УНИВЕРЗИТЕТ „ГОЦЕ ДЕЛЧЕВ“ - ШТИП

ПРАВЕН ФАКУЛТЕТ

Магистерски труд

Тема:

Компјутерски криминал

Сајбер тероризам

Кибернетичка војна

Ментор:

доц. д-р Олга Кошевалиска

Кандидат:

Наташа Донева

Број на индекс: 207562

Штип, ноември 2018 година

СОДРЖИНА

Компјутерски криминал 1

Сајбер тероризам 1

Кибернетичка војна 1

Апстаркт: 5

I ДЕЛ 9

Поимно определување на сајбер/компјутерски криминалот 9

1. Поим и дефеници на сајбер криминал, компарација со поимот на компјутерски криминал 9

2. Специфичноста наречена компјутерски криминал 14

3. Карактеристики на компјутерскиот „магионичар”-криминалец 18

4. Феноменологија на сајбер криминалитетот. 21

4.1. Компјутерски измами 22

4.2. Изработка и употреба на лажна платежна картичка 25

4.3. Измама при тргување со хартии од вредност 26

4.4. Кражба на индентитет 27

4.5. Зграпчување и узурпирање на компјутерски услуги 27

4.6. Манијачење- Cyberstalking 27

4.7. (зло)Употреба на правата од интелектуална сопственост 28

4.8. Производство и дистрибуција на нелегални порнографии 30

4.9. Компјутерска диверзија 30

4.10. Компјутерска саботажа 31

4.11. Компјутерска шпионажа 31

II ДЕЛ 33

Меѓународна правна рамка 33

1. Документи донесени од Советот на Европа 35

2. Документи донесени од ООН 36

3. Европска конвенција за сајбер криминал 38

3.1. Дополнителен Протокол на Конвенцијата за сајбер криминал за инкриминација на дела од расистички и ксенофобистички вид по пат на информатички системи 42

4. Релацијата сајбер криминал и меѓународните полициски организации-Интерпол 43

5. Релацијата сајбер криминал и меѓународните полициски организации-Европол 44

6. Дигитална Женевска конвенција 47
III ДЕЛ 51
Сајбер тероризам 51

1. Дистинкција помеѓу сајбер криминал и сајбер тероризам 51
2. „Интерна" класификација на сајбер нападите 56
CASE STUDY: PETYA / NOTPETYA 66
CASE STUDY: WANNA CRY ATTACK 68
CASE STUDY: UKRENEGRO/ UKRAINIAN BLACKOUT 68
CASE STUDY: STUXNET 68
CASE STUDY: OPERATION BUGDROP 69
CASE STUDY: TV5 MONDE CYBER ATTACK 69
CASE STUDY: SHAMOON 70
CASE STUDY: LulzRaft 70
CASE STUDY: RED OCTOBER 71
CASE STUDY: SONY PICTURES HACK 71
CASE STUDY: OPERATION CLEAVER 72
CASE STUDY: CYBERATTACK DURING THE PARIS G20 SUMMIT 72
IV ДЕЛ 75
Кибер(информатичка) војна: Хакери наместо војници на фронтот 75
1. Дефинирање на кибер војна 75
2. Закани за компјутерскиот систем 78
2. Одбрана за компјутерските системи 81
V ДЕЛ 83
Компаративен осврт на правната регулатива-инкриминација на компјутерскиот криминалот и сајбер тероризмот 83
1. Приказ на законската инкриминација на компјутерските кривичните дела низ преглед на законодавствата на повеќе држави 83
1.1. Република Србија 84
1.2. Република Хрватска 86
1.3. Франција 86
1.4. Германија 87
1.5. Канада 87
VI ДЕЛ 89

Казненото законодавство во Република Македонија – борба против компјутерскиот криминалот и сајбер нападите 89
1. Правната регулација на компјутерскиот криминалво Р. Македонија 89
Правната регулација на компјутерскиот криминал во Република Македонија 90
2. Ретроактивна компарација на компјутерските инкриминации во македонскиот КЗ .. 91
3. Компјутерски кривични дела предвидени во Кривичниот законик од 1996 година. .. 92
4. Компјутерски кривични дела предвидени со Кривичниот законик од 2004 година 93
5. Компјутерски кривични дела предвидени со измените на Кривичниот закон од 2008 година 94
6. Компјутерски кривични дела со измените на Кривичниот законик од 2009 година ... 95
7. Компјутерските инкриминации во Кривичниот законик на Р. Македонија 96
8. Домашните институции кои имаат ингеренции за борба со компјутерскиот криминал 98
9. Заеднички истражни тимови-Joint Investigation Teams 101
Прилог: Обезбедување докази во електронска форма 102
Заклучок: 105
Компјутерски поими користени во магистерскиот труд 117
Користена литература: 122

Апстаркт:

Сајбер криминалот, сајбер тероризмот и кибернетичката војна за жал сè уште се енигма која засега, но и е проучувана од различен профил на експерти. Затоа во овој труд ќе се обидиме да направиме дистинкција помеѓу компјутерски и сајбер криминал, да го објасниме преку case studies манифестирањето на сајбер тероризмот, но уште поважно да ги доловиме далекусежните репрекусии што истиот ги предизвикува. Тенденцијата е да се објасни и поактуелната кибер (информатичка) војна, односот на светските сили кон новата замена за конвенционалната војна, припремање и формирањето на сајбер центри од страна на државите и евентуалниот повидок на нова армија составена единствено од хакери вооружени со еден единствен арсенал-компјутер. Оттука е неизбежно да се осврнеме на правната регулатива која се обидува да се справи со „сајберманијата" како на национално така и на меѓународно ниво. Покрај македонската правна рамка, ќе дадеме компаративен приказ на инкриминацијата во други држави, но ќе обработиме и дел од моменталните документи со меѓународен предзнак кој ја регулираат оваа материја и нивното (не)успешно имплементирање. Во прилог на овој труд ќе бидат прикажани и дел од објавените извештаи на организации чиј таргет е проучување на овој нов виртуелен криминал.

Клучни зборови: меѓународен криминал, законски инкриминации, хакери, сајбер криминал, сајбер војна.

Abstract:

Cyber crime, cyber terrorism and cyber war are unfortunately still an enigma that has been studied by a different expert profile for now. Therefore, in this paper we will try to make a distinction between computer and cyber crime, to explain through case studies the manifestation of cyber terrorism, but more importantly, to capture the far-reaching repressions that it causes. The tendency is to explain the frequent occurrence of cyber (information) war, the attitude of the world powers to the new replacement for conventional war, the preparation and formation of cyber centers by the states and the possible view of a new army made up of only hackers armed with a single arsenal - computer. Therefor, it is inevitable not to refer to the legal regulation that seeks to cope with "cybermania" both nationally and internationally. In addition to the Macedonian legal framework, we will provide a comparative overview of the incrimination in other countries, but we will also process some of the current documents with an international reference which regulate this matter, and their (not) successful implementation. In addition to this paper, some of the published reports of organizations whose target is the study of this new virtual crime will be shown.

Keywords: international crime, legal incriminations, hackers, cyber crime, cyber war.

Мистеријата наречена сајбер криминал е особено интересна за следење со оглед на фактот дека е динамична, постојано се модифицира, се менуваат појавните облици, се менува modus operandi, се продира во сфери и области кои се од круцијално значење за опстанокот на самите држави. Се злоупотребува информатичкиот изум за започнување на нови бескрупулозни војни, за ширење ксенофобични пораки, за крадење парични средстава, за крадење на берзанските тајни, за инсајдерски информации и сл. Речиси и да нема крај на енормната листа на полиња на продор, проблеми кои не се започнати токму со овој вид модерен криминал. Потребата од негово сузбивање и те како е алармантна и бара меѓународна соработка и помош, за резултати кои иако нема да бидат утопистѝчки, барем ќе се задоволителни.

За жал ова е област која сè уште може да се нарече енигма за органите на прогон. Различен кадар на профили е засегнат и работи на превенција на оваа „современо зло", но секогаш информатичките генијалци се еден чекор пред правдата. Вешто ги прикриваат своите траги, умешно ги извршуваат кривичните дела со користење на само една направа - компјутер, кој како магија за кратко време предизвикува репрекусии низ цел свет. Чудно, но материјата за сајбер криминалот и тероризмот иако присутна во сите држави, сепак различно е регулирана. Што значи различни држави имаат различен систем на регулирање и справување со оваа материја, но и различни законски инкриминаации. Затоа се донесени плејада на меѓународни документи преку кои светот се обидува да се заштити од сајбер криминалот. Но дали нивната имплементација на државно ниво е толку успешна, колку што се очекува. Дали постои документ со интернационална сила и глобално значење, на кој сите држави би му се „покориле" за да се заштитат од дигиталниот анонимен криминал?

Вовед

Секое време носи свои предизвици пред кои треба да се исправиме и умешно да се справеме. Колку маркантно, успешно, сеопфатно ќе биде тоа, зависи од проблематиката, нејзината распространетост, вмреженост, засегнатоста на општеството, но и средствата со кои располагаме. Така дел од кривичните дела кои биле доминантни во минатото, денеска се „навика" која се повторува и речиси рутински решава. Но што со оние криминални активности кои допрва сега се појавуваат, за кои никој во минатото не ни помислил дека ќе постојат и своевремено би ги сместиле во научна фантастика? Што со оние кривични дела кои брзо, незабележано продуцираат мноштво на проблеми, пропаст на цели економии, загрозување на сигурноста на граѓаните и пострашно безбедноста на државата? Колку сме запознати со оваа флктуирачка материја, колку добро можеме да го следиме темпото што го диктира современиот – наречен сајбер криминал? Проблемот на 21-от век, но започнат кон средината на 20-от век, денеска сеприсутен во секојдневното живеење и сите пори на општественото функционирање, сајбер криминалот и те како е проблем кој бара сеопфатно ангажирање, како во негово детално објаснување и разглобување, така и во негово детектирање, превенирање и анулирање на негативните последици од неговото дејствување.

Информатичката револуцијата со право многумина ја нарекуваат трета индустриска револуција. Истата отвори еден цел нов свет-виртуелен со чија помош може многу полесно, побрзо, попрактично да се остварат и достигнат многу работи. Информатички изуми кои го доближуваат светот до нас, кој ни овозможуваат со еден клик да постигнеме нешта за кои претходно со месеци би чекале. Но колку и да има бенефити, не може да го изоставиме фактот дека и оваа проблематика е медал со две страни. За жал, сè почесто сме сведоци на злоупотреба на новата технологија и информатичките изуми се користат како параван за извршување кривични дела.

Користена литература:

1. Ачкоски, J. Сигурноста на компјутерските системи, компјутерски криминал и компјутерски тероризам, Скопје,2012 година.
2. Ачкоски, J, Дојчиновски, М. Сајбер криминал и заштита на дигиталните податоци во компјутерските мрежи.
3. Adler F; Mueller G; Laufer W. Criminology and the criminal justice system – sixth edition.
4. Богданоски, М, Петрески, Д. Меѓународно научно списание за одбрана, безбедност и мир.
5. Богданоски,М,Богданоски,М. Сајбер нападите како најсовремена закана за воените операции и критичната инфраструктура.
6. Боцевски, Д. Компјутерски инциденти и истражување на компјутерски криминал во Република Македонија.
7. Витларов, Т. Казнено право,2013 година.
8. Видојковиќ, М. Компјутерски криминалитет- магистерски труд, Ниш, 2015 година.
9. Водич за протоколите за меѓуагенциска и за меѓународна соработка во истраги што вклучуваат приноси од криминал стекнати преку интернет.
10. Габеров,М. Феноменологија на сајбер криминалитетот,2015 година.
11. Габеров, М. Правото на приватност и сајбер просторт,2015 година.
12. Гарфинкел,С, Спафорд,Џ. Безбедност и заштита на мрежниот сообраќај.
13. Гелке,А.Новата ера на тероризмот и меѓународниот политички систем.
14. Димовски,Д. Компјутерски криминалитет, UDK:343.4:004.
15. Калач, J. Сајбер тероризмот како закана кон безбедноста на државата,2017 година.
16. Милошески, В. Компјутерски криминал-предизвици и новини во македонското материјално законодавство, 2016 година.

17. Милошески,В,Зврлевски,М,Андонова,С. Прирачник за компјутерски криминал, 2014 година.
18. Николоска,С. Методика на истражување компјутерски криминалитет,Скопје, 2013 година.
19. Николоска,С. Појавни облици и форми на компјутерски криминал во банкарското работење и кривично правна заштита во Република Македонија.
20. Смиљаноска Ј; Јанкоска М; Богданоски М, Крадење на идентититет и методи за намалување на ефектите на овој напад.
21. Стоилковски,М; Цветановски,Ј, Обезбедување докази во електронска форма од меѓународни и домашни интернет провајдери,2017.
22. Хаџи-Јанев,М; Богданоски,М, Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare.
23. Cyber terrorism: Assesment of the threat to insurance, Cambridge centre for Risk Studies, 2017.
24. Шалијан,Ж,Блин,А. Историја на тероризмот.

Закони

1. Кривичен Законик на Р. Македонија (Службен весник на Р. Македонија број. 37/1996, 80/99, 4/02, 43/03, 19/04, 81/05, 50/06, 60/06, 73/06, 87/07, 7/08, 139/08, 114/09, 51/11,135/11, 185/11, 142/12, 143/12, 166/12, 55/13, 82/13.)
2. Закон за криивчна постапка (Службен весник на Р. Македонија број. 15/97, 44/2002, 74/2004, 18/99, 27/2004, 15/2005,)
3. Закон за електронски комуникации (Службен весник на Р. Македонија број. 39/14, 188/14, 44/)
4. Закон за следење на комуникациите (Службен весник на Р. Македонија број.121/2006, 110/2008, 116/2012).

5. Закон за електронска трговија (Службен весник на Р. Македонија број. 133/2007, 17/11, 104/15, 192/15).
6. Закон за електронско управување (Службен весник на Р. Македонија број.105/2009, 47/2011).
7. Закон за парнична постапка (Службен весник на Р. Македонија број. 79/2005, 110/2008, 83/2009, 116/2010, 124/2015).
8. Закон за податоците во електронски облик и електронски потпис (Службен весник на Р. Македонија број. 34/2001, 6/2002, 98/2008, 33/2015).
9. Декларација за побезбеден интернет (Службен весник на Р. Македонија број. 31/2010).

Конвенции:

10. Европска конвенција за сајбер криминал, Будимпешта, 2001 година.
11. Дополнителен протокол на Конвенцијата за сајбер криминал за инкриминација на дела од расистички, ксенофобички вид по пат на информатички системи-Стразбур, 2003 година.
12. Конвенција на Советот на Европа за перење, откривање, заплена и конфискација на приноси од казниво дело и финанасирање на тероризам-Варшава, 2005 година.
13. Конвенција на Советот на Европа за заштита на децата од сексуална експлоатација и сексуална злоупотреба.

Линкови:

1. http://www.jpacademy.gov.mk/upload/materijali%202017/zakon_za_ratifikacija_na_konvencijata_za_kompjuterski_kriminal_41_24062004.pdf .
2. https://www.coe.int/en/web/cybercrime/the-budapest-convention
3. https://daucimezaedno.wordpress.com/%D0%B8%D1%81%D1%82%D0%BE%D1%80%D0%B8%D1%98%D0%B0-%D0%BD%D0%B0-%D0%BA%D0%BE%D0%BC%D0%BF%D1%98%D1%83%D1%82%D0%B5%D1%80%D0%B8%D1%82%D0%B5/

4. https://www.nw3c.org/
5. http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf
6. http://www.notohatespeech.com/wp-content/uploads/2016/08/AP-Cybercrime.pdf
7. https://www.coe.int/en/web/cybercrime/iproceeds
8. http://www.unis.unvienna.org/pdf/05-82111_E_6_pr_SFS.pdf
9. http://nssarchive.us/NSSR/2010.pdf
10. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
11. https://www.itu.int/en/Pages/default.aspx
12. https://ccdcoe.org/tallinn-manual.html
13. https://en.wikipedia.org/wiki/Hacktivism
14. https://www.iab.org/
15. https://www.urbandictionary.com/define.php?term=leet+speak
16. https://rm.coe.int/3156-25-guide-interagency-international-cooperationprotocolmk-mkd/16807be221
17. http://www.mioa.gov.mk/files/pdf/POIMNIK.pdf
18. http://www.childrensembassy.org.mk/WBStorage/Files/Konvencija%20na%20Sovetot%20na%20Evropa%20za%20zastita%20na%20deca%20od%20seksualna%20zloupotreba.pdf
19. http://www.wipo.int/edocs/lexdocs/laws/mk/mk/mk008mk.pdf
20. https://www.pravdiko.mk/wp-content/uploads/2013/11/Zakonot-za-avtorskoto-pravo-i-srodnite-prava-23-08-2010.pdf
21. http://www.eurojust.europa.eu/Practitioners/JITs/Pages/JITs-sitemap.aspx
22. https://www.europol.europa.eu/activities-services/joint-investigation-teams
23. http://www.jpacademy.gov.mk/upload/materijali%202015/Konvencija%20na%20ON%20za%20OK%20so%20protokoli.pdf
24. http://www.customs.gov.mk/images/documents/borbaKorupcija/oonProtivKorupcija.pdf
25. https://www.computerworld.com/article/2474163/cybercrime-hacking/red-october-5-year-cyber-espionage-attack--malware-resurrects-itself.html

26. https://ccdcoe.org/tallinn-manual-20-international-law-applicable-cyber-operations-be-launched.html
27. http://bezbednonainternet.org.mk/component/option,com_frontpage/Itemid,1/lang,mk/
28. http://www.apprm.gov.mk/webdata/dokumenti/ZastiaNaPravataOdIndSopstv.pdf
29. http://journal.maclc.mk/2015/17.pdf
30. http://www.stat.gov.mk/
31. http://www.mvr.gov.mk/analiza/kriminal/19
32. https://www.pravdiko.mk/wp-content/uploads/2013/11/Zakonot-za-megunarodna-sorabotka-vo-krivichnata-materija-14-09-2010.pdf
33. https://www.pravdiko.mk/wp-content/uploads/2013/11/Zakon-za-sledene-na-komunikatsiite-21-11-2006.pdf
34. https://www.pravdiko.mk/wp-content/uploads/2013/11/Zakon-za-izmenuvane-i-dopolnuvane-19-09-2012.pdf
35. https://www.pravdiko.mk/2786/evropska-konventsija-za-megusebna-pravna-pomosh-vo-krivichnata-materija-ets-030/
36. https://www.pravdiko.mk/2786/evropska-spogodba-za-prenos-na-baran-ata-za-pravna-pomosh-ets-092/
37. http://www.cilc.nl/
38. http://prosecutorsnetwork.org/uimages/Final%20Manual%20Criminal%20Law%20Macedonian%20version%206%20December%202016.pdf
39. http://www.aon.com/2018-political-risk-terrorism-and-political-violence-maps/index.html?utm_source=aoncom&utm_medium=2017-prm-redirect&utm_campaign=riskmaps2018
40. http://large.stanford.edu/courses/2015/ph241/holloway1/
41. https://anydifferencebetween.com/difference-between-cyberterrorism-and-cyberextortion/
42. https://anydifferencebetween.com/difference-between-cybercrime-and-cyberterrorism/
43. https://www.europol.europa.eu/iocta/2017/index.html

44. https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain
45. http://journals.sagepub.com/doi/abs/10.1177/0096340210393703
46. https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain
47. https://books.google.mk/books?id=YIiRyO6ctzMC&printsec=frontcover&dq=Cyber-threats,+information+warfare&lr=&as_drrb_is=q&as_minm_is=0&as_miny_is=&as_maxm_is=0&as_maxy_is=&as_brr=0&ei=C4TOS-ieFY2GkAS13JjSAQ&cd=1&redir_esc=y&hl=en#v=onepage&q&f=false
48. https://www.cbsnews.com/news/pentagon-bill-to-fix-cyber-attacks-100m/
49. https://aecnewstoday.com/2015/black-money-cleaning-scam-see-how-its-done/#axzz5OvBrSZv9
50. https://www.researchgate.net/publication/313662110_The_History_of_Cybercrime_1976-2016
51. http://www.unhcr.org/innovation/digital-geneva-convention-mean-future-humanitarian-action/
52. http://www.cybercrimelaw.net/documents/Presentation1.pdf
53. http://www.cybercrimelaw.net/Cybercrimelaw.html
54. http://hrbrief.org/hearings/18652-2/
55. https://www.itu.int/itunews/manager/display.asp?lang=en&year=2008&issue=06&ipage=05&ext=html
56. http://www.cybercrimelaw.net/documents/ICTC.pdf
57. http://cybercrimelaw.net/documents/cybercrime_history.pdf
58. https://www.researchgate.net/publication/267946947_The_History_of_Global_Harmonization_on_Cybercrime_Legislation_-The_Road_to_Geneva