Универзитет Џон Незбит
Факултет за право, јавну управу и безбедност

Живанка Миладиновић

КРИВИЧНО ДЕЛО ПРЕВАРЕ КАО МОДЕЛ ОСТВАРИВАЊА САЈБЕР КРИМИНАЛА

-ДОКТОРСКА ДИСЕРТАЦИЈА-

Београд, 2016

Универзитет Џон Незбит
Факултет за право, јавну управу и безбедност

Живанка Миладиновић

КРИВИЧНО ДЕЛО ПРЕВАРЕ КАО МОДЕЛ ОСТВАРИВАЊА САЈБЕР КРИМИНАЛА

-ДОКТОРСКА ДИСЕРТАЦИЈА-

Предмет: кривично право
Име и презиме ментора: проф. др Срето Ного

Име и презиме студента: Живанка Миладиновић
Број индекса: 1003/2013
Студијски програм: докторске академске студије
Матични број:

Београд, април, 2016

САДРЖАЈ

АПСТРАКТ

Безбедност је често само илузија којој погодују лаковерност, наивност или незнање. Најчувенији светски научник двадесетог века, Алберт Ајнштајн, рекао је: „Само су две ствари безграничне, универзум и људска глупост, а за оно прво нисам сигуран.” Дакле, обмањивање може да успе када се наиђе на људску глупост или, чешће, на непознавање добрих безбедносних правила. Како се развијају све боље и боље безбедносне технологије, које отежавају проналажење техничких пропуста, нападачи се све више окрећу људском чиниоцу као централном елементу у информационо-комуникационој инфраструктури, а без ког рачунари или мреже не би могли да функционишу. Поражавање људског сигурносног бедема је често лако, не изискује никаква улагања и подразумева минималан ризик.

Чињеница да је интернет повезао око две стотине земаља, и да је напредак технологије у последњих двадесет година достигао границе потпуне компјутерске контроле најважнијих друштвених процеса допринели су њиховом настанку и њиховој злоупотреби. Поједини аутори те злоупотребе називају компјутерским криминалом, неки рачунарским криминалом, а у Србији је званичан назив високотехнолошки криминал. Међутим, пратећи светске трендове који су уважили назив сајбер криминал како у својим законодавствима, тако и у радовима из ове области, у раду ће се користити тај термин, којим ће се означавати све противправне активности почињене у сејбер простору, који чине мреже рачунара и обухвата становнике било ког дела света, свих старосних група и друштвених слојева.

Убрзан развој информационо-комуникационе технологије и незаустављиви раст примене у свим сферама људског друштва, поред несумљивих предности, ствара и погодне услове за одређене појаве с негативним предзнаком, као што је сајбер криминал. На тај начин савремено друштво постаје веома рањиво и изложено озбиљним опасностима, те се ризици морају благовремено уочити и на адекватан начин ставити под контролу.

Према најновијим подацима, у тзв. сајбер простору налази се више од милијарду и по људи. То је условило нова правила понашања, нове обичаје, нове опасности. Сајбер криминал је глобални проблем, који изискује пуно учешће и сарадњу друштвеног и приватног сектора у свим државама. Кад би само један одсто од милијарду и по људи имао

намеру да коришћењем информационих технологија чини кривична дела, то би створило ситуацију да на светском нивоу имамо 15 милиона потенцијалних преступника.

У првом поглављу докторске дисертације, као увод у ову комплексну област обрађена су питања одређења кривичног дела преваре, опште карактеристике кривичног дела преваре, радња извршења и правна регулатива кривичног дела преваре.

Друго поглавље докторске дисертације садржи објашњења значења израза „сајбер" и синтагме „сајбер простор", као и приказе различитих дефиниција и карактеристика сајбер простора и утицаја сајбер простора на свакодневни живот људи. У истом поглављу докторске дисертације обрађен је феномен сајбер криминала путем следећих проблемских целина: појам, облици и карактеристике. До адекватног објашњења појма сајбер криминала дошло се анализом значења тог појма у литератури и анализом његовог обима и садржаја. Обрађене су заједничке карактеристике компјутерског и сајбер криминала, а затим и специфичности сајбер криминала које га одвајају у посебну категорију високотехнолошког, односно криминала у опште.

Следеће поглавље односи се на појам кривично дело преваре као модел остваривања сајбер криминала. У том поглављу нуди се приказ облика којима се остварује сајбер криминал. На основу наведеног дата је садржајна и методолошки коректна дефиниција сајбер превара. Представљене су различите класификације сајбер криминала, а у зависности од примењеног критеријума. Од више критеријума класификације, аутор се определио за једну, која по његовом мишљењу најбоље обухвата обим појма.

Посебно значајани сегменти тог дела поглавља представљају целине у којима се обрађују последице сајбер превара: материјалне, нематеријалне и комбиноване.

Значајан део докторске дисертације посвећен је регулацији сајбер криминала као веома важном кораку у супротстављању, и то путем следећих сегмената: иностранa и домаћа регулатива. Приказана је правна регулатива преваре као модела остваривања сајбер криминала, приликом чега је обрађено законодавство Републике Србије путем регулатива датих у Кривичном законику и Закону о организацији и надлежности државних органа у борби против високотехнолошког криминала. Такође, ради бољег сагледавања проблема, дата је упоредна правна анализа законодавства различитих држава које су донеле посебан закон о сајбер криминалу.

У четвртом поглављу докторске дисертације обрађени су начини извршења преваре као модели остваривања сајбер криминала. Обрађена је техника социјалног инжињеринга навођењем теоријских одређења те технике и њиховог психолошког утицаја искоришћавањем хеуристичког начина размишљања. Развој информационо-комуникационих технологија условио је развој малициозних програма који су моћно оружје у рукама сајбер преваранта. У раду су приказани разни малвери и њихово деловање приликом одвраћања од систематичног размишљања и немарности корисника интернета. Комбиновани модел је најзаступљенији и као најсофистициранији начин за остваривање циљева сајбер преваранта с разлогом је обрађен у докторској дисертацији.

Пето поглавље садржи две проблемске целине: профил сајбер преваранта и поступак откривања и доказивања преваре као модела остваривања сајбер криминала.

У тежњи да се прикаже профил лица која чине ту врсту криминала, обрађени су мотиви који узрокују извршење те врсте кривичних дела, психолошки профил лица и њихова класификација на аматере и професионалце – хакере у области информационих технологија.

Због специфичности кривичних дела сајбер криминала, њихово откривање и доказивање битно се разликују од класичног вида криминала. У раду су приказане те специфичности, а приказани су и електронски докази и њихова заштита, идентификација, прикупљање, анализа, реконструкција и презентација.

У последњем поглављу докторске дисертације приказани су државни органи надлежни за откривање и процесуирање сајбер криминала, као и активности међународних организација у циљу сузбијања те појаве. Како нема успешне борбе против сајбер криминала без развијене међународне сарадње, у раду је приказан облик међународне сарадње предвиђен у Конвенцији о сајбер криминалу, који одудара од класичног облика сарадње путем замолница уважавајући нужност брзине деловања и доступности 24 сата, 7 дана у недељи.

Будући да је први корак у борби против тих негативних појава стварање свести о постојању опасности од тог проблема, ова докторска дисертација је покушај да се различити аспекти сајбер криминала, с нагласком на сајбер криминалу који се врши помоћу кривичог дела преваре, прикажу и приближе стручној јавности, као и колегама у институцијама за

борбу против сајбер криминала, а с пуном вером у њихова даља залагања на путу супротстављања тој појави.

ABSTRACT

Security is often just an illusion convenient for credulity, naivety and ignorance. The most famous world scientist of the twentieth century, Albert Einstein, said: 'Only two things are infinite, the universe and human stupidity, and I'm not sure about the former'. Therefore, deception can be successful when there is human stupidity or, more often, ignorance of good safty rules. By developing better and better security technologies which impede the discovery of technical omissions, the attackers turn their attention more and more to human factor as the central element in information and communication infrastructure, without which computers and networks couldn't function. Beating human security bastion is often easy. It doesn't require any investments and takes minimal risk.

The fact that the Internet has connected around two hundred countries, and that the development of technology in the last twenty years has reached the boundries of complete computer control of the most important social processes have contributed to their development and abuse. Certain authors those abuses name computer crime, others call it cybercrime, and in Serbia the official term is high technology crime. However, following the world trends which accepted the term cyber crime in their legislations, as well as in the published articles from this field, in this thesis will further be used that term, which will denote unlawful activities committed in cyberspace, which consists of computer networks and includes citizens of any part of the world, of all ages and social layers.

The rapid development of information and communication technology and unstoppable growth of the application in all fields of human society, besides undoubted advantages, also creates suitable conditions for certain occurrences with a bad omen, such as cyber crime. In that way, modern society becomes vulnerable and exposed to serious dangers and therefore the risks have to be noticed promptly and brought under control adequately.

According to the newest data, there are more than billion and a half people in so-called cyberspace. That caused new rules of behavior, new customs and new dangers. Cyber crime is a global problem which requires full participation and cooperation of public and

private sector in all states. If only one per cent of billion and a half of people had the intention to commit crimes by using information technologies, there would be fifteen million of potential criminals.

In the first chapter of this PhD thesis, as an introduction to this complex field, the questions of defining deception as a criminal act, general characteristics of the criminal act of deception, perpetration and regulation of the criminal act of deception, are being processed.

The second chapter of the PhD thesis contains the explanations of the meanings of the term ‘cyber’ and the phrase ‘cyberspace’, as well as display of various definitions and characteristics of cyberspace and its influence on everyday life of people. In the same chapter of the thesis, the phenomenon of cyber crime is processed through the following problem units: term, forms and characteristics. Analyzing the meaning of the term cyber crime and analyzing its scope and contents led to adequate explanation of that term. Mutual characteristics of computer and cyber crime are processed, and after that the specifics of cyber crime which put it into the separate category from high technology crime, more exactly from crime in general.

The following chapter refers to the term criminal act of deception as a model of performing cyber crime. In that chapter, the review of the forms of performing cyber crime is given. Based on that, informative and methodologically correct definition of cyber deceptions is given. Various classifications of cyber crime, depending on the applied criterion, are presented. Out of several criteria of classification, the author chose the one which covers the scope of the term best, in her personal opinion.

Particularly significant segments of that part of the chapter are the units in which are processed the consequence of cyber deceptions: material, nonmaterial and combined.

Significant part of the PhD thesis is dedicated to the regulation of cyber crime as a very important step in opposing it, by means of the following segments: foreign and domestic regulation. The regulation to deception as a model of realizing cyber crime is presented. The legislation of the Republic of Serbia is processed by regulations given in the Criminal Code and Law on Organization and Jurisdiction of Government Authorities for Suppression of Cybercrime. Furthermore, in order to perceive the problem better, comparative analysis of legislations of different countries, which enacted special law on cyber crime, is given.

In the fourth chapter of the PhD thesis the ways of committing deception are processed as the models of committing cyber crime. The technique of social engineering is processed by giving the theoretical entries of the technique and their psychological influence using the heuristic way of thinking. The development of information and communication technologies caused the development of malicious programs which are powerful weapon in the hands of cyber criminals. In the thesis are presented various malwares and their performance during averting from systematic way of thinking and carelessness of the Internet users. The combined model is the most present and, as the most sophisticated way of accomplishing goals of cyber criminals, is processed in the thesis with a reason.

The fifth chapter contains two problem units: the profile of cyber criminals and the procedure of discovering and proving the deception as a model of committing cyber crime.

Striving to present the profile of the people who commit that type of crime, motives which cause performance of those types of crimes are processed, as well as psychological profile of those people and their classification into amateurs and professionals-hackers in domain of information technologies.

For the reason of specificity of the criminal acts of cyber crime, revealing and proving them in comparison with classic form of crime, is considerably different. Those specificities are shown in the thesis, as well as electronic evidence and its protection, identification, gathering, analysis, reconstruction and presentation.

In the last chapter of this PhD thesis are presented government agencies authorized for revealing and prosecuting cyber crime, in addition to the activities of international organizations with the aim of suppressing that phenomenon. As there is no successful fighting against cyber crime without developed international cooperation, the form of international cooperation provided by Convention on Cybercrime is shown in this thesis. It differs from classic form of cooperation by letters rogatory, considering the necessity of speed of action and availability 24 hours per day, 7 days in a week.

Considering the fact that the first step in fighting against those negative phenomena is increasing awareness of problem existence, this thesis is an attempt to present

different aspects of cyber crime, with an emphasis on cyber crime committed by criminal act of deception, and bring it closer not only to experts, but also to colleagues in the institutions for fighting against cyber crime believing in their further commitment to oppose this phenomenon.

I МЕТОДОЛОШКИ ОКВИР ИСТРАЖИВАЊА

1.ФОРМУЛАЦИЈА ПРОБЛЕМА ИСТРАЖИВАЊА

У формулацији предмета истраживања пошли смо од хипотетичких ставова, значаја идентификованог проблема истраживања и резултата претходних истраживања о проблему докторске дисертације.

1.1 Хипотетички ставови о проблему истраживања

Док год Интернет не буде правно регулисан, извршиоци кривичних дела имају доста простора за вршење криминалних активности.

Развој савремених информационих технологија, посебно на пољу електронске трговине и комуникације, створио је нови простор за деловање криминалаца и криминалних група.

Сајбер преваре су постале једана од најчешћих опасности на интернету, због врло честог мењања начина извршења и прилагођавања брзим променама у области информационих технологија.

Правна регулатива у Републици Србији не пружа добру основу за ефикасно спречавање овог вида кривичног дела преваре.

Непостојање посебног кривичног дела ,,сајбер превара`` утиче на смањење и отежавање борбе против ове појаве.

Чињеница је да феномен „сајбер превара“ код нас није довољно познат широј јавности и корисницима интернета, посебно зато што та тема није довољно заступљена у медијима.

Међутим, као основни проблем јавља се чињеница да се ова кривична дела врше од стране лица која се налазе ван територије Републике Србије, углавном са територије афричког континента, са којима је међународна полицијска сарадња знатно отежана.

Превентивно деловање државних органа као што су полиција и тужилаштво има кључну улогу када је спречавање те појаве у питању. Пошто сарадња са државама из којих се врши ова врста кривичних дела није на завидном нивоу, потребно је што хитније деловати проактивно, искористити потенцијал медија и скренути пажњу домаћој јавности на финансијске губитке који настају као последица тих кривичних дела.

Превентивна улога полиције у заштити корисника интернета са територије Републике Србије од сајбер превара таквим активностима сигурно би била успешнија и сврсисходнија од репресивних активности које се предузимају након сазнања да је кривично дело извршено.

1.2. Резултати досадашњих истраживања

Резултате досадашњих истраживања о сајбер преварама можемо поделити на главне и споредне.

У главне резултате убрајају се она истраживања која су посвећена сајбер преварама као начину остваривања сајбер криминала и њих је веома мало. Једно од ретких дела које се баве овим проблемом у којем се изучава тактика и техника извршења сајбер превара је „*Cyber fraud: tactics, techniques and procedures*“ [1]. У овом делу аутор Rick Howard поред објашњења тактике, рачунарске технике и процедуре које се користе при извршењу сајбер преваре, бави се и питањима мотивације и профила сајбер превараната.

Споредни извори се односе на нека друга питања, а само делимично на питања сајбер превара.

Од домаћих споредних извора из ове области истиче се дело„ *Компјутерски криминал*“ где је објашњен појам компјутерског криминалитета и његово разликовање од сајбер криминалитета. У истом делу су представљене врсте сајбер криминалитета: сајбер превара, сајбер шпијунажа, ‘’хакинг’’, сајбер саботажа, сајбер криминал везан за садржаје, криминал везан за производе и супстанце и повреде приватности. Посебну пажњу аутор је посветио класификацији економских сајбер кривичних дела: cyber преваре, haking, крађа Интернет услуга и времена, пиратство софтвера, микрочипова и база података, cyber

[1] Више о томе: Howard, R.,*Cyber fraud: tactics, techniques and procedures*. Auerbach Publications, 2009

индустријска шпијунажа, преваре Интернет аукције (неиспоручивање производа, лажна презентација производа, лажна процена , награђивање цене производа, удруживање ради постизања веће цене, трговина робом са црног тржишта, вишестуке личности). [2]

За дефинисање сајбер простора заслужни су аутори Шварту, Аркила и Ронфелт. Захваљујући поменутим ауторима сајбер простор је на сликовит начин описан као неопипљиво место између рачунара, где информација накратко постоји у свом току са једног на други крај глобалне мреже. Он је етерична стварност, безброј електрона који се крећу бакарним жицама или стакленим влакнима брзином светлости. Овај простор егзистира где год постоје телефонски каблови, линије стакленог влакна или електромагнетни таласи, а који је настањен знањем електронског облика". [3]

Питања како изгледа у стварности извођење превара које се врше методом социјалног инжињеринга и са којим се проблемима сусрећу преваранти како би убедили у своју причу жртву до детаља је описао Кевин Митник, познати и осуђени хакер за упаде у велике рачунарске системе Мотороле, Фуџицуа, Нокије и Сан мајкросистемс.[4] Овај са правом проглашени најпознатији хакер је део своје књиге „*The Art of Intrusion* " посветио стварним причама и примерима како се социјални инжењеринг може комбиновати са хаковањем. После сваке приче извршена је анализа извођења напада, као и мера одбране против њега. У својим делима Кевин Митник указује на важност метода социјалног инжењеринга у извођењу преваре, јер је много лакше некога преварити на овај начин него пробити корисникову сигурносну заштиту и користити рањивости његовог софтвера путем *IP spoofinga - Internet Protocol (IP) Address Spoofing* који представља процес фалсификовања IP адресе у оквиру IP пакета).

Штетне утицаји сајбер превара су описани у делу ,, *Fraud, corruption and cyber crime in a global digital network*". И ако се ово дело поред превара описује и корупцију и друге видове сајбер криминала, сајбер преваре су означене као велика опасност економијама како

[2] Више о томе : Петровић, С., Компјутерски криминал, Министарство унутрашњих послова Републике Србије, 2001

[3] Више о томе: Schwartau, W., Information Warfare, Chaos on the electronic superhighway. *Thunder's Mouth Press, New York*, 1994. ; Arquilla, J., & Ronfeldt, D., *Cyberwar is coming!*. RAND Corporation, 1992

[4] Више о томе: Mitnik K D., Sajmon V. L., Уметност обмане: утицај људског фактора на безбедност, Микро књига, Београд, 2003; Mitnik K D., Sajmon V. L.,, Умеће провале", Микро књига, Београд, 2005

развијених држава, тако и држава у развоју, јер су њихове жртве како појединци, тако и мултинационалне компаније. Највећи број извршилаца ових кривичних дела припада мањим организованим криминалним групама, али се понекад дешава да функционишу и самостално. Уколико извршиоци кривичних дела нису добро организовани, онда не могу да изврше преваре већих размера и оштете веће компаније, али су јако опасни за средњу класу грађана и мала предузећа.[5]

Случај „ Нигеријска превара`` због распрострањености и великих новчаних средстава које су жртве изгубиле заинтригирао је стручну јавност, па о овом случају најважнији извори су: *„Investigating and Prosecuting Nigerian Fraud"* и *„ Nigeria Tackles Advance Fee Fraud",* у којима је дата дескрипција поступка извршења ове преваре. Истраживања у овим делима су показала да у највећем броју случаја постоји једнообразност поступака у извршењу нигеријске преваре. Најпре, извршиоци кривичних дела траже уплату новчаних износа како би се нпр. надокнадили одређени трошкови које сноси неко измишљено лице (нпр. трошкови подмићивања, накнаде у банкама, трошкови адвоката и др.) како би дошли до предметног новца. Након што оштећени уплати одређени новчани износ према инструкцијама извршилаца кривичних дела следи одлагање новчаних трансакција везаних за исплату обећане суме новца. Стално се појављују нови трошкови за оштећеног на име реализације посла и траже нова одлагања, стално се обећава „експресна" исплата новца, уз убеђивање жртве преваре да ће јој се улагање у договорени посао вишеструко исплатити. [6]

Дескрипција показатеља сајбер превара у бизнису, начини заобилажења и борбе против ове друштвено опасне појаве дата је у делу *„Avoiding Cyber Fraud in Small Businesses: What Auditors and Owners Need to Know". Посебан* акценат дат је на коришћењу лажних докумената са лажним печатима, потписима, лажном садржином и сл. које израђују посебна предузећа уз новчану накнаду, а која се шаљу жртви преваре ако пристане на понуђени „посао", при чему се остварује крађа идентитета, и злоупотреба фотографија лица које су прикупљена са интернета.[7]

---

[5] Више о томе: Ionescu L, Irea V, Blăjan A, Fraud, corruption and cyber crime in a global digital network. - Economics, Management & Financial Markets, 2011.

[6] Више о томе: Buchanan, J., Grant, A., *Investigating and Prosecuting Nigerian Fraud*, U.S. Attorneys' Bulletin, Vol 49, No 06, USA, 2001; Chawki, M., *Nigeria Tackles Advance Fee Fraud*, Journal of Information, Law & Technology, University of Warwick, Great Britain,2009

[7] Више о томе: Bologna, G. Jack, Jack Bologna, and Paul Shaw. *Avoiding Cyber Fraud in Small Businesses: What Auditors and Owners Need to Know*. John Wiley & Sons, Inc., 2000.

1.3. Значај истраживања

1.3.1. Научни значај

У теорији није у потпуности разрађена и објашњен проблем сајбер криминала. Реч је о релативно новој појави која се из часа у час мутира и усавршава.

О овом облику претње у сајбер простору на нашим просторима није написано ни једно озбиљније дело које би у потпуности објаснило појам сајбер преваре и његово разликовање од других начина остваривања сајбер криминала.

Научни значај истраживања кривичног дела преваре као начина остваривања сајбер криминала огледа се у **научном објашњењу** појама „сајбер преваре“, начина њеног извршења, сагледавање посебних врста сајбер превара, **дескрипцији и класификацији** правне регулативе у Републици Србији везане за спречавање ове појаве и у **научном уопштавању** досадашња искуства МУП-а Републике Србије у вези спречавања сајбер превара у Републици Србији на основу којих ће се открити начини унапређења борбе у овој за друштво значајној материји.

1.3.2. Друштвени значај

Сајбер преваре су постале веома честа и распрострањена појава, која је од стране многих полицијских служби широм света означена као велика опасност по финансијску безбедност, како појединаца, тако и привредних и пословних субјеката и државе у целини.

Неопходно је детаљно регулисање кривичних дела сајбер превара и осталих начина остваривања сајбер криминала, како не би некажњено прошло противправно присвајање имовинске користи и остали облици угрожавања безбедности сајбер простора.

Главни проблем истраживања у овој дисертацији јесу преваре са акцентом на сајбер преваре у Републици Србији, тежишно усмереним на утврђивање: информатичких ресурса за одвијање сајбер превара, модела сајбер превара, начина извршења (modus operandi) и реалног функционисања сајбер превара кроз студије случаја у низу.

Истраживање овако постављеног проблема биће тежишно усмерено на анализи постојећих облика сајбер превара, са дескрипцијом и класификацијом законске регулативе у области спречавања сајбер превара, анализом рада надлежних органа и идентификацији субјеката задужених за борбу против ових превара.

2. ОДРЕЂЕЊЕ ПРЕДМЕТА ИСТРАЖИВАЊА

Предмет истраживања у овој докторској дисертацији је кривично дело преваре као модел остваривања сајбер криминала тј. лажно приказивање и прикривање података с циљем да се прибави противправна имовинска корист, где се компјутер или рачунарска мрежа употребљавају као средство или циљ, доказ или окружење извршења кривичног дела.

Полазећи од тога, предмет истраживања су акти манипулације којим се жртве наводе да одају поверљиве информације о себи у сајбер простору као "заједници" сачињене од мреже компјутера у којој се елементи традиционалног друштва налазе у облику бајтова и битова.

2.1. Теоријско одређење предмета истраживања

Појам „сајбер" (или кибер) учестало се користи кад год је потребно створити нове термине да би се објаснили концепти везани за информационе и комуникационе технологије и револуцију информација. Први га је употребио научник Норберт Винер, у другој половини четрдесетих година XX века, у својим истраживањима која су представљала основу нове научне дисциплине кибернетике.

Кривично дело превара је начин остваривања сајбер криминала (engl. *Cyber crime*), који представља облик криминалног понашања, код кога се коришћење компјутерске технологије и информационих система испољава као начин извршења кривчног дела, где се компјутер или рачунарска мрежа употребљавају као средство или циљ, доказ или окружење извршења кривчног дела.

Поред кривичног дела преваре, остали начини остваривања сајбер криминала су: злоупотреба мреже за ширење недозвољеног материјала, дечија порнографија, упад у систем као модел остваривања сајбер криминала, сајбер тероризам и сајбер ратовање.

Сајбер преварантима на располагању стоје многи начини коришћења рачунара и рачунарске мреже за извршење сајбер превара, који се из дана у дан, развојем информационих технологија све више усавршавају.

Уз коришћење рачунара и мрежа, што чини одлику сајбер криминала, сајбер преваранти да би извршили кривично дело сајбер преваре, користе фалсификовану документацију како би преузели новац који им је оштећени уплатио, бежичне трансфере новца за пренос противправно стечених новчаних средстава, техничка средства која им омогућују анонимну комуникацију, Web-базирану електронску пошту, електронске налоге који су предходно преузети од правих корисника, факс машине за слање факс порука при размени документације са жртвама преваре, услуге телекомуникационих сервиса за директну комуникацију са жртвом преваре, лажне странице на интернету којима оштећене доводе у заблуду да комуницирају и сарађују са представницима легалних и легитимних институција, и друго.[8]

Друштвене мреже попут Facebooka или Twittera су непресушан извор вредних информација у извршењу сајбер превара. Разлог томе је што се људи слободније понашају него у стварном животу, без проверавања идентитета својих наводних виртуалних пријатеља, те спремно откривају детаље из свог живота које нападач лако може злоупотребити за своје намере.

Спам поруке се најчешће користе за ово кривично дело. У поруци се често наводи да корисник треба да потврди или промени податке, поверљиве природе. Када корисник попуни наведена поља, информације долазе до власника лажне странице, која изгледа скоро истоветно као и права, али се адреса разликује. Те информације он користи у разне сврхе, али најчешће за крађу новца с банковног рачуна или за провалу у е-пошту жртве.

У многим преварама жртве се примамљују обећавањем добијања велике своте новца („лутријска“ и „ нигеријска превара“). За узврат жртва треба само да плати трошкове отварања рачуна у одређеној банци, или да плати таксе, или на неки сличан начин учествује у трошковима. Тражени износ је обично од неколико хиљада, па до десетак хиљада долара,

[8] Више о томе: Howard, R., *Cyber fraud: tactics, techniques and procedures*. Auerbach Publications, 2009.

франака, фунти или евра. Могућност да преварант сноси трошкове, наводно, не постоји, јер новац мора да буде уплаћен са рачуна особе која ће подићи милионску суму. Ова превара има много варијација, па се од жртве може тражити да уплати више мањих сума, а трошкови се поткрепљују наводним званичним документима.

Овај криминал се сврстава у најизразитији облик транснационалног криминала против кога ни борба не може бити конвенционална. Борба против сајбер превара се заснива на превентивним и репресивним мерама. Репресивне мере су исте као и код других видова криминалитета, док су оперативне веома специфичне. Наиме, оне морају бити усмерена на предузимање активности у циљу отклањања извора, услова, околности или пропуста који погодују неовлашћеном коришћењу или злоупотреби компјутера.

Најважнија међународна конвенција која регулише питања сајбер криминала, па и сајбер превара је Конвенција Савета Европе о високотехнолошком криминалу донета 2001.године у Будимпешти, а ступила је на снагу јула 2004.године. Она представља водич за државе које желе да развију легислативу у борби против сајбер криминала.

Дана 18.03.2009. године у Службеном гласнику Републике Србије, број 19-09 објављен је и Закон о потврђивању Конвенције о високотехнолошком криминалу. У члану 3 тог Закона наводи се да су за њено спровођење задужени министарство надлежно за правосуђе, министарство надлежно за унутрашње послове и министарство надлежно за телекомуникације.

У *Кривичном законику* који је ступио на снагу 1. јануара 2006. године, законодавац је омогућио кривично правну заштиту лица и имовине и створио правне оквире за ефикасно спречавање кривичних дела рачунарске преваре.

У поглављу XXVII Кривичног законика под називом „Кривична дела против безбедности рачунарских података“, у ставу 1 члана 301, дефинише се радња извршења кривичног дела «Рачунарска превара» на следећи начин: „Ко 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, казниће се новчаном казном или затвором до три године.“ У ставу 2 овог члана се наводи се да ће се учинилац казнити затвором од једне до осам година ако је делом из става

1. тог члана прибављена имовинска корист која прелази износ од 450.000 динара, а ставом 3. је предвиђено да ће се учинилац казнити казном затвора од две до десет година ако је делом из става 1 тог члана прибављена имовинска корист која прелази износ од 1.500.000 динара. Ставом 4 предвиђена је новчана казна или затвор до шест месеци уколико је дело из става 1. тог члана извршено само у намери да другог оштети.[9]

Институционални оквир за борбу против сајбер криминала, постављен је у Закону о организацији и надлежности државних органа за борбу против високотехнолошког криминала. Овим Законом уређује се образовање, организација, надлежност и овлашћења посебних организационих јединица државних органа ради откривања, кривичног гоњења и суђења за кривична дела одређена тим Законом. Наведеним Законом су установљене институције за борбу против високотехнолошког криминала: два заменика јавног тужиоца који су специјализовани за борбу против високотехнолошког криминала, служба за борбу против високотехнолошког криминала (део МУП-а) и веће Окружног суда за борбу против високотехнолошког криминала Окружног суда у Београду.[10]

На територији Републике Србије створени су кривично-правни и институционални оквири за борбу против високотехнолошког криминала, а тиме и за борбу против кривичних дела преваре и рачунарских превара на интернету.

2.2. Дефинисање категоријално-појмовног система

У овој докторској дисертацији основни категоријално-појмовни апарат у директној вези са предметом истраживања чине појмови: *кривично дело преваре, сајбер криминал и сајбер превара.*

1) Кривично дело превара

У *Кривичном законику*, који је ступио на снагу 1. јануара 2006. године, у поглављу XXI под називом „Кривична дела против имовине“, у ставу 1 члана 208, кривично дело

[9] Више о томе: Кривични законик “Службени гласник РС“, бр. 85 / 2005, 88 / 2005, 107, 72 /2009, 111 / 2009, 121/2012, 104 / 2013, 108 / 2014.

[10] Више о томе: Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала „Службени гласник РС“, бр. 61 од 18. јула 2005, 104 од 16. децембра 2009.

Превара се дефинише на следећи начин: „Ко у намери да себи или другом прибави противправну имовинску корист доведе кога лажним приказивањем или прикривањем чињеница у заблуду или га одржава у заблуди и тиме га наведе да овај на штету своје или туђе имовине нешто учини или не учини, казниће се новчаном казном или затвором до три године“.[11]

Намера лица које чини превару треба разумети као његову свест да ће радње које је предузео изазвати заблуду код другог лица. Може бити реализована путем радњи или поступака који произлазе из активног или пасивног понашања лица које чини превару (нпр. лажно уверавање да ствар поседује одређени квалитет или пак прикривање чињеница које би биле одлучне за доношење одлуке на страни лица у заблуди, а пасивно понашање постоји у случају када једно лице примети код другог лица заблуду али ништа не учини да је отклони).

У зависности од намере учиниоца, разликујемо два облика преваре – ако извршилац намерава да обманом прибави себи или другом противправну имовинску корист, постоји основни облик преваре, а ако примењује обману само у намери да другог оштети, постоји лакши облик преваре. Та дистинкција прави се и у Кривичном законику Републике Србије, у ком се у члану 208 предвиђају различите санкције за та два вида преваре. У члану 208, ставу 2 наводи се: „Ко дело из става 1. овог члана учини само у намери да другог оштети, казниће се новчаном казном или затвором до шест месеци.”[12]

У теорији се као најкарактеристичније и најучесталије облике превара у савременом свету сматрају: 1) интернет преваре, 2) превара у вези с уговорима о пружању туристичких услуга, 3) организоване преваре, и 4) пореске преваре.[13]

[11] Кривични законик “Службени гласник РС“, бр. 85 / 2005, 88 / 2005, 107, 72 /2009, 111 / 2009, 121/2012, 104 / 2013, 108 / 2014., члан 208, став 1

[12] Кривични законик Републике Србије („Службени гласник Републике Србије”, бр. 85/2005, 88/2005 и 107/2005), члан 208.

[13] Више о томе: Вујовић, И., *Превара у савременом уговорном праву* – докторска дисертација одбрањена на Правном факултету Универзитета у Београду, 2009.

2) Сајбер криминал

Осим израза „сајбер криминал", неретко се употребљавају и други термини: *интернет-криминал*, *електронски криминал*, *криминал високих технологија*, *мрежни криминал* и сл.

Сајбер криминал је комплексан феномен, а сам појам се сматра кишобран-термином, који покрива разноврсне криминалне активности, укључујући ту и нападе на рачунарске податке и системе, нападе повезане с рачунарима, као и нападе на садржаје или интелектуалну својину, који се одвијају у електронском окружењу.

У Конвенцији о сајбер криминалу (енгл. *Convention on Cybecrime*) Савета Европе сајбер криминал је дефинисан као криминал за чије постојање је неопходна употреба рачунарских система тј. „сваког уређаја или групе међусобно повезаних уређаја којима се врши аутоматска обрада података или било којих других функција и рачунарских мрежа које служе као мреже за повезивање разних субјеката.

Једна од најобухватнијих дефиниција сајбер криминала је:„Сајбер криминал представља облик криминалног понашања једног или више лица у сајбер простору, у којем се рачунарске мреже појављују као средство, циљ, доказ или окружење извршеног кривичног дела".[14]

О сајбер криминалу можемо говорити ако је кривично дело „извршено коришћењем информационе технологије у сајбер простору". Остале деликте, чији се учиниоци користе информационом технологијом, а који нису извршени у сајбер простору, исправније је називати кривичним делима повезаним с рачунарском технологијом (*енгл. Cyber related crimes*). Та кривична дела била би регулисана одредбама о рачунарском криминалу.

Конвенција Савета Европе о сајбер криминалу класификује кривична дела сајбер криминала у пет група. Прва група састоји се од дела против поверљивости, интегритета и доступности компјутерских података и система, као што су илегалан приступ, незаконито прислушкивање, мешање података, систем уплитања. Другу групу чине дела повезана с

[14] Вулетић, Д., *Сајбер криминал и могућност његовог откривања* (-докторска дисертација), Факултет организационих наука, Београд, 2008, стр. 35.

коришћењем рачунара као средство извршења кривичних делан– наиме као средство манипулације информацијама. Ова група укључује рачунарске преваре. Трећу групу чине кривична дела повезана са садржајем (садржај података) који су сачувани на рачунарским мрежама. Најчешћи пример из ове групе су кривична дела која се односе на дечју порнографију. Четврта група обухвата кривична дела повезана с кршењем ауторских и сродних права. Пета група уведена је *Протоколом* уз Конвенцију о сајбер криминалу. Она прописује кривична дела расистичке и ксенофобичне природе извршена путем рачунарских мрежа.

3) Сајбер превара- Кривично дело преваре као модел извршења сајбер криминала

Сајбер преваре подразумева прикривање и лажно приказивање података с циљем да се себи или другоме прибави противправна имовинска корист и тиме другом лицу нанесе штета, где се компјутери или рачунарске мреже употребљавају као средство или циљ, односно, доказ или окружење извршења ове врсте преваре.

Сајбер преваре представљају врсту високотехнолошког криминала чија је дефиниција дата у члану 2. Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала, који је ступио на снагу 26. јула 2005. године: „Високотехнолошки криминал у смислу овог закона 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.”[15]

У Кривичном законику који је ступио на снагу 1. јануара 2006. године, у поглављу XXVII, под називом „Кривична дела против безбедности рачунарских података”, у ставу 1 члана 301. на следећи начин дефинише се радња извршења кривичног дела рачунарска превара: „Ко 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

[15] Закон о организацији и надлежности државних у борби против високотехнолошког криминала "Сл. Гласник РС", бр. 61/2005 и 104/2009 (члан 2)

другом проузрокује имовинску штету, казниће се новчаном казном или затвором до три године."[16]

У научној теорији идентификаовано је више врста сајбер превара, као што су: фишинг, вишинг, фарминг, клик преваре, нигеријске преваре, сајбер преваре преко сајтова за упознавање и четовање, преваре у вези интернет куповине и аукције.

2.3. Операционално одређење предмета истраживања

Полазећи од теоријског одређења предмета истраживања, у операционалном погледу под појмом „кривично дело превара као модел извршења сајбер криминала" или скраћено „сајбер превара" у овој докторској дисертацији подразумеваће се: *лажно приказивање и прикривање података с циљем се себи или другоме прибави противправна имовинска корист и тиме другом лицу нанесе штета, где се компјутер или рачунарска мрежа употребљавају као средство или циљ, доказ или окружење извршења ове врсте преваре.*

2.3.1. Чиниоци предмета истраживања

Овако формулисан предмет истраживања је научно-теориски елаборирaн разрадом следећих структуралних чинилаца предмета истраживања:

Први структурални чинилац предмета истраживања обухвата: методолошки оквир истраживања са тежиштем на формулисању проблема истраживања, одређивању предмета истраживања, дефинисању циљева истраживања, формулисању хипотеза истраживања, одређивању начина истраживања и друштвене и научне оправданости истраживања.

Други структурални чинилац предмета истраживања обухвата теоријско одређење кривичног дела преваре са тежиштем на појмовном одређењу кривичног дела преваре, карактеристикама кривичног дела преваре, радњи извршења кривичног дела преваре и правној регулативи кривичног дела преваре у Републици Србији.

[16] Кривични законик Републике Србије („Сл. гласник РС", бр. 85/2005, 88/2005 – испр., 107/2005 – испр., 72/2009 и 111/2009).

Трећи структурални чинилац предмета истраживања обухвата теоријско одређење сајбер криминала, са акцентом на дефинисању појма „сајбер“, сајбер простор, сајбер криминал, опште карактеристике сајбер криминала и појавним облицима сајбер криминала.

Четврти структурални чинилац предмета истраживања односи се на:

појам кривично дело превара као модел остваривања сајбер криминала, са тежиштем на дефинисању појама преваре као модела остваривања сајбер криминала, класификацији превара као модела остваривања сајбер криминала, последице преваре као модела остваривања сајбер криминала и правној регулативи преваре као модела остваривања сајбер криминала.

Пети структурални чинилац обухвата начин извршења преваре као модела остваривања сајбер криминала, које обухвата социјални инжењеринг, употребу малициозних програма и комбиновани модел.

Шести структурални чинилац предмета истраживања обухвата профил сајбер превараната, мотиве сајбер превараната, класификација сајбер преваранта, психолошки профил сајбер превараната (аматера, хакери, оганизоване групе) итд. Предмет истраживања унутар овог структуралног чиниоца обухвата дескрипцију и научно објашњење начина откривања, разјашњавања и доказивања сајбер превара као и опис и објашњење места, друштвене улоге, функција, мисија, циљева, задатака, организације и надлежности државних органа у борби против сајбер криминала (посебно тужилаштва, службе за борбу против сајбер криминала, судова).

Седми структурални чинилац предмета истраживања односи се на надлежности државних органа у борби против сајбер криминала са акцентом на службу за борбу против сајбер криминала у оквиру МУП-а, посебном тужилаштву у случајевима сајбер криминала, организацији судова у случајевима сајбер криминала и главним активностима међународних органа и организација на пољу сузбијања сајбер криминала, као и међународној сарадњи у области сајбер криминала.

2.2.1 Временско, просторно и дисциплинарно одређење предмета истраживања

С обзиром да је прекретница у борби против сајбер превара и сајбер криминала била усвајање Конвенције Савета Европе о сајбер криминалу из 2001. године у Будимпешти,

предмет истраживања обухвата период од 2001. до 2016. године, односно период после ступања на снагу Конвенције Савета Европе о сајбер криминалу.

Полазећи од тога да су многе међународне организације као најризичније државе из којих се врше сајбер преваре означиле територије држава Западне Африке: Нигерија, Гана, Бенин, Обала Слоноваче, Того и Буркина Фасо, те Јужну Африку, Шпанију, Холандију и друге државе, *просторно,* предмет истраживања обухвата најчешће облике сајбер превара на територији Републике Србије, наведених и других држава.

Практично, узимајући у обзир да се кривично дело сајбер преваре остварује у сајбер простору као "заједници" сачињеној од мрежа компјутера у којима се елементи традиционалног друштва налазе у облику бајтова и битова, то предмет истраживања, просторно гледано, захвата "простор који креирају компјутерске мреже", како у Републици Србији, тако и простор компјутерских мрежа других земаља, пре свега, оних са којих се најфреквентније чине кривична дела сајбер превара.

Дисциплинарно, предмет истраживања припада пољу друштвено хуманистичких наука, научним областима правних и делимично информатичких наука, тежишно научним дисциплинама кривичног права, међународног кривичног права, кривичног процесноог права, сајбер права, компјутерског права, међународног привредног права, пословног права, финансијског права, компанијског права, сајбер форензике, међународног приватног права, права интелектуалне својине и права заштите података о личности.

Полазећи од мултидисциплинрности предмета истраживања, резултате овог истраживања моћиће користити више научних дисциплина које истражују овај проблем.

3. ЦИЉЕВИ ИСТРАЖИВАЊА

Основни циљ истраживања у овој докторској дисертацији јесте да се, пре свега, укаже на друштвени и научни значај темељног и објективног проучавања кривичног дела преваре као модела остваривања сајбер криминала као једне од најозбиљнијих безбедносних претњи које се одигравају у сајбер простору на почетку 21. века, те упозори научна и шира јавност на могуће последице и размере које могу попримити сајбер преваре у 21. веку.

3.1. Научни циљеви истраживања

Научни циљеви истраживања у овој докторској дисертацији су *дескрипција (опис), класификација и типологизација* начина остваривања сајбер криминала и појавних облика сајбер превара као начина остваривања сајбер криминала, те *научно откриће и научно објашњење* главних чинилаца сајбер превара у сајбер простору и *научна прогноза* даљег процеса развоја сајбер превара и могућих облика борбе против сајбер превара у ближој и даљој будућности.

3.2. Друштвени циљ истраживања

Основни друштвени циљеви истраживања јесу идентификација реалних безбедоносних претњи од сајбер превара; анализа директних и индиректних разлога несигурности сајбер простора и појаве сајбер превара; идентификовање главних актуелних и потенцијалних актера и начина њиховог деловања у сајбер преварама и стварање основе за успостављање концептуалног аналитичког модела за испитивање остваривости сајбер превара у сајбер простору Републике Србије и основе за редефинисање стратегије борбе против сајбер превара.

Истраживање ове области је од великог друштвеног значаја за конципирање платформе за унапређење прописа из области сајбер и компјутерског (рачунарског) права.

4. ХИПОТЕТИЧКИ ОКВИР ИСТРАЖИВАЊА

Хипотетички оквир истраживања садржи једну генералну хипотезу истраживања и шест посебних хипотеза са припадајућим појединачним хипотезама истраживања.

4.1. Генерална (општа) хипотеза

Генерална хипотеза истраживања гласи: *Економски и информатички прогрес, процес глобализације и развој саобраћајне инфраструктуре допринели су порасту сајбер криминала у свим државама света.*

4.2. Посебне хипотезе истраживања

Прва посебна хипотеза (Х-1) гласила је**:** *У правном систему Републике Србије кривично дело преваре је у основи добро регулисано, у складу са стандардима земаља које припадају континенталном правном систему.*

Појединачне хипотезе:

1) У правном систему Републике Србије кривично дело преваре је у основи добро регулисано, али су присутни проблеми у његовој практичној примени.

2) У правном систему Републике Србије кривично дело преваре је регулисано у складу са стандардима земања које припадају континенталном правном систему, али у практичној примени постоје недоследности.

Друга посебна хипотеза (Х-2) гласила је: *Кривичноправна и криминолошка теорија о сајбер криминалу у Републици Србији заостаје за савременом теоријом ове врсте криминалитета.*

Појединачне хипотезе:

1) У Републици Србији није на потребном нивоу развијена кривичноправна и криминолошка теорија о сајбер криминалу.

2) У Републици Србији кривичноправна и криминолошка теорија о сајбер криминалу заостаје за савременом теоријом ове врсте криминалитета.

Трећа посебна хипотеза (Х-2) гласила је: *Што су модалитети остваривања кривичног дела сајбер превара развијенији, то су и последице преваре као модела остваривања сајбер криминала веће.*

Појединачне хипотезе:

1) Развој компјутерске технологије, смањење ризика извршењем без физичког присуства у виртуелном свету и тешкоће у откривању утичу на повећање злоупотреба сајбер простора као средства масовне комуникације.

2) Доступност компјутерских технологија широком кругу корисника, повећава ризик извршења кривичног дела сајбер криминала без физичког присуства у виртуелном свету.

Четврта посебна хипотеза истраживања (Х-4) гласила је: *Лоша економска ситуација, недостатак сталног запослења, жеља за сигурном егзистенцијом и пад моралних вредности утичу на усавршавање начина извршења сајбер превара.*

Појединачне хипотезе:

1) У начинима извршења преваре као модела остваривања сајбер криминала присутан је модел социјалног инжењеринга.

2) У начинима извршења преваре као модела остваривања сајбер криминала доминира употреба малициозних програма.

3) У начинима извршења преваре као модела остваривања сајбер криминала у значајној мери присутан је конбиновани модел.

Пета посебна хипотеза истраживања (Х-5) гласила је: *Од профила сајбер превараната зависи поступак откривања и доказивања преваре као модела остваривања сајбер криминала.*

Појединачне хипотезе:

1) Од психолошког профила сајбер превараната зависе мотиви сајбер превара.

2) Постоји више врста сајбер превараната, од аматера и хакера до организованих сајбер криминалних група.

3) Откривање и доказивање сајбер превара зависи од модела остваривања сајбер криминала.

Шеста посебна хипотеза истраживања (Х-5) гласила је: *Успех борбе против сајбер криминала зависи од ефикасности државних органа Републике Србије, активности међународних организација и међународне сарадње релевантних субјеката на националном, регионалном и глобалном нивоу.*

Појединачне хипотезе:

1) Успех борбе против сајбер криминала зависи од ефикасности државних органа Републике Србије.

2) Ангажовањем посебног тужилаштва, судова и службе за борбу против сајбер криминала у оквиру Министарства унутрашњих послова, смањује се број неоткривених, неразјашњених и недоказаних сајбер превара.

3) Успех борбе против сајбер криминала зависи активности међународних организација.

4) Успех борбе против сајбер криминала зависи од развијености међународне сарадње релевантних субјеката на националном, регионалном и глобалном нивоу.

5. НАЧИН (МЕТОДЕ) ИСТРАЖИВАЊА

Формулација проблема и одређење предмета истраживања одредили су битне компоненте садржаја докторске дисертације на који ће се сазнање односити, а циљеви истраживања су одредили нивое очекиваног научног сазнања, док су индикатори повезани са хипотезама определили методе, технике, инструменте и поступке који ће бити прмењени у пракси истраживања у овој докторској дисертацији.

У изради докторске дисертације коришћене су следеће научне методе, технике, инструменти и поступци:

5.1. Основне методе сазнања и истраживања

Од основних метода сазнања и истраживања у овој докторској дисертацији коришћене су готово све методе, али је тежиште било на: методама анализе, синтезе, апстракције и конкретизације, генерализације и специјализације, методи класификације, дихотомији и индуктивно и дедуктивној методи.

Методом анализе је вршено растављање предмета истраживања на његове саставне чиниоце и начине извршења, појавне облике сајбер превара с тежиштем на последњих 10 година. У раду је примењена дескриптивна анализа (којом је описан предмет истраживања са тежиштем на опису чиниоца и својства сајбер превара) и експликативна анализа (која је допринела бољем схватању сајбер превара, њиховом научном објашњењу и сазнању правилности и законитости које се дешавају при сајбер преварама).

Методом сиснтезе извршено је спајања више чинилаца сајбер превара у једну целину, чиме смо дошли до сазнања сложених целина сајбер криминала преко појединачних и посебних делова, њиховим спајањем, односно стављањем у разне односе и везе.

Методом апстракције извршено је сазнавање општег у посебном довољне одређености да се могло издвојити и истражити као целина сајбер превара и сазнавање посебног у општем, као могућа издвојена целина сајбер криминала. Уз помоћ ове методе открили смо у деловима предмета анализе одредбе, својства, садржаје, облике и моменте одређеног степена општости односно посебности сајбер превара.

У области сајбер простора, сајбер криминала и сајбер превара сусрели смо се са апстрактним замислима које смо одређеном процедуром конкретизовали у друштвене реалности, кроз додавање, мењање обима и садржаја апстрактног појма сајбер криминала и његово приближавање конкретном појму сајбер превара.

Методом генерализације извели смо опште ставове, судове и закључке о сајбер преварама из посебних и појединачних ставова да би смо сазнали опште правилности и законитости у сајбер преварама и њих искористили за заснивање теорије о сајбер преварама.

Методом специјализације смо дошли до сазнања посебног и појединачног у општем сазнању о сајбер преварама, при чему је опште схваћено као целина састављена од чланова који су сви међусобно повезани извесним заједничким својствима, али су међу њима задржане евидентне разлике на основу којих смо могли идентификовати њихову посебност.

Методом класификације смо сазнали односе елемената сајбер превара међусобно и са целином сајбер криминала, дистанце и редоследе, те могуће ваљане критеријуме за раздеобе или сажимања. У дисертацији је извршена класификација начина остваривања сајбер криминала и појавних облика сајбер превара (поделе по начину извршења и оспособљености субјеката извршења).

Индуктивном методом смо дошли до сазнања о емпиријском, реално-конкретном и разноврсном, конституисаном у појединачне целине тј. извођење општег става из више посебних ставова о сајбер преварама. Само увидом у одређене појединачне целине, методом индукције смо омогућили образовање појмова, ставова и судова о сајбер криминалу и сајбер преварама.

Индукцији је претходила метода дедукције као аналитички и специјализаторски методшки поступак, којим смо из и на основу општег законског сазнања о сајбер преварама стекли посебна сазнања и то са неупоредиво већим степеном извесности и поузданости.

5.2. Општенаучне методе

Из корпуса општенаучних метода у овој докторској дисертацији су примењене хипотетичко-дедуктивна метода и компаративна метода.

Хипотетичко-дедуктивна метода је примењена како би се формирала постулациона основа евидентирањем разноврсних искустава стечених у борби против сајбер превара. Овом методом смо у истим и различитим ситуацијама уз више понављања упоредили и констатовали истоветности сајбер превара у периоду од десет година.

Компаративна метода је примењена за компарирање теоријског модела и практичних модалитета могућих сајбер превара и међусобно различитих модалитета њихових појавних облика. Такође, ова метода је коришћена за поређење сајбер превара и других безбедносних претњи у сајбер простору, као и за компарирање нормативних решења у пракси Републике Србије са упоредноправним решењима, како би се установиле идентичности, сличности и различитости правних и институционалних оквира на разним просторима.

5.3. Методе за прикупљање података

У докторској дисертацији, од метода за прикупљање података примењене су метода испитивање, применом технике интервјуа и то диригованог и индивидуалног интервјуа.

Испитаници су били запослени у служби за борбу против високотехнолошког криминала у оквиру Министарства унутрашњих послова и већа Окружног суда у Београду за борбу против високотехнолошког криминала, као и еминентни стручњаци и професори из области информатике и дигиталне форензике.

Њихова знања и искуства из области сајбер криминала су значајно допринела бољем сагледавању реалног функционисања сајбер превара, ефикасности постојећег законског и институционалног оквира у борби против сајбер превара и сајбер кримала у опште, и предлога за унапређење поступка откривања, разјашњавања и доказивања сајбер превара.

Од оперативних метода за прикупљање података у докторској дисертацији су коришћене метода студије случаја и метода анализе садржаја документа.

У оквиру *методе студије случаја* разматрани су најпознатији случајеви у низу „Нигеријске преваре“, или преваре позната под називом „превара 419“, у којима је заступљена техника социјалног инжињеринга и то: „Miss Wumi Abdul“ , „Orient Bank Nigeria

PLC“, „Charity distribution“, „ Use for the less privileged“, „Mrs Tema Williams“, „ Johnson Savimbi“, „Mother Sarah Alan Rowland“, „Engr David Koni , Sgt. „Joey Jones“ и „Mr. Wong Du“.

Приликом истраживања преваре са наградама анализирани су следећи случајеви који су однели највише жртава: „Фејсбукова наградна игра“, „ prime lottery international“, „ Eu commonwealth lottery promotions“, „ Google наградне игре и „ UK national lottery“.

Метода студије случаја коришћена је и за спознају преваре са злонамерним апликацијама, при чему су анализирани следећи случајеви: „верификација Твитера“, „Твитер верификација плавим бецом“, „случај – онемогућен приступ фејсбук налогу“, „случај – апликације које нуде могућност сазнавања ко посећује профил“, „случај – промена боје фејсбук налога“ и „ фишинзи усмерени на мобилне телефоне новије генерације“.

У докторској дисертацији примењена је и метода анализе садржаја докумената, и то обе њене технике квалитативна и квантитативна анализа садржаја докумената са израдом једног динамичког инструмента - кодекса појмова и шифара о кривичном делу преваре као моделу остваривања сајбер криминала.

У изради докторсе дисертације анализирани су:

- научни и стручни радови који се, посредно или непосредно, баве проблемом превара, сајбер криминала, сајбер простора и безбедносним претњама у сајбер простору;
- научни и стручни истраживачки пројекати из ове области;
- позитивноправни прописи (национални, регионални и међународни)
- институционални извори (статистички извештаји, документа из архива државних институција);
- евиденције компанија и других организација, извештаји осталих релевантних институција;
- евиденције државних и међународних тела задужених за праћење високо-технолошког криминалитета, међународни документи, конвенције, протоколи, међународни уговори и други акти, који су директно или индиректно везани за проблем сајбер претњи у сајбер простору.

6. ДРУШТВЕНА И НАУЧНА ОПРАВДАНОСТ ИСТРАЖИВАЊА

6.1. Научна оправданост истраживања

Овај вид криминала за разлику од других не представља још увек заокружену феноменолошку категорију, те су у овој области изостале дефиниције и прецизна одређења категоријално-појмовног система.

Отуда се научна оправданост ове дисертације изражава, пре свега, као допринос у спознаји саме појаве кривичног дела преваре као модела остваривања сајбер криминала, њеном разликовању од осталих модела остваривања сајбер криминала, као и у сагледавању њеног места и значаја у области кривичноправних наука.

Такође, научна оправданост истраживања у овој дисертацији повезана је са претпостављеним доприносом науци кроз верификаторне резултате истраживања облика сајбер превара (проверу и постављање нових хипотеза), чиме је дат допринос методологији, логици и истраживању појавних облика сајбер превара.

У том смислу, научна оправданост резултата истраживања у овој докторској дисертацији се може изразити и као допринос научној теорији кривичног права.

6.2. Друштвена оправданост истраживања

Као веома специфичан облик преваре који има међународне размере и изазива оштећења која се могу исказати стотинама милиона америчких долара, сајбер превара заслужује посебну пажњу и анализу.

Експанзију сајбер криминала, и сајбер превара као његовог појавног облика показују подаци компаније за рачунарску безбедност Symantec, произвођача антивирусног софтвера Norton, сајбер криминалом у свету у 2011. години био је погођен 431 милион људи, уз финансијску штету од 14 милијарди долара. Према наводима у истом извештају Symanteca, више од две трећине одраслих у свету користе Интернет, или прецизније 69 одсто њих, било је некад у свом животу жртва сајбер криминала, што значи да је милион људи дневно

погођено тим незаконитим радњама.[17]

Сајбер право није развијено у Републици Србији. Ово истраживање има за циљ да кроз анализу преваре као модела остваривања сајбер криминала укаже на нужност правног регулисања сајбер простора и стварања и примене сајбер права, како би Интернет и остале мреже биле правно регулисана поља, а не изворишта криминала које штети како појединцу, компанијама, тако и целокупном друштву.

[17] Више о томе: Symantec, Cybercrime Report for 2011, http://www. symantec.com/content /en/us/home_homeoffice/html/ cybercrimereport/, последњи пут приступили 12.04.2016. године

1. ТЕОРИЈСКО ОДРЕЂЕЊЕ КРИВИЧНОГ ДЕЛА ПРЕВАРЕ

1.1. ПОЈАМ КРИВИЧНО ДЕЛО ПРЕВАРЕ

Кривично дело преваре спада у класична кривична дела против имовине, а која су систематизована у посебну групу кривичних дела.

Још је Римско право познавало правни институт „*dolus*" за означавање преваре и зле намере. Тај термин су римски правници користили за лукаво и преварно поступање учињено у настојању да друго лице буде заведено, преварено и оштећено. Долозно понашање дефинише се као: „свака намерно учињена радња с циљем да се друга страна доведе у заблуду или одржава у заблуду и имовински оштети". За разлику од обичне заблуде (*error*), овде се улазило у питање кривице онога који је својим преварним понашањем довео другу страну до погрешне представе о неком битном елементу правног посла и тиме је стекао корист на штету његове имовине".[18] Како би се изворном термину *dolus* додао негативни смисао користи се атрибут *malus* (зао,лош).

У зависности од намере учиниоца, разликујемо два облика преваре – ако извршилац намерава да обманом прибави себи или другом противправну имовинску корист, постоји основни облик преваре, а ако примењује обману само у намери да другог оштети, постоји лакши облик преваре. Та дистинкција прави се и у Кривичном законику Републике Србије, у ком се у члану 208 предвиђају различите санкције за та два вида преваре. У члану 208, ставу 2 наводи се: „Ко дело из става 1. овог члана учини само у намери да другог оштети, казниће се новчаном казном или затвором до шест месеци."[19]

Амерички аутори кривичног права су на екстензиван начин дефинисали кривично дело преваре: „Превара је свесно изазивање, појачавање или одржавање погрешне представе о неком елементу правног посла код другог лица, како би се лице намерно довело у заблуду да учини изјаву воље коју иначе не би учинило. Превара обухвата активну радњу лица које је врши, али и прећуткује, намерно необавештавање, одржавање у заблуди другог учесника у

[18]Бујуклић, Ж., *Форум Романум, Римска држава, право,религија и митови*,Правни факултет Универзитета у Београду и Службени гласник,Београд,2007,стр. 269-271.

[19] Кривични законик Републике Србије („Службени гласник Републике Србије", бр. 85/2005, 88/2005 и 107/2005), члан 208.

правном послу. Да би превара постојала потребно је постојање узрочне везе између преваре и изјаве воље."[20]

Превара се појављује и у међународном праву, а постоји ако је једном међународно правном субјекту, односно органу свесно успело да погрешним информацијама, лажним приказивањем, кривотвореним исправама, географским картама и сл. наведе други субјекат на склапање уговора и тада правни послови нису ваљани.[21]

Превара у грађанскоправном смислу не мора да садржи елементе појма превара у кривично правном смислу. У правном послу закљученом преваром оштећени има могућност поништаја на захтев правно заинтересованих лица. Уколико су закључени преваром, правни послови су рушљиви, тј. не производе правна дејства. За те послове важи римско правило „*Fraus omnia corrumpit*" (Превара све квари) и свака превара, без обзира на то од кога потиче, утиче на пуноважност правног посла.

Као најкарактеристичнији и најучесталији облици превара у савременом свету се наводе:

1) интернет преваре, које су настале с појавом интернет мреже, тако што се преко интернет мреже пласирају информације које нису истините с намером да се неодређени број лица доведе у заблуду;

2) превара у вези с уговорима о пружању туристичких услуга.

3) организоване преваре.

4) пореске преваре, чији је циљ изигравање закона избегавањем плаћања пореза.[22]

[20] Више о томе: Jescheck, H., *Lehrbuch des Strafrechts*, Berlin, 1972, str.122.

[21] Више о томе: Balkan, S., Berger,R., Schmidt, J., *Crime and deviace in America, A crecital approach*, California, 1977, str.201.

[22] Више о томе: Вујовић, И., *Превара у савременом уговорном праву* – докторска дисертација одбрањена на Правном факултету Универзитета у Београду, 2009.

1.2. РАДЊА ИЗВРШЕЊА И ОПШТЕ КАРАКТЕРИСТИКЕ КРИВИЧНОГ ДЕЛА ПРЕВАРЕ

Радња је одређено понашање човека у спољном свету и основни елемент у појму друштвено опасног дела за чије постојање је битно да су испуњени објективни и субјективни услови. Објективан услов обухвата манифестацију акта, док се субјективан услов односи на вољно предузимање.[23] Радњом кривичног дела извршава се кривично дело и то је она радња која је у опису кривичног дела означена као радња извршења.

Постоје две врсте кривичних дела: кривична дела чињења и кривична дела нечињења. Кривична дела чињења (*delicta commissiva*) врше се у највећем броју случајева и учинилац поступа супротно норми која забрањује предузимање извесне делатности, односно, предузимањем те делатности проузрокује одређену забрањену последицу. Кад се ради о кривичном делу нечињења (*delicta ommissiva*), учинилац пропушта, односно, уздржава се да поступи по норми која наређује предузимање извесне делатности и тиме проузрокује забрањену последицу. [24] Код је реч о кривичним делима нечињења, прави се подела на:
1. права кривична дела нечињења, која се могу вршити само пропуштањем предузимања одређене делатности, нечињењем;
2. неправа кривична дела нечињења, а то су кривична дела која се иначе врше чињењем, с тим што се у одређеним случајевима могу извршити и нечињењем.[25]

Кад се ради о кривичном делу преваре, она се састоје у навођењу неког лица на то да учини или не учини нешто што је штетно за његову или туђу имовину, а састоји се у обмани. Према томе, свако навођење другог да на штету своје или туђе имовине нешто учини или не учини, не чини ово кривично дело уколико то није учињено на преваран начин. У закону су као начини извршења преваре изричито наведени: лажно приказивање или прикривање чињеница, довођење у заблуду или одржавање у заблуди неког лица.

Обмана је довођење у заблуду и може се остварити на различите начине. Закон их на уопштен начин наводи као лажно приказивање чињеница или као прикривање чињеница.

[23] Више о томе: Welzel, H., *Deutsches Strafrech*, Berlin, 1954, str. 92.

[24] Више о томе: Gerraud, R., *Traite theorique et pratique de droit penal francais*, Paris, 1924, str. 40.

[25] Више о томе: P. Bouyat – Pinatel, J., *Traite de droit penal et de criminologe*, Paris, 1970, str.52.

Обмана се врши, нпр., представљањем као постојећег нешто што у опште не постоји, тврђењем нечег што није стварно или истинито, затајивањем чињеница или недостатака, прикривањем мана и недостатака, али и конклудентним радњама, када се из самог представљања једне чињенице нормално подразумева постојање неке друге чињенице, тако да непостојање увек представља обману.[26]

Навођење се дефинише као стварање одлуке код другог лица да предузме или да се уздржи од предузимања неке делатности. Да би се нешто сматрало преваром, навођење неког лица обманом да нешто учини или не учини на штету своје или туђе имовине треба да се врши у намери прибављања за себе или другог неке противправне имовинске користи. Навођење се може вршити на три начина: довођењем неког лица у заблуду, одржавањем неког лица у заблуди и коришћењем заблуде.[27]

Довођење у заблуду може да се изврши лажним приказивањем или сакривањем извесних чињеница, прикривањем чињеница,чиме се код другог ствара погрешна представа како би на штету своје или туђе имовине нешто учинио или не учинио.[28]

Постоје различита становишта у вези с питањем одржавања у заблуди. Једно од њих је да:„Одржавање неког лица у заблуди означава делатност којом се неко лице, које се већ налази у заблуди, одржава у таквом стању погрешног убеђења, скривањем извесних чињеница, односно њиховом лажном приказивању.” Са друге стране, поједини аутори се залажу за мишљење да одржавање у заблуди не значи поступање у правцу обмањивања неког, односно у правцу стварања погрешне представе неког о нечему, већ погрешна представа постоји и без утицаја учиниоца кривичног дела преваре. [29]

Конститутивно обележје кривичног дела преваре је начин њеног вршења– лажно приказивање чињеница и прикривање чињеница.

[26] Више о томе: Таховић, Ј., *Кривично право*, посебан део, Београд, 1953, стр. 348.

[27] Више о томе: Вучковић, В., *Кривично дјело преваре*, Обод, Цетиње,2003, стр.88-90.

[28] Више о томе: Чејовић, Б., *Кривично право у судској пракси*, посебан део, књига друга, Београд, 1986, стр.785-786.

[29]Више о томе: Чејовић, Б., *Кривично право*, посебан део, Београд, 2002, стр. 320.; Атанацковић, Д., *Кривично право*, посебан део, Београд, 1978, стр. 296.

Лажно приказивање чињеница као начин довођења у заблуду или одржавања у заблуди подразумева тврдњу да постоји нека чињеница која не мора да постоји или се пак постојећа чињеница приказује другачијом него што јесте. Тврдња се састоји у убеђивању, а може да се врши посредно стварањем такве ситуације из које ће произаћи закључак о постојању неке чињенице која иначе не постоји. То се може односити како на постојеће чињенице, тако и на оне које су постојале а и на оне будуће. Лажно приказивање може се састојати у нечињењу, нпр., у непорицању нечијег тврђења ћутањем ако је постојала правна обавеза на изјашњавање о извесној тврдњи.

Под прикривањем чињеница подразумева се спречавање да друго лице сазна чињенице које би га одвратиле од неког чињења или нечињења. Прикривање се врши чињењем (нпр., неки недостаци робе понуђене на продају учине се неприметним) или нечињењем (нпр., прећуткивањем мана и недостатака кад је постојала обавеза да се саопште извесне чињенице или својства ствари).[30] Разлика између лажног приказивања чињеница и прикривања чињеница је у томе што се при лажном приказивању чињница настоји да се неко лице увери у постојање неких чињеница које не постоје, или се пак постојеће чињенице приказују другачијим него што јесу, док се при прикривању чињеница лице спречава да сазна одређене чињенице. Заједнички именитељ лажног приказивања чињеница и прикривања чињеница је да је неко лице обмануто о стварности.

Превара се може извршити према физичком и према правном лицу. Оштећени у случају овог кривичног дела може да буде и лице које се наводи на чињење или нечињење али и неко друго лице чија се имовина оштећује. Оштећени је лице према ком се превара врши и који трпи штету. Циљ преваре је обично материјална корист, али може да буде и нешто друго, на пример: освета, сузбијање конкуренције, наношење некоме штете из зависти итд.

Преваре, ако нису крајње очигледне, прилично тешко се откривају и доказују јер их грађани не пријављују – што из страха да су саучесници у нечему недозвољеном – што из убеђења да су сами криви због своје лаковерности и наивности.

[30] Коментар Кривичног закона Србије, група аутора, Београд, 1995, стр. 618.

1.3. ПРАВНА РЕГУЛАТИВА КРИВИЧНОГ ДЕЛА ПРЕВАРЕ У РЕПУБЛИЦИ СРБИЈИ

У Кривичном законику који је ступио на снагу 1. јануара 2006. године, у поглављу XXI, под називом „Кривична дела против имовине", у ставу 1 члана 208. кривично дело превара дефинише се на следећи начин: „Ко у намери да себи или другом прибави противправну имовинску корист доведе кога лажним приказивањем или прикривањем чињеница у заблуду или га одржава у заблуди и тиме га наведе да овај на штету своје или туђе имовине нешто учини или не учини, казниће се новчаном казном или затвором до три године."[31]

За ово кривично дело законодавац је прописао новчану казну или казну затвора до шест месеци ако је дело учињено само у намери да се друго лице оштети. У случају да је овим делом прибављена имовинска корист или је нанета штета у износу који прелази 450.000,00 динара, извршиоца следује казна затвора од једне године до осам година, а ако прибављена имовинска корист или је нанета штета која прелази 1.500.000,00 динара предвиђена казна је затвора од две године до десет година.

Новим законом о изменама и допунама Кривичног законика од 31.08.2009. године, који је објављен у „Службеном гласнику Републике Србије" бр. 72-09, а који је ступио на снагу дана 08.09.2009. године, чланом број 68. предвиђене су измене у члану 208, где су у ставу 1 речи: „новчаном казном или затвором до три године" замењене речима: „затвором од шест месеци до пет година и новчаном казном". У ставу 2 речи: „новчаном казном или затвором до шест месеци" замењене су речима: „*затвором до шест месеци и новчаном казном*".[32]У ставу 3, после речи: „осам година" додате су речи: „и новчаном казном", а у ставу 4 су после речи: „десет година" додате речи: „и новчаном казном".

На основу изнетог можемо закључити да је у правном систему Републике Србије кривично дело преваре је у основи добро регулисано, у складу са стандардима земаља које припадају континенталном правном систему, што пружа добру полазну основу на путу кажњавања и искорењивања ове појаве.

[31] Кривични законик Републике Србије („Службени гласник Републике Србије", бр. 85/2005, 88/2005 и 107/2005).

[32] Закон о изменама и допунама Кривичног законика, „Службени гласник РС", бр.72/2009 од 3. 9. 2009.године. (члан 68).

2. ТЕОРИЈСКО ОДРЕЂЕЊЕ САЈБЕР КРИМИНАЛА

2.1. ПРЕФИКС „САЈБЕР“

Префикс ,,сајбер” (или кибер) учестало се користи кад год је потребно створити нове термине повезане с рачунарима, рачунарским мрежама и, у ширем смислу, с виртуелном стварношћу. Први га је употребио амерички научник Норберт Винер (Nobert Winer), у другој половини четрдесетих година XX века, у својим истраживањима која су представљала основу нове научне дисциплине кибернетике, као целе области теорије управљања комуникација.[33]

Кибернетика је научна дисциплина која проучава живе и неживе системе, њихову структуру (рецепторе, меморију, програме и ефекторе), комуникационе могућности, принципе деловања, а посебно механизме контроле, регулације и ауторегулације стања равнотеже путем повратне везе. Кибернетика настоји да развије метод управљања неким системом који ће се користити иформацијама о ранијем деловању система за корекцију садашњих операција, као и у планирању будућих.[34] У књизи *Cybernetics, or control and communication in the animal and machine,* објављеној 1948. године, Винер је указао на то да научни и технички прогрес имају огромне и сложене друштвене последице. Префикс сајбер очито указује на изузетну сложеност, непрекидност интеракција, неограниченост простора и неогрничен број различитих услуга, непрестано наилажење на нешто ново и неочекивано, у свету рачунарских мрежа.

У књижевности појам ,,сајбер“ се везује за термин "*cyberpunk*", који се први пут појавио у краткој причи "*Cyberpunk*" аутора Бруса Беткеа (Bruce Bethke), објављеној новембра 1983. године у магазину "Amazing", који објављује научно-фантастичне приче. Радња приче врти се око скупине тинејџера хакера. Према речима самог аутора, његова намера је била чисто маркетиншка. Желео је у наслову једносложну реч која ће бити лако памтљива. Тако је у наслову спојио кибернетику као комуникацијску науку и панк као анархистички покрет младих, који је био доминантан 1970-их.

[33] Више о томе: Винер, Н., *Кибернетика или управљање и комуникација код живих бића и машина*, Издавачко-информативни центар студената, Београд, 1972, стр. 9.

[34] Више о томе: Требјешанин, Ж., *Речник психологије*, Стубови културе, Београд, 2004, стр. 217.

У домаћој литератури, многи аутори инсистирају на употреби речи ,,кибер" уместо сајбер, мислећи да тиме бране чистоту српског језика, што није оправдано будући да су готово сви термини рачунарских технологија енглеског порекла. Пошто се префикс ,,сајбер" везује за термин кибернетика (*cybernetics*), отуда у свакодневној пракси долази до сукобљавања око термина ,,сајбер" или ,,кибер". Префикс ,,кибер", који је присутан у руској, немачкој и хрватској литератури, потиче од речи „кибернетика", а која потиче од старогрчке речи ,,кибернетикос" (κυβερνητικος), која има значење управљати, руководити, кормилати. Њен англосаксонски изговор је „сајбер",а словенски и германски „кибер".

2.2. САЈБЕР ПРОСТОР

Реч ,,простор" има различито значење у различитим научним дисциплинама, те је стога тешко наћи универзалну, општеприхваћену дефиницију. Простор је један од основних квантитета у науци који не може да буде дефинисан ппутем других квантитета, као што су сила или енергија, које су већ дефинисане путем простора. У *Речнику* Матице српске, простор се дефинише као неограничена протегнутост, растојање у свим димензијама и правцима.[35]

Термин ,,сајбер простор" први је употребио Вилијам Гибсон 1984. године у научнофантастичном роману *Неуромант*.[36] По Гибсону, сајбер простор је универзум рачунарских мрежа, дигитални свет у којем се мултинационалне компаније, друштва и информатичари–пирати боре за освајање података и информација. Синтагму ,,сајбер простор" Гибсон види као универзум рачунарских мрежа рачунара у којој се елементи класичног друштва налазе у облику битова и бајтова, односно као простор који креирају рачунарске мреже.[37]

Префикс сајбер очито указује на изузетну сложеност, непрекидност интеракција, неограниченост простора и неограничен број различитих услуга, непрестано наилажење на

[35] Више о томе: *Речник српскохрватског књижевног језика* (књига пета), Матица српска, Нови Сад, 1973, стр. 226-227.

[36] Више о томе: Гибсон, В., *Неуромант*, IPSMedia, Београд, 2008.

[37] Више о томе: Дракулић, М., Дракулић, Р., *Сајбер криминал*, www.bos.org.yu/cepit/idrustvo/sk/cyberkriminal.pht, последњи пут приступили 12.04.2016.године

нешто ново и неочекивано, у свету рачунарских мрежа. Сајбер простор у суштини представља глобално повезану информационо-комуникациону инфраструктуру. То је вештачка творевина настала као резултат друштвених потреба и технолошких иновација. Пружа огромне могућности и у информационом друштву представља доминантан медиј комуникације. То је простор различитих садржаја, лак за коришћење. У сајбер простору још увек нису сва правила потпуно дефинисана и нови креативни процеси и даље ће се дешавати. Сајбер простор представља нову форму јавног места, које пружа могућност за изражавање, обезбеђује слободу кретања, за разлику од физичког простора, који има одређене димензије, границе, збијеност и друге ограничавајуће факторе.[38]

Иако се сајбер простор најчешће перципира као нематеријално краљевство података или као нека врста виртуелне стварности, он заправо има и сасвим физичку инфраструктуру, сачињену од жица које се налазе изнад и око наших глава, каблова који леже поред наших ногу и сателита на небу који круже око наше планете, а што омогућава интеракцију која на нивоу сензација материјализује квалитет нематеријалности, којим сајбер простор најчешће описују његови конзументи. [39] Он представља алтернативну просторну димензију унутар које се успоставља веза између различитих персоналних рачунара, рачунарских мрежа, различитих виртуелних заједница и појединаца који могу, али и не морају да буду њихови чланови при чему настаје симулирана реалност као последица интеракције људског и артифицијелног интерфејса.[40]

У теорији су присутне следеће дефиниције сајбер простора, и то да он представља:
– ,,електронски медиј рачунарских мрежа, у којем се остварује онлајн комуникација”[41];
– ,,нематеријални простор заснован на информационо-комуникационој технологији”[42];
– ,,место на коме функционишу рачунарски програми и крећу се подаци”[43], или као

[38] Више о томе: Jones, S., *Virtual Culture-Identity and Communication in Cybersociety*, SAGE Publications, London, 1997, p. 25,36.

[39] Више о томе: Arquilla, J., & Ronfeldt, D., *Cyberwar is coming!*, RAND Corporation, 1992, p.9

[40] Више о томе: Мимица, А., Богдановић, М., *Социолошки речник*, Завод за уџбенике, Београд, 2007, стр. 60.

[41] Више о томе: *The Free Dictionary* http/www.thefreedictionary.com/cyberspace, последњи пут приступили 12.04.2016.године

[42] Више о томе: *Origins of the word cyberspace*, http/encyclopedia.thefreedictionary.com/cyberspace, последњи пут приступили 12.04.2016.године

Речнику *Webopedia,* http://www.webopedia.com/, последњи пут приступили 12.04.2016.године

– ,,глобална заједница где живе рачунарски повезане индивидуе и групе”[44].

Наведене дефиниције, у суштини, повезују сајбер простор с рачунарским мрежама. Сајбер простор, дакле, представља нематеријалан, неограничен интерактивни простор сачињен од рачунарских мрежа. Стварање сајбер простора омогућују Microsoft, CISCO и друге компаније које производе савремене уређаје информационо-комуникационе технологије.

Сајбер простор је место где се хиљаде група људи састају да деле информације, дискутују о заједничким стварима, обављају посао. Неке од тих група су велике и добро развијене, али неки критичари тврде да те групе не могу да представљају праве заједнице, док други сматрају да имају могућности да подрже традиционалне (*face-to-face*) заједнице и помажу да се локалне заједнице држе заједно. Комуникација се и унутар сајбер простора успоставља тренутно, при чему је физичка локација корисника најчешће потпуно неважна. Баш као и физички простор, сајбер простор садржи ентитете, тј. информације (различитих облика, попут порука, електронске поште, веб-сајтова, фајлова итд.), који могу да буду транспортовани, испоручени или преузети. Критичари описују онлајн заједнице као више изоловане него стварне (*real-life*) групе.[45] Одређени аутори изражавају страх да ће велико учешће у виртуелним заједницама удаљити људе од учешћа у стварним заједницама (породице, пријатеља).

Сајбер простор успешно подржава друштвене везе између људи који се не могу често виђати. Виртуелне заједнице разликују се од реалних заједница по томе на чему учесници заснивају своје везе. Људи на мрежи имају већу тенденцију да заснивају осећања блискости на заједничким интересима пре него на заједничким друштвеним карактеристика као што су пол и друштвено-економски статус. Те заједнице су вероватно хомогеније у својим интересима и ставовима, али су вероватно хетерогеније по питању година, друштвеног

[43] Више о томе: Collin, B., *The Future of Cyberterrorism*, http/afgen.com/terrorism1.html, последњи пут приступили 12.04.2016.године

[44]Више о томе: Hutchinson encyclopedia, http/encyclopedia.farlex.com/cyberspace, последњи пут приступили 12.04.2016.године

[45] Kollock, P., Smith, M., ,,*Communities in cyberspace*, Routledge, New York, 2001, p. 3–17.

статуса или националне припадности.[46] Због предоминације енглеског језика, који се успоставља и као језик нове писмености, сајбер простор је упркос својој отворености управо простор у којем западни свет потврђује своју доминацију. Због глобалистичке концентрације, која му је битна одлика, сајбер простор представља претњу националним културама и националним идентитетима, јер обликује готово сваки сегмент живота грађана, укључујући ту и забаву, потрошњу, образовање, политички ангажман и друго. То је универзум који пружа илузију анонимности, а који, у ствари, зависи од реалне инфраструктуре (одређених институција, комерцијалних интереса, реалних односа моћи).[47]

У свакодневном говору „сајбер простор" се најчешће користи као синоним за интернет, полазећи од става да он обухвата онлајн свет интернета (рачунарских мрежа) али и дигитални свет уопште.[48] . Интернет представља интерконекцију милиона рачунара у целом свету, а сваким од њих независно управљају појединци или организације који су изабрали да се прикључе општим протоколима комуникације, нарочито протоколима познатим као TCP/IP (*TransmissionControlProtocol/InternetProtocol*). Протоколи TCP/IP чине могућим интернет, а њихова основна карактеристика је дефинисање мреже која ради на основу размене пакета, метода помоћу којег се подаци пре слања деле на стандардизоване пакете, а који се затим шаљу на одредиште. Трасирање путање (*routing*) обавља се помоћу безбројних посредничких диспозитива (*router*). Када један од тих посредника прими пакет података, чија дестинација није рачунар у локалној мрежи, шаље га према неком другом рутеру оптималним путем. Рачунар пошиљалац и рачунар прималац не морају да знају ништа о путањи којом пакети путују, а чест је случај да различити делови информације путују различитим путањама. Још важније је да, с техничког гледишта, рачунари у мрежи могу

[46] Више о томе: Wellman, B., Gullia, M., *Virtual communities as communities – Net surfers dont ride alone*; Kollock, P., Smith, M., *Communities in cyberspace*, Routledge, New York, 2001, p. 181–186.

[47] Више о томе: Томић, З., *Сајбер простор и проблеми разграничења*, „Култура", бр. 107–108, Завод за проучавање културног развитка, Београд, 2004, стр. 10–13.

[48] Више о томе: Tipton, H., Krause, M., *Information Security Management Handbook* (fifth edition), CRS Press, New York, 2004, p.3171.

Computing Dictionary, http/computingdictionary.thefreedictionary.com/cyberspace, последњи пут приступили 12.04.2016.године

Encarta encyclopedia, htpp/encyclopedia.msn.com/encyclopedia_761582824/Cyberspace.html, последњи пут приступили 12.04.2016.године

Тасић, В., Беуер, И., *Речник компјутерских термина*, Микро књига, Београд, 2003, стр. 125

комуницирати без икаквог познавања технологије мреже која преноси податке. Коришћење стандардизованих протокола TCP/IP даје илузију кориснику интернета да је он део јединствене велике мреже, иако је, у суштини, интернет збир независних мрежа. Заправо, појединци, државе и институције власници су делова комуникационих канала или рачунарске и комуникационе опреме које се користе на интернету. При томе, власник рачунара сам бира начин прикључења на интернет, количину и врсту информација које ће преузимати, као и властите садржаје које ће учинити доступним осталим корисницима мреже.

Са друге стране, поистовећивање сајбер простора са Интернетом по многим стручњацима из области високотехнолошког криминала није оправдано. Први аргумент састоји се у тврдњи да је појам „сајбер простор" шири од појма „интернет" будући да обухвата и друге типове мрежно повезаних рачунарских система (као што су, на пример: интранет, LAN, WAN итд.). Други аргумент је онтолошке природе. Према њему, та два појма описују две другачије стварности: док интернет представља прецизну технолошку инфраструктуру, сачињену од физички постојећих елемената, кибер простор односи се на не-физичку димензију, нематеријални простор створен информационом инфраструктуром, када се она користи за размену информација.

Међутим, имајући у виду да интернет представља највећи информационо-комуникациони систем међусобно повезаних рачунарских мрежа, и то како по величини, тако и по броју корисника, намењен размени података различитих типова, аутор овог текста сматрамо да је оправдано појам „сајбер простор" поистовећивати с интернетом.

Специфична категорија претњи са префиксом „сајбер" су, као и традиционалне претње, усмерене против ИК система и информација које су садржане у њима, али су извори ових претњи и средства неопходна за њихову експликацију везани за сајбер простор. Другим речима, њихово манифестовање омогућено је стварањем глобалне рачунарске мреже. То је, дакле, њихово дистинктивно обележје. Велике силе, нпр. САД, посматрају сајбер простор као ново, пето подручје ратовања (поред копна, мора, ваздуха и космоса). Он сматра да се претње у сајбер простору могу градирати од ометања комуникационих система па све до губитка борбених способности.[49]

[49] Више о томе: Wagner, B., *Electronic Jihad*, National Defense, National Defense Industrial Association, July 2007, p. 35.

Под појмом ,,сајбер претња“ експлицитно се подразумева ,,злонамерна употреба технологија која припадају сајбер простору као инструмената претње, али и као циљева од стране великог броја актера-криминалаца, терориста, организација и држава. У најопштијем смислу, безбедносна претња у сајбер простору може се рашчланити на две компоненте: начин изазивања (технике и инструменти) и субјект (актер) претње. Начин изазивања претње представља прави механизам претње, док је субјект претње особа или организација која иницира настанак претње или извршава акцију.

У односу на начин изазивања сајбер претњи, тј.технике и инструмента који се користе у циљу њиховог остваривања, претње је могуће груписати у 2 групе. У досадашњим истраживањима у подручју сајбер безбедности, безбедносне претње у сајбер простору најчешће се поистовећују са сајбер нападима техничког типа (тј. нападе помоћу малициозних програма или нападе усмерене на опструкцију услуга) и оним нападима у сајбер простору који се заснивају на обмањивању других корисника сајбер простора и злоупотреби њиховог поверења (сајбер преваре).

2.3. САЈБЕР КРИМИНАЛ

Криминалитет је општа друштвена појава, која је присутна у свим државама и друштвеним заједницама света без обзира на њихово друштвено-економско уређење и политички систем. Ова негативна друштвена појава, стара колико и људско друштво, која је постојала још у племенским родовским заједницама, развијала се упоредо с државом и правом уопште пратећи напредовање и изуме људског рода. У различитим државама постоје различити облици криминалитета, који се разликују по обиму и структури, као и већем или мањем распрострањењу.[50]

У правној теорији криминалитет се дефинише као појава у друштву која се манифестује у вршењу друштвено опасних дела која су законом утврђена као кривична дела.[51]

[50] Више о томе: Алексић, Ж., Миловановић, З., *Лексикон криминалистике*, Глосаријум, Београд, 1995, стр. 142.

[51] Више о томе: *Правна енциклопедија*, Савремена администрација, Београд, 1985, стр. 675.

Речник српскохрватског књижевног језика (књига трећа), Матица српска, Нови Сад, 1969, стр. 71–72.

Ова негативна друштвена појава се може састојати од више чињења или нечињења једног лица или више лица, тј. криминалне праксе, на одређеном простору, која су инкриминисане у позитивним законским прописима, а за чије непоштовање следује кривична санкција, чија врста и висина зависе од степена друштвене опасности конкретне инкриминације.Сходно наведеном, криминална радња постоји ако су испуњени следећи услови:

1) повређеност позитивне законске одредбе;
2) постојање извршиоца криминалне радње;
3) постојање жртве која је оштећена извођењем кривичне радње, и то било да је реч о појединцу, групи, или институцији.

Савремени криминалитет, који карактерише висок степен организованости и трајног ширења на унутрашњем и на међународном плану, представља сигурносни проблем и озбиљну претњу економској и социјалној стабилности и сигурности сваке државе и међународне заједнице.

Једна од најобухватнијих класификација криминалитета је на следеће типове:

1) „насилнички криминалитет (*violent crime*), тј. криминалитет извршен против особа,укључујући ту убиство, силовање, напад и телесне повреде;
2) имовински криминалитет (*property crime*),тј. криминалитет извршен против имовине, укључујући ту крађу, провалу и подметање пожара;
3) криминалитет против јавног реда (*public order crime*), тј. понашање које је означено као криминално зато што је у супротности с утврђеним друштвеним вредностима, обичајима и нормама, као што су, нпр., проституција и коцкање;
4) криминалитет белих крагни (*white-collar crime*), тј. ненасилнички криминалитет који извршавају корпорација и појединци ради добијања личне или пословне предности;
5) организовани криминалитет (*organized crime*), тј. злочиначко удруживање између појединца или криминалних група ради трговине нелегалним производима и услугама, као што су незаконита трговина дрогом или ватреним оружјем;
6) високотехнолошки криминалитет (*high-tech crime*), који је директно повезан с повећаном употребом рачунара у свакодневном животу, а у који се убрајају следећа дела: продаја порнографског материјала преко интернета, искоришћавање

рањивости рачунара одређене компаније ради рачунарске саботаже, крађа одговарајућих података коришћењем рачунара и рачунарских мрежа“.[52]

Глобална рачунарска мрежа отворила је нове могућности за извршавање криминалних дела. Интернет, који је по својој природи рањив и несигуран, услед огромног броја корисника, отворености и правне нерегулисаности, постао је полигон, али и идеално скровиште за криминалце различитог типа. У литератури се могу уочити схватања по којима сајбер криминал подразумева „криминалне прекршаје који су створени или омогућени развојем ИКТ или традиционални криминал који је трансформисан употребом рачунара тако да је лицима које спроводе истрагу неопходно познавање рачунара”. Поред дела против безбедности рачунарских података, обухвата и традиционалан криминал трансформисан развојем ИКТ (нпр., крађа идентитета).[53]

Међутим, ово одређење сајбер криминала не задовољава методолошка правила дефинисања, не указује на улогу рачунарске мреже и друге битне елементе сајбер криминала. Имајући у виду претходна сагледавања појма сајбер криминала, посебно различитост у приступима појединих аутора, неопходно је имати веома широк приступ приликом дефинисања ове врсте криминалног понашања. Наиме, једна свеобухватна дефиниција мора инкорпорисати три битна елемента: начин извршења, средство извршења и последицу криминалног деловања. Дакле, без обзира на постојање бројних тешкоћа у дефинисању овог криминала, као и постојање изражених тенденција да му се не признају специфичности које прате криминал уопште, ипак је јасно да такви ставови не могу бити прихватљиви јер се не могу занемарити ни застрашујући начини реализације овог криминала, као ни последице таквог деловања.

Осим израза „сајбер криминал”, неретко се употребљавају и други термини: *интернет-криминал*, *електронски криминал*, *криминал високих технологија*, *мрежни криминал* и сл.

[52] Више о томе: Gaines, G., Miller, R., *Criminal Justice in Action* (second edition), Wadsworth/Thomson Learning, Belmont, The United States of America, 2003. p. 7–9.

[53] Више о томе: Koenig, D., *Investigation of Cybercrime and Technology-related Crime*, http/www.neiassociates.org/cybercrime. htm , последњи пут приступили 12.04.2016.године.

У покушају да протумаче размере ове врсте криминала и његове последице, Уједињене нације су на Десетом конгресу, посвећеном превенцији криминала и третману починилаца, у документу *Криминал везан за рачунарске мреже* (*енгл. Crime related to computer networks*), под сајбер криминалом подразумевале „криминал који се односи на било какав облик криминала који се може извршавати посредством рачунарских система и мрежа, у рачунарским системима и мрежама или против рачунарских система и мрежа".[54]

Сајбер криминал је онај за чије постојање је неопходна употреба рачунарских система тј. „сваког уређаја или групе међусобно повезаних уређаја којима се врши аутоматска обрада података (или било којих других функција)", како је то дефинисано у Конвенцији о сајбер криминалу (енгл. *Convention on Cybecrime*) Савета Европе, и рачунарских мрежа које служе као мреже за повезивање разних субјеката.

Сматра се да рачунарске мреже могу да буду укључене у активности сајбер криминала на 3 начина, и то као:
1) „циљ напада, а што се дешава када су угрожени поверљивост, интегритет и расположивост података, односно мреже (нпр., дистрибуцијом вируса који оштећује одређене мрежне уређаје);
2) средство да се почини кривично дело, а што подразумева криминалне активности које олакшава употреба информационо-комуникационих технологија, као што су превара, дечија порнографија, продаја нелегалних супстанци преко мреже;
3) случајно умешане у кривично дело, али да имају изузетан значај за органе реда, као када је доказни материјал који се тиче криминалних активности евидентиран на рачунарима и серверима (нпр., садрже информације о илегалној продаји дроге)". [55]

Сајбер криминал је комплексан феномен, а сам појам се сматра кишобран-термином, који покрива разноврсне криминалне активности, укључујући ту и нападе на рачунарске податке и системе, нападе повезане с рачунарима, као и нападе на садржаје или интелектуалну својину, који се одвијају у електронском окружењу. Сајбер криминал представља облик криминалног понашања једног или више лица у сајбер простору, у којем

[54] Више о томе: *UN Crime related to the computer networks*, http://www.unis.unvienna.org/pdf/05-82111_E_6_pr_SFS.pdf , последњи пут приступили 12.04.2016.године.

[55] Више о томе: Westby, J., *Међународни водич за борбу против компјутерског криминала*, Продуктивност АД, Београд, 2004, стр. 127.

се рачунарске мреже појављују као средство, циљ, доказ или окружење извршеног кривичног дела.[56] Наведена дефиниција сајбер криминала једна је од најобухватнијих.

Сајбер криминал дешава се у тзв. сајбер простору, који се може дефинисати као симулирани информациони рачунарски простор, који садржи информације о лицима, предметима, чињеницама, догађајима, појавама, као и процесе представљене у математичком, симболичком или било којем другом облику, а у процесу кретања у локалним и глобалним рачунарским мрежама, или податке који се налазе у меморији свих физичких или виртуелних уређаја, као и других медија, а специјално је дизајниран за складиштење, обраду и пренос. Дакле, о сајбер криминалу можемо говорити ако је криминално дело „извршено коришћењем сајбер технологије у сајбер домену". Остале деликте, чији се учиниоци користе сајбер технологијом, а који нису извршени у сајбер простору, исправније је називати криминалним деликтима повезаним са сајбер технологијом (*енгл. Cyber-related crimes*).

Рачунар или компјутер је електронски уређај који се користи за уношење, обрађивање, спремање и дељење података према строго одређеној процедури. У енглеском језику реч *computer* изворно се користила за људе запослене да обављају аритметичке прорачуне механичким помагалима или без њих, али је касније коришћена за саме рачунске машине. Исто важи и за српску реч рачунар. Рачунарски криминалитет обухвата незаконите активности које се врше на рачунару или код којих је рачунар средство извршења. Он обухвата криминални упад у други рачунарски систем, крађу рачунарских података, или коришћења он-лине система за вршење или помоћ у извршењу превара.[57]

У дефинисању компјутерског криминала често се ставља нагласак на злоупотребу података, уз констатацију да је улога рачунара првенствено обрада података, те да је злоупотреба рачунарске технологије заправо напад на тачност обраде података и на дистрибуцију података. Сходно наведеном, под компјутерским криминалитетом подразумевају се све противправне повреде имовине при којима се рачунарски подаци с умишљајем мењају (компјутерска манипулација), уништавају (компјутерска саботажа),

[56] Више о томе: Вулетић, Д., *Сајбер криминал и могућност његовог откривања* (-докторска дисертација), Факултет организационих наука, Београд, 2008, стр. 35.

[57] Више о томе: Parker, D.B., Nycum, S., Aura, S., *Computer Abuse*, Stanford Research Institute, Menlo Park, California, 1973, p. 12.

неовлашћено захватају и искоришћавају (компјутерска шпијунажа) или се користе заједно са хардвером (крађа времена). Ове дефиниције компјутерски криминалитет поистовећују са сваким мешањем у аутоматску обраду података и у комуникацију са подацима.[58]

У теорији компјутерског права, заступљено је мишљење да компјутери могу имати четвороструку улогу:

,, – објекта, када су криминалне активности усмерене на уништење самих компјутера, података или програма, као и других уређаја који им омогућују рад

– субјекта – када се компјутер појављује као одредиште или окружење криминала, извор или повод за коришћење јединствених форми и врста напада на имовину

– инструмента – неки типови или методе криминала су комплексни, те захтевају коришћење компјутера као оруђа или инструмента. Компјутер може да се користи активно и пасивно

– симбола – када се компјутер користи за застрашивање или обмањивање."[59]

Тумачећи размере ове врсте криминала и његове опасности, у документу Криминал везан за рачунарске мреже с Десетог конгреса Уједињених нација, посвећеног превенцији криминала и третману делинквената, Радна група експерата дефинисала је ову појаву на следећи начин: ,,Рачунарски криминалитет је општи појам који обухвата кривична дела која се врше посредством рачунарског система или мреже у рачунарском систему или мрежи, или против рачунарског система или мреже".[60] У принципу он укључује било које кривично дело које се врши у електронском амбијенту, и може обухватати злоупотребе рачунара, рачунарске преваре, деликте помоћу рачунара, и криминалитет путем електронске обраде података, крађе услуга, информацијски, финансијски, имовински и традиционални криминалитет.

На нашем простору, једна од првих дефиниција о компјутерском криминалу настала је почетком осамдесетих година, када је рачунарска технологија била доступна само малом

[58] Више о томе: Sieber, U., *Computer Crime and Criminal Justice*, Koln, 1977, p. 188.

Sieber, U., *The International Emergence of Criminal Information Law*, Carl Heymanns Verlag KF, Koln, 1992, p. 5.
Taylor, P., *Hackers-Crime in the Digital Sublime*, Routledge, 1. edition, p. 200.

[59] Lipner, S., Kalman, S., *Computer Law, Cases and Materials*, Columbus, Merrill Publishing Company, 1989, p. 514.

[60] Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, year 2000, ,,Background paper for the workshop on crimes related to the computer network-Crime fighting on the Net" http://www.un.org/en/conf/crimecongress2010/pdf/55years_ebook.pdf, последњи пут приступили 12.04.2016.године.

броју високообразованих људи и када се није могао наслутити домет злоупотреба у овој области. Тада је ова врста криминалитета дефинисана на следећи начин: „Компјутерски криминал обухвата кривична дела код којих се компјутер појављује као средство (оруђе), предмет или објекат напада, за чије је извршење или покушај неопходно извесно знање из рачунарства и информатике."[61] У дефинисању компјутерског криминала често се кривична дела у којима се рачунар јавља као средство извршења другог кривичног дела сврстава под овом врстом криминала. Полазећи од таквог става, разликује се компјутерски криминалитет у правом (ужем смислу), којим обухвата рачунарску превару, саботажу и шпијунажу, и компјутерски криминалитет у неправом (ширем смислу), који се односи на противправно присвајање рачунара и његових делова крађом, проневером и слично.[62] Поједини аутори одустали су од идеје да дефинишу компјутерски криминал, а њихов истомишљеник је и Паркер (Parker), који истиче: „Рачунарски криминалитет је немогуће дефинисати једнинственим и прецизним појмовним одређењем. То је општа форма кроз коју се испољавају различити облици криминалне активности, форма која ће у будућности постати доминантна."[63]

Као што можемо закључити из досада реченог, начин извршења ових деликата се заснива на употреби компјутера, при чему то коришћење рачунара може да буде испољено као целовит *modus operandi*, или као један његов сегмент. Компјутер може бити и основно средство извршења ових кривичних дела, а потребно је поред тога да је испуњена нека у кривично правном смислу кажњива последица, с тим што последица може бити испољена и на самим компјутерима, информатичкој или комуникацијској мрежи.

Термин „сајбер криминал" често се користи заједно с појмом „компјутерски криминал", често се ови термини користе наизменично. Концепт „сајбер-криминала" је шири од концепта „компјутерског криминала" и прецизније одражава природу овог феномена као злочина у информативном простору. Сматрамо да је термин „компјутерски криминал" ужи у свом значењу, и доноси суштину феномена на злочине почињене од стране рачунара. На

[61] Брвар, Б., *Појавне облике злорабе рачуналника*, „Ревија за криминалистико ин криминологијо", Љубљана, бр. 2/1982, стр. 29.

[62] Водинелић, В., *Методика откривања, доказивања и разјашњавање рачунарског криминалитета*, „Приручник", Загреб, бр.4/1990, стр. 323.

[63] Parker, D., *„Fighting computer crime*, New York, 1983, стр. 70.

пример, данас, скоро сви мобилни телефони имају приступ интернету захваљујући 3Г могућности.

Савет Европе је у новембру 2001. године усвојио Конвенцију о сајбер криминалу, користећи термин „сајбер криминал", а не „компјутерски криминал". Дакле, сајбер криминал може да се дефинише као укупност злочина почињених у сајбер простору или путем рачунарских система или мрежа, као и других средстава приступа сајбер простору у оквиру рачунарских система или мрежа, али и против рачунарских система, рачунарских мрежа и компјутерских података.

2.4. ОПШТЕ КАРАКТЕРИСТИКЕ САЈБЕР КРИМИНАЛА

2.4.1 Просторна димензија криминалног деловања

Специфично окружење – сајбер простор, повлачи за собом мноштво нових и занимљивих импликација. Имајући у виду ову битну карактеристику компјутерског криминалитета да се извршава у информационом амбијенту, му даје одређене специфичности које се огледају у чињеници да се криминал у информационом амбијенту односи на класичну ситуацију извршава лакше, брже, разноврсније, обимније и значајно анонимније. [64] Сајбер простор нуди бесконачне могућности: различите начине комуникације с другим лицима и изражавање сопствених мисли и осећања, садржајне и бесплатне информације о било којој теми, различите форме забраве, могућности пословања и још много тога. Важне карактеристике сајбер простора су глобалан и транснационалан обим, који превазилазе територијалну контролу националних држава. За разлику од класичних видова криминалитета, сајбер криминалитет карактерише знатно проширен простор криминалног деловања, које не изискује присуство извршиоца на месту извршења кривичног дела.

Сајбер криминалитет не зна за границе, прелази лако из једне државе у другу, с једног континента на други. „Ово имплицира промену дефиниције лица места, а самим тим и изграђивања нове, томе прилагођене тактике криминалистичких мера и радњи које се на

[64] Петровић, С., *О информационој револуцији у контексту злоупотребе информационе технологије*, file:///C:/Users/0020578/Desktop/ZT04%20-%20O%20informacionoj%20revoluciji% 20u%20 kontekstu %20zloupotrebe%20informacione%20tehnologije.pdf, последњи пут приступили 12.04.2016.године.

њему предузимају, па и проблеме важења кривичних закона и полицијске и судске надлежности."[65] Корисници се без контроле могу кретати у вирутелном сајбер свету, који не познаје државне границе. Недозвољене радње могу се вршити без обзира на временску категорију и без обзира на то где се починилац налази. Мета могу да буду било који систем, лице или ситуација. Управо због тога међународна размена података носи многобројне ризике. Често се дешава да је место предузимања радње у једној, а место наступања последице у другој земљи. То може за последицу имати крупне тешкоће, јер иста радња у разним земљама може имати различиту правну квалификацију.[66]

Зато транснационални карактер ове врсте криминалитета, као његова специфична категорија изискује сарадњу која мора да буде на високом нивоу и заснована на међусобно прихваћеним принципима. Неусклађеност нациналних законодавстава и непостојање општеприхваћених правних стандарда и овлашћења надлежних органа у борби против сајбер криминала може успорити, па чак и онемогућити ефикасно откривање починиоца кривичних дела. ,,Брзина реакције након сазнања да је кривично дело извршено од пресудног је значаја за откривање починилаца и обезбеђење доказа, имајући у виду да се трагови извршеног дела лако могу уништити, сакрити или на други начин учинити недоступним или неупотребљивим."[67] Друштвени, социјални, економски контекст овог криминала није истоветан класичном транснационалном криминалу, јер за сајбер простор важе друга правила, што показује *Глобална студија о организованом криминалу* Центра за превенцију међународног криминала и Института Уједињених нација за истраживање интеррегионалног криминала.[68]

---

[65] Више о томе: Бановић, Б., *Обезбеђење доказа у криминалистичкој обради кривичног дела привредног криминалитета*, Виша школа унутрашњих послова, Београд–Земун, 2002, стр. 135.

[66] Више о томе: Фејеш, И., *Компјутерски криминалитет криминалитет будућности, изазов садашњости*, „Правни живот – часопис за правну теорију и праксу", Удружење правника Србије, бр. 9/2000, год. 2, књ. 452, Београд, стр. 377.

[67] Више о томе: Јерковић, Р., *Високотехнолошки криминал: актери и жртве*, „Ревија за безбедност – стручни часопис о корупцији и оргаизованом криминалу", Центрар за безбедносне студије, бр. 3/2009, год. 3, стр. 27–34, Београд, стр. 28.

[68] Више о томе: *Global studies on organized crime*, United Nations office at Vienna, http://www.globalinitiative.net/download/general/global/UN%20-%20Global%20studies%20on% 20organized %20crime.pdf , последњи пут приступили 12.04.2016.године.

С обзиром на специфичност радње и понашања које проузрокују ова дела, као и на починиоце и оруђа којима се врши, сајбер криминал није физички везан за једно место, нити за једну жртву. Довољно је улетети у неку интернационалну мрежу па да се могу чинити невидљиво и готово неухватљиво, крађе, преваре, саботаже и др. Интернационалност представља особеност и тенденцију ових дела. Због те карактеристике, међународно повезивање истражних и других тела и органа представља, не само потребу, него и императив. Једно од могућих решења за превенцију и кажњавање ухваћених починилаца је хармонизација и унификација казненог и процесног права, тако да претња у једној значи исту такву претњу у другој земљи. То је особито важно и због обезбеђивања интернационалних мрежа података.

2.4.2 **Временска димензија криминалног деловања сајбер криминала**

Захваљујући расположивим техничким могућностима и с обзиром на аутоматизован амбијент, сајбер криминално деловање веома брзо се реализује. Управо таква временска димензија спречава управљање разноврсним начинима манипулисања подацима и надзор над њима. На тај начин време потребно за извршење кривичног дела скраћује се на делове секунде, што имплицира висок ниво прикривености и значајне тешкоће у откривању такве делатности.[69]

Време је такође категорија која не ограничава могућности за појаву овог облика криминалитета. Овај деликт може извршити и за три хиљадита дела секунде.[70] Због брзине рада фактори простор и време се у компјутерсом криминалитету јављају у сасвим другачијем виду него у класичном крииналитету. Ова спознаја веома је важна с аспекта правне регулације.[71]

---

[69] Више о томе:Бановић, Б., *Обезбеђење доказа у криминалистичкој обради кривичног дела привредног криминалитета*, Виша школа унутрашњих послова, Београд–Земун, 2002, стр.135.

[70] Више о томе:Будимлић, М., Пухарић, П., *Компјутерски криминалитет – криминолошки, кривичноправни и сигурносни аспект*, Факултет за криминалистику, криминологију и сигурносне студије, Сарајево, 2009, стр. 9.

[71]Више о томе: Фејеш, И., *Компјутерски криминалитет – криминалитет будућности, изазов садашњости*, „Правни живот – часопис за правну теорију и праксу", Удружење правника Србије, бр. 9/2000, год. 2, књ. 452, Београд, стр. 377.

2.4.3 Начин вршења и откривања сајбер криминалних радњи

Често се каже да је најсигурнији рачунар онај који је искључен или онај који није прикључен на мрежу. Чињеница да га било ко може укључити и повезати у мрежу значи да је чак и угашен рачунар рањив. Овај вид криминала остварује се специфичним нападима – сајбер нападима, док се у други план стављају физички напади. Физички напад подразумева употребу конвенционалног оружја против инфраструктуре у којој се налазе информациони системи или против линија преноса информација. Ова врста напада усмерена је на расположивост нападнутог система и налази примену у рачунарском криминалу.

Сајбер који су уперени против рачунара у мрежи, или саме мреже могу се поделити на:

– сајбер нападе техничког типа (тј. нападе помоћу малициозних програма или нападе усмерене на опструкцију услуга) и

– нападе у сајбер простору који се заснивају на обмањивању других корисника сајбер простора и злоупотребу њиховог поверења (сајбер преваре).

Напади помоћу малициозних програма обухватају употребу злонамерних или малициозних (енгл. *malware*) информатичких програма чији је задатак да заразе информациони систем противника са циљем да га оштете или да украду разноврсне, а нарочито поверљиве или осетљиве информације (на пример, лозинке – *passwords*, бројеве кредитних картица итд.).

Реч је о веома развијеним техникама и изузетно осмишљеним активностима приликом злоупотребе података. У том смислу, карактеристика сајбер криминала је социјални инжињеринг, односно сугестивна комуникација и активно навођење људи на то да одају информације о себи, а до којих би се, да није тог метода, могло доћи хакерским методама. То може да буде давање имена и лозинке, података о платној картици, месту рођења, социјалном осигурању, броју пасоша итд. Дакле, амбијент вршења наведених криминалних активности јесу и суптилне технике и методи који се извршавају истим механизмима као и легалне, не остављају трагове, нити ометају редован рад система, па је самим тим, могућност откривања сведена на најмању меру, а у појединим случајевима ограничена само на

откривање у тренутку извршења дела.[72] Специфичност материјалних трагова повезаних с компјутерским кривичним делима, као и могућност њиховог благовременог проналажења и обезбеђења у непосредној је вези с одговарајућим начином откривања таквих тела. Технологија рада с компјутерима омогућава неовлашћену интервенцију, тако да за разлику од класичног облика фалсификовања, овде не остају никакви трагови. [73]У пракси се показало да је веома тешко прикупити поуздане и прецизне податке о распрострањености рачунарског криминалитета, динамици, фреквенцији и врстама кривичних дела из ове области, као и последицама предузетих радњи.

Карактеристично је и да, када је оштећени открио да је жртва кривичног дела, често не подноси пријаву због страха од губитка поверења пословних партнера, што лако може да узрокује банкротирање. Тако, нпр., ако се догодио неовлашћен продор у информациони систем банке и ако се та чињеница обзнани, странке с правом могу страховати да подаци о њима нису у добрим рукама, па ће потражити другог пословног партнера. Због тога у великом броју случајева руководиоци оштећених субјеката настоје да заташкају такво кривично дело и радије трпе насталу штету него ли да подношењем пријаве рескирају несагледиве последице пољуљаног поверења.[74] Према извештају Међународног удружења за кривично право, сачињеном на основу података из земаља чланица, године 1992. процењено је да само 5% извршених кривичих дела високотехнолошког криминала бива пријављено надлежним органима.[75]

Бројни су разлози због којих је тамна бројка ове савремене форме криминалитета велика. Приликом различитих злоупотреба компоненти рачунарске технологије оштећено лице није ни свесно да је у конкретном случају жртва кривичног дела, па самим тим изостаје подношење кривичне пријаве, а ако се и открије извршено дело, често је већ касно да би се

[72]Више о томе: Бановић, Б., *Обезбеђење доказа у криминалистичкој обради кривичног дела привредног криминалитета*, Виша школа унутрашњих послова, Београд–Земун, 2002, стр. 135.

[73] Више о томе: Бошковић, М., *Криминалистичка методика*. 2, Полицијска академија, Београд, 1996, стр. 376.

[74] Више о томе: Фејеш, И., *Компјутерски криминалитет – криминалитет будућности, изазов садашњости*, „Правни живот – часопис за правну теорију и праксу", Удружење правника Србије, бр. 9/2000, год. 2, књ. 452, Београд, стр. 378.

[75] Више о томе: Извештај Међународног удружења за казнено право, http//www.uplink.com.au/lawlibrary/Documents/ Docs/Doc122.html#fn0, последњи пут приступили 12.04.2016.године.

могла предузети нека ефикасна мера. Ситуацију отежава и то што могућности рачунарске технологије пружају одличне услове за прикривање криминалних активности и учињених последица, а поготово чињеница да је за откривање великог броја злоупотреба потребно поседовати висок степен стручног знања. Недовољна обученост надлежних служби у комбинацији с недовољном информисаношћу потенцијалних жртава о опасностима које прете и мерама превенције, као и неодговарајућа законска регулатива за последицу имају ситуацију у којој је могуће и замисливо да највећи број кривичних дела сајбер криминала никада не буде пријављен.Ако се, пак, кривична дела из ове области и открију, често се сами оштећени, нарочито ако су то правна лица, уздржавају од пријављивања случајева у којима им је нанета штета, јер сматрају да би тиме погоршали свој положај на тржишту или се плаше губитка конкурентских предности услед неспособности да се ефикасно заштите.

2.4.4. Специфичан профил учиниоца сајбер кривичних дела

Злоупотребом било ког елемента рачунарске технологије у већини случајева се баве лица која ту технологију добро и познају. Нарочито у првим годинама развоја рачунарске технологије висока стручност и добро познавање руковања компјутером и његовим компонентама узроковали су веома споро и тешко разоткривање почињених кривичних дела.

Сајбер криминал могу извршити и малолетна лица, што га битно разликује од класичног криминала. Да су деца од најранијег узраста упућена у информационе комуникације и обилато их користе, сведочи и пример петогодишњака из Сан Дијега, који се нашао на *Microsoft*-овој листи безбедносних истраживача који су открили и проследили информације о рањивостима у производима компаније. Дечак Кристофер фон Хасел (Kristofer von Hasel), искористивши безбедносне пропусте, успео је да се пријави на очев *Xbox Live* и да игра игре. Испоставило се да малишан није украо очеву лозинку, већ је искористио безбедносни пропуст који је *Microsoft* након тога исправио. Наиме, он је откуцао нетачну лозинку, после чега се појавио прозор за потврду лозинке. Он је у том прозору једноставно откуцао размак неколико пута и пријавио се на налог свог оца без праве шифре. На тај начин Кристофер се нашао на листи проналазача багова *Microsoft* компаније. За тај допринос дечак је награђен с 50 долара, годишњом претплатом за *Xbox Live* и четири игре.[76]

[76] Више о томе: http://www.informacija.rs/Vesti/Petogodisnjak-hakovao-Xbox-Microsoft-ga-nagradio.html, последњи пут приступили 12.04.2016.године.

Сматрамо да ће се старосна граница учиниоца сајбер криминала све више смањивати, и да ће тинејџери махом користити ове противправне активности како би на лак начин стицале новац са великом могућношћу да никада не буду откривени.

2.4.5. Вишеструка улога рачунарске технологије

Скоро свако домаћинство данас има рачунар, док се пословни простор више не може замислити без те техничке подршке. Таква динамика развоја условила је и еволуцију различитих врста учинилаца рачунарских кривичних дела. Све једноставнија употреба компјутерске технологије, и то све већег броја корисника, којима више није ни нужно посебно техничко образовање, шири круг потенцијалних извршилаца кривичних дела компјутерског криминалитета, тако да је све теже утврдити њихову типологију и карактеристике. С обзиром на брзину обраде података и разноврсне могућности њиховог укрштања, повезивања, селекције и слично, могућности криминалног деловања појединца расту чак толико драстично да се може рећи да сајбер криминалац замењује на десетине класичних криминалаца.[77]

С обзиром на то да је рачунарска технологија присутна у скоро свим сферама живота и рада, свакодневно уочавамо појаву криминалних активности у новим областима и ситуацијама у односу на нове категорије оштећених лица, а у сасвим новим условима и могућностима. Ова врста криминалитета развија се таквом брзином што узрокује настанак и ширење рачунарског криминалитета могу се узети: 1) софистицирана технологија која отежава откривање, 2) неоспособљеност истражитеља, као и то што 3) жртве не користе сигурносне савете и често се не осећају угроженим таквим деловањима.[78]

Рачунарска технологија може се појавити у вишеструкој улози, односно као:

1) циљ напада – нападају се сервиси, функције, садржаји који се на мрежи налазе.
2) алат – криминалци од памтивека користе разна оружја, а данас модерни криминалцине „прљају руке” користећи мрежу за чињење дела и реализовање својих намера. окружење – у ком се напади реализују. Најчешће то окружење служи за

[77] Више о томе: Петровић, С., *Компјутерски криминал*, „Безбедност”, МУП РС, бр. 1/94, стр. 18–19.

[78] Више о томе: Будимлић, М., Пухарић, П., К*омпјутерски криминалитет – криминолошки, кривичноправни и сигурносни аспект*, Факултет за криминалистику, криминологију и сигурносне студије, Сарајево, 2009, стр. 9.

прикривање криминалних радњи, као што то веома вешто успевају да ураде педофили, а ни други криминалци нису ништа мање успешни;

3) доказ – као што се у класичном криминалу појављују нож, отров, пиштољ, или неко друго средство извршења дела, тако се и мрежа и информационо комуникациона технологија могу јавити у доказном поступку за сајбер криминал.

Након представљених карактеристика сајбер криминалитета, јасно је да је ово криминалитет који брзо мења форме и облике испољавања, границе међу државама, као и врсту оштећеног. Приликом његовог извршења рачунар могу бити и средство, циљ и доказ извршења. Рачунарска технологија има вишеструку улогу која се огледа како у начину извршења, тако и приликом откривања и доказивања.

2.5. ПОЈАВНИ ОБЛИЦИ САЈБЕР КРИМИНАЛА

Као што још увек не постоји јединственост у томе шта је компјутерски криминал, тако не постоји сагласје ни која дела и понашања треба третирати као дела у којима постоји противправно, неетичко понашање којим се остварује биће кривичних дела сајбер криминала.

У теорији су присутна два начина дефинисања појавних облика сајбер криминала: прво схватање полази од генералног појма сајбер криминала и сва дела која имају њему особена својства подразумевају се под сајбер криминалом. Насупрот наведеном гледишту, са друге стране се користи метод енумерације, при чему се таксативно наводе дела сајбер криминала.

Првој групи припадају схватања Едвардса, Сејвџа и Валдена (Edwards C, Savage N, Walden), који сматрају да се дела сајбер криминала могу поделити на она у којима компјутери имају ,,активну" улогу, односно криминал повезан с компјутерима и она у којима се компјутери појављују као периферни објект криминала.[79] Сличан метод се користи приликом класификације сајбер криминалитета по томе да ли је у питању сајбер криминалитет у ужем или ширем смислу. Под сајбер криминалитетом у ужем смислу овај

[79] *Information Technology & The Law*, Basingstoke, Macmillan Publicers LTD, 1990. p. 12

аутор подразумева рачунарске преваре, шпијунажу, саботаже, док под ових делима у ширем смислу подразумева и сва остала дела.[80]

Другој групи припадају схватања Зиебер-а (Sieber-a), који прихвата одређења и поделу Комитета експерата ОЕЦД-а и сматра да се дела компјутерског криминалитета могу сврстати у односу на последице (ако су нападнути економски интерес, приватност и сл.) у три велике групе:

1) ,,дела компјутерског криминалитета везана за економски криминал, као што су превара, крађа, компјутерска шпијунажа и саботажа, неауторизован приступ системима и хакинг, пиратство софтвера и сл.
2) дела компјутерског криминалитета везана за кршење права приватности, као што су коришћење нетачних података, илегално прикупљање и чување личних података, илегално откривање и злоупотреба података, кршење формалности права приватности и сл.
3) угрожавање осталих правно заштићених интереса, као што је угрожавање националне сигурности, контрола прекограничног тока података, интегритет процедура везаних за компјутере и мреже података и друга дела.”[81]

Одговарајуће законодавне комисије (нпр., Енглеске, Шкотске) још детаљније наводе појединачне облике, односно кривична дела која се могу сматрати компјутерским криминалитетом. То су:

1) компјутерска превара;

2) недозвољено коришћење рачуарских података, као што је хакинг, компјутерско прислушкивање, недозвољена употреба компјутера за личну корист;

3) недозвољена примена или деструкција меморисаних података;

4) одбијање приступа овлашћеном кориснику;

5) недозвољено уклањање података.

Комитет експерата ЕУ, у П*репоруци о криминалитету повезаном с компјутерима*, а коју је прихватио Комитет министара Савета Европе, препоручује државама чланицама да промене постојеће или стварају ново национално законодавство повезано са сајбер криминалом. Предвиђена је листа минимума која се мора уградити у национална

[80] Више о томе: Водинелић, В., *Методика откривања, доказивања и разјашњавања рачунарског криминалитета*, „Приручник”, 4/1990, стр. 323–328.

[81]Више о томе: *The International Handbook of Computer Crime*, Chichester, John Wiley&sons, 1991, стр. 3–27.

законодавства, као и опциона листа, која је факултативна за државе чланице. Листа минимума обухвата следеће противправне радње:

1) „Рачунарска злоупотреба (унос, измена, брисање или потискивање рачунарских података или програма, као и остале врсте мешања у обраду података које утичу на њен резултат, а чиме се изазива економски или имовински губитак другог лица с намером да се стекне незаконита економска добит за себе или треће лице – алтернатива – с намером да се то лице лиши имовине на незаконит начин)
2) Рачунарски фалсификат (унос, измена, брисање или потискивање рачунарских података или програма, као и остале врсте мешања у обраду података на рачунару или под условима предвиђеним домаћим законом који би представљао дело фалсификата. Оштећење рачунарских података или рачунарских програма (бесправно брисање, оштећивање, кварење или потискивање рачунарских података или рачунарских програма)
3) Рачунарска саботажа (унос, измена, брисање или потискивање рачунарских података или рачунарских програма или мешање у рачунарски систем с намером да се онемогући функционисање рачунара или телекомуникационог система)
4) Неовлашћен приступ (бесправан приступ рачунарском систему или мрежи кршењем мера безбедности)
5) Неовлашћено ометање (бесправно ометање техничким средствима улазне или излазне комуникације, као и комуникације унутар рачунарског система или мреже)
6) Неовлашћено копирање заштићеног рачунарског програма (бесправно копирање, дистрибуција или јавно објављивање рачунарских програма заштићених законом)
7) Неовлашћено копирање топографије (бесправно копирање законом заштићене топографије, полупроводничког производа или бесправно комерцијално коришћење или увоз у те сврхе топографије или полупроводничког производа направљеног коришћењем топографије).

Опциона листа обухвата:

1) промену компјутерских података или компјутерских програма;
2) компјутерску шпијунажу;
3) неауторизовано коришћење компјутера;
4) неауторизовано коришћење заштићених компјутерских програма и топографије“.[82]

[82] „Recommendation”, No . R (89)9, on computer-related crime.

Приручник за заштиту и контролу криминалитета повезаног с компјутерима на сажетији начин набраја основне типове сајбер криминала:

1) компјутерске манипулације;
2) компјутерска кривотворења;
3) оштећења на компјутерским подацима или програмима;
4) приступ компјутерском систему или компјутерскимсервисима.[83]

Постоје, пак, и класификације које дела сајбер криминалитета разврставају на основу „улоге" коју у извршавању дела има компјутер, односно да ли се ради о делима у којима је компјутер периферни објект или оруђе или компјутер има „активну улогу". Такво схватање омогућује, осим укључивања класичних дела криминала, укључивање и оних која се појављују само у вези с компјутерима, као што су хакинг, пиратство софтвера, стварање и убацивање вируса, али не само њих него и других продуката повезаних с информационом технологијом која носи све облике злоупотреба.[84]

Једна од најобухватнијих класификација појавних облика сајбер криминала је полажење од одређења злоупотреба рачунара у ширем и ужем смислу. Таква класификација у дела сајбер криминала у ширем смислу сврстава:

1) „дела повезана с економским вредностима:

   - кривична дела против интелектуалне својине: неауторизовано модификовање, уништавање, откривање или узимање података, програма или докумената који су повезани (екстерно или интерно) с компјутерским системом, комуникацијама и другим објектима интелектуалне својине (пиратство и крађа програма, дизајