велики број слободних грађана, корисника интернета је кренуо у „јурњаву“ за пропагандним материјалом ИСИС-ових следбеника.

VI. ЗАВРШНО РАЗМАТРАЊЕ

На основу обрађене теме, неки од ставова које бих ја као аутор могао да изнесем јесу:

- Модерно доба, само по себи, је друштву донело доста тога доброг, али је са друге стране омогућило и доста лоших ствари,
- Компјутерски тероризам је последица све веће тежње друштва за развојем технологије,
- Постојећи начини угрожавања друштва, све више добијају на својој снази, и константно се шири спектар њихове употребе,
- Са развојем технологије ће долазити до нових, опаснијих начина коришћења компјутера у сврху терориста,
- Сваки наредни сукоб ће све више добијати интернет аспект,

[87]Memri Cyber and Jihad Lab, “ *Jihadi Hacking Griuop Cyber TeamRox Active on Telegram, Facebook*”, 2016 http://cjlab.memri.org/lab-projects/monitoring-jihadi-and-hacktivist-activity/jihadi-hacking-group-cyber-teamrox-ctr-active-on-telegram-facebook/ приступљено 01.10.2018

[88]Corcoran. K. “ *The UK government has developed AI so powerful it can block 99,99% of ISIS propaganda videos before ther reach the internet*”, 2018 https://www.businessinsider.com/home-office-launches-ai-to-stop-isis-videos-says-its-9999-accurate-2018-2 приступљено 01.10.2018

- У будућности ће интернет ратови одлучивати победника сукоба,
- Неопходност развоја проактивног деловања у циљу спречавања компјутерског тероризма,
- Развој средстава суочавања са овом врстом тероризма, већа улагања у систем безбедности,
- Неопходна је већа улога међународних законодавних институција, у што скоријем доношењу аката с циљем деловања против компјутерског тероризма,
- Мора доћи до повећања државног активирања у вези са овим проблемом, као и много већа међудржавна сарадња,

Са аспекта обичног корисника интернета, и члана овог друштва, надам се да ће се овај проблем решити у скорије време, што због повећања осећаја безбедности мене самог, тако и друштва.

VII. ЛИТЕРАТУРА

1. Основни извори:

Bruce. G. "*Definition of terrorism Social and Political effect"*, Journal of Military and Veterans Health, vol 21, No 2, интернет верзија https://jmvh.org/article/definitionof-terrorism-social-and-political-effects/ приступљено 21.7.2018

Barry C. *"The Future of Cyberterrorism*", 11th annual International Symoposium on Criminal Kustise Issues, The unive0rsity of Illinois at Chicago,1997

Beal. V. "*Trojan Horse*", Webopedia https://www.webopedia.com/TERM/T/Trojan_horse.html приступљено 04.10.2018

Centre of Excellence Defense Against Terrorism, *Responses to Cyber Terrorism*, Amsteredam, 2008

Corcoran. K. " *The UK government has developed AI so powerful it can block 99,99% of ISIS propaganda videos before ther reach the internet*", 2018 https://www.businessinsider.com/home-office-launches-ai-to-stop-isis-videos-says-its-9999-accurate-2018-2 приступљено 01.10.2018

CTITF Working Group Compendium, " *Countering the use of the Internet for Terrorist Purposes- Legal and Technical Aspects*", 2011 http://www.un.org/en/terrorism/ctitf/pdfs/ctitf_interagency_wg_compendium_legal_technical_aspects_web.pdf приступљено 04.10.2018

Димитријевић. В. Стојановић. Р. *"Међународни односи"*, Службени лист СРЈ, Београд 1996

Denning.D. "*Activism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*", Georgetown University,2000, пдф извор http://www.iwar.org.uk/cyberterror/resources/denning.htm

Decker. B. Triplet. C. "*Beijing`s Electronic Pearl Harbor*" , The Washington Times, 2011 https://www.washingtontimes.com/news/2011/nov/11/beijings-electronic-pearl-harbor/ приступљено 25.09.2018

Gunderman. D. "*Incident of the Week: DDOS Attack Hits 3 Banks Simultaneoysly*" Cyber Security Hub, 2018 https://www.cshub.com/attacks/news/incident-of-the-week-ddos-attack-hits-3-banks приступљено 01.10.2018

Hoffman. B. "*Inside Terrorism"* ,New York, Columbia University Press, 2006

Holloway. M. "*Stuxnet Warm Attack on Iranian Nuclear Facilities"*, Standford University, CA,2015, http://large.stanford.edu/courses/2015/ph241/holloway1/ приступљено 03.10.2018

Игњатовић. Ђ. "*Криминологија"*, Осмо, измењено издање, Службени гласник, Београд, 2007

Janczewski. L, Colarik. A, "*Cyber Warfare and Cyber Terrorism*", New York, 2008

Littlefield. R. "*Cyber Terrorism: understanding and preventing acts of terror within our cyber space*",2017 https://littlefield.co/cyber-terrorism-understanding-and-preventing-acts-of-terror-within-our-cyber-space-26ae6d53cfbb приступљено 10.09.2018

Lister. T. Sanchez. R. Bicxler. M. O`Key. S. Hogenmiller. M. Tawfeeq. M. " *ISIS goes global: 143 attacks in 29 countries have killed 2043*", CNN, 2018 https://edition.cnn.com/2015/12/17/world/mapping-isis-attacks-around-the-world/index.html приступљено 03.10.2018

Милошевић. М. "*Тероризам као кривичноправна категорија"*,Београд, Безбедност, број 4/1988

Милошевић. М. "*Терористи, жртве и злочинци-фактори криминалне мотивације*", Факултет безбедности, Београд, 2009
Mannik. E. "Terrorism: its past, present and future Prospects", пдф https://www.ksk.edu.ee/wp-content/uploads/2011/03/KVUOA_Toimetised_12-M%C3%A4nnik.pdf приступљено 10.09.2018

Mc Lean. I. Mc Millan. A. "*The Concise Oxford Dictionary of Politics"*, Oxford University press, 2003

Memri Cyber and Jihad lab, " *Pros ISIS Cyber Jihadi Group Kalachnikov E-Security Team Operates On Social Media, Publishes Adresses of Federal Reserve Board od Governors*", 2016 http://cjlab.memri.org/lab-projects/monitoring-jihadi-and-hacktivist-activity/pro-isis-cyber-jihadi-group-kalachnikov-operates-on-multiple-digital-media-platforms-publishes-reported-addresses-of-federal-reserve-board-of-governors-a-review-of-their-account/ приступљено 01.10.2018

Memri Cyber and Jihad Lab, " *Jihadi Hacking Griuop Cyber TeamRox Active on Telegram, Facebook*", 2016 http://cjlab.memri.org/lab-projects/monitoring-jihadi-and-hacktivist-activity/jihadi-hacking-group-cyber-teamrox-ctr-active-on-telegram-facebook/ приступљено 01.10.2018

Post. J. Sprinzak. E. Denny. L. "The terrorist in their own words, Interviews with 35 incarcerated Middle Easter Terrorist, *Terrorism and Political Violence"*, 2003

Pollitt. M. " *A Cyberterrorism Fact or Fancy*" Proceedings of the 20th National Information Systems Security Conference, 1997

Reich. W. "*Understanding Terrorist behavior, the limits and opportunities of psychological Inquiry, Orgins of Terrorism, Psychologies, Ideologies, Theologies, States of Mind"*, Cambridge University press, Њујорк, 1990

Rusell. J. "*Japanesse government hit by Chinesse Trojan Atack*:", Азија, 2011 https://thenextweb.com/asia/2011/10/25/japanese-government-hit-by-chinese-trojan-horse-attack/ приступљено 04.10.2018

Савић. А. "*Основи државне безбедности"*, ВШУП, Београд, 1998

Стајић. Љ. *"Основи система безбедности"* ,Правни факултет у Новом Саду, Нови Сад, 2008

Симоновић. Б. "*Криминалистика"*, Правни факултет у Крагујевцу, Крагујевац, 2004

Schmid. A. Jongman. J. "*Political terrorism: a new Guide to Actors, Authors,Cencepts, Data Bases, Theories and Literature"*, Transaction Books, Њу Џерси, 1988

S. Baldi. E. Gelbstein. J. Kurbalija. "*Hacktivism, cyber-terrorism and cyberwar*", Diplofoundation, Малта, 2003

Sherpa. S. „*Cyber Attacks that Affect India in 2017*", Gizbot, 2017 https://www.gizbot.com/internet/features/cyber-attacks-that-affected-india-in-2017/articlecontent-pf82316-046533.html приступљено 04.10.2018

Symantec employeehttps://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html приступљено 03.10.2018

Tsfati. Y. Weimann. G. "*Terror on the internet*", Haifa university, Тел Авив, 2002

Vatis. M. "*Cyber attacs during The War On Terrorism*", Institute for Security technology Studies, Darthmouth University, Хановер, 2001 http://www.ists.dartmouth.edu/docs/cyber_a1.pdf

Veerasamy. N. "*Motivation for Terrorism*" Defence, Peace, Safety and Security,CSIR, Јужна Африка , https://www.researchgate.net/publication/46175365_Motivation_for_cyberterrorism приступљено 15.09.2018

Weimann. G. Winn. C. "*The Theatre of terror*", Longman Publication, Њујорк, 1994

Weimann. G. "*Terror on the Internet: The New Arena, the New Challenges*" Вашингтон, 2006

Webroot https://www.webroot.com/us/en/resources/tips-articles/computer-security-threats-computer-viruses приступљено 03.10.2018

Zerzi. M. "*The treat of cyber terrorism and recommendarion for coyntermeasures*", C.A. Perspectives on Tunisia No. 04-2017

Zetter. K."*Logic Bomb Set Off Sout Korea Cyberattack*", Wired, 2013 https://www.wired.com/2013/03/logic-bomb-south-korea-attack/ Приступљено 04.10.2018

2. Остала истраживачка грађа

ОУН резолуција бр A/RES/45/121 http://www.un.org/documents/ga/res/45/a45r121.htm приступљено 24.6.2018

OSCE препорука број P(85) https://polis.osce.org/node/4651 приступљено 24.6.2018

Конвенција Савета Европе о високотехнолошком криминалу, Будимпешта, 2001- https://www.mpravde.gov.rs/files/KONVENCIJA%20O%20VISOKOTEHNOLOSKOM%20KRIMINALU.doc пристпупљено 23.06.2018

Кривични законик Републике Србије, *Службени Гласник* бр. 85/2005

Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала- https://www.paragraf.rs/propisi/zakon_o_organizaciji_i_nadleznosti_drzavnih_organa_za_borbu_protiv_visokotehnoloskog_kriminala.html приступљено 22.06.2018

3. Електронски извори

INTERPOL

https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime приступљено 15.05.2018

https://www.interpol.int/Crime-areas/Cybercrime/Operations/Simda-botnet приступљено 16.07.2018
https://www.interpol.int/Crime-areas/Cybercrime/Operations/Operation-Aces приступљено 16.07.2018

Сајт Министарства Унутрашњих Послова
http://www.mup.gov.rs/wps/portal/sr/gradjani/saveti/visokotehnoloski%20kriminal/!ut/p/z0/fY6xDoIwFEV_RQdG8woqwbFxINEQV-xCSq3waG1LqSh_bwdXne65ycnNBQY1MMNn7HhAa7iO_cry5nKo8rQk2bnYkZTQnJYF2RdZmW7hBOy_EBdwGEdGgQlrgnwHqN2z1SgasXjUERLirJDB8IR0nt8GbjAhE59liDnjZJUNsjdW20nhSnI84Pdb5qtj1QFzPPQbNHcL9W_fKdYuL7r-AIS9X0w!/ приступљено 22.06.2018

https://www.techopedia.com/definition/4010/logic-bomb

https://www.wsj.com/video/isis-releases-new-recruitment-video-and-more/3A84C33C-768D-4E94-B135-BCB12433FFE0.html

https://www.dailystar.co.uk/news/latest-news/586411/ISIS-Mosul-Execution-Fire-Civilians-Burning-Spies-Iraq-Army-Siege-Battle-Liberation

https://www.christianpost.com/news/isis-burns-3-women-alive-refusing-slaughter-innocent-civilians-178566/

https://www.youtube.com/watch?v=mlGoILUv4S0

https://www.it-klinika.rs/blog/sta-su-deep-web-dark-web-darknet

https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf

https://www.ncia.nato.int/NewsRoom/Pages/19_12_2017.aspx

http://www.jihadica.com/how-do-you-become-a-member-of-al-qaeda/

http://hamas.ps/en/
https://www.moqawama.org/
http://almanar.com.lb/

https://poseidon01.ssrn.com/delivery.php?ID=690083116027127090074090094107004126014080037007054060088098125105090006071000127005030030106023013098105085004119080093099103106045047052093072066118118112117090008008079079111027008027069102005125017090126012127011109088010067029099002115100103075006&EXT=pdf

VIII. САЖЕТАК И КЉУЧНЕ РЕЧИ

Развој друштва са собом носи развој различитих сфера . Тај развој поред свих добрих ствари, са собом доноси и нешто лоше, злоупотребу тих истих ствари. Сфера угрожавања која је искористила тај напредак је и тероризам, односно Компјутерски тероризам, као један од његових облика. Анализу Компјутерског тероризма сам желео да обрадим пре свега због жеље за знањем на који начин се технологија коју познајемо може злоупотребити. Ова тема је занимљива пре свега због његове константне експанзије, није једна од оних које су јединственог облика без могућности развоја. Да бих анализирао Компјутерски тероризам, користио сам се пре свега сагледавањем тема Компјутерски криминалитет као и Тероризам, као појмове који су у блиској вези са овом темом. Сагледавајући њихове карактеристике, њихово правно тумачење, решавање, могли смо полако долазити и до података о самој теми. Користећи се мишљењем различитих теоретичара, трудио сам се да што више продрем у ову тему. Илуструјући се примерима, желео сам да сагледам да ли стварно Компјутерски тероризам на наизглед једноставним начинима може угрозити друштво, што смо и могли закључити кретањем кроз ову тему. Компјутерски тероризам полако постаје претња број 1 за целокупно друштво.

Кључне речи: компјутерски криминалитет, тероризам, компјутерски тероризам, интернет рат,

IX. ABSTRACT OF THE TOPIC AND KEY WORDS

The development of the society brings with it a development of different spheres. That development, with all that good thins, brings with it and something bad, misusing that things. Endangering sphere that used that progress is Terrorism, Cyber terrorism, as one of his forms. In the analysis od Cyber terrorism I wanted to deal primary because of desire for knowledge on which way we may abuse technology we know. This topic is interested because of it constant expansion, it is not one of those which are unique form without expansion possibility. In order to analyze Computer Terrorism, I used primarily the topic of Computer Crime as well as Terrorism, as the concepts that are closely related to this topic. By looking at their characteristics, their legal interpretation, resolution, we could slowly come up with information about the topic itself. Using the opinions of various theorists, I tried to get more into this topic. By illustrating the examples, I wanted to see whether Cyber Terrorism in seemingly simple ways could endanger society, which we could conclude by moving through this topic. Cyber terrorism slowly becomes the number 1 threat for the entire society.

Key words: Cyber crime, terrorism, Cyber terrorism, internet war

X. БИОГРАФИЈА СТУДЕНТА

Студент Васић Милош, рођен је 30.01.1992. у Гњилану, Република Србија. Основну школу похађао је у Гњилану и Бујановцу, где је завршио и средњу стручну школу, у смеру Економски техничар.

Основне академске студије уписао је 2010. у Београду, на Факултету безбедности, које је завршио 2015. Након завршених основних студија, мастер студије је уписао на Правном факултету, Универзитет у Нишу, 2016. Године.

Поседује сертификат Nansen dialogue centra, са знањем Медијације у школама.

Знање енглеског језика.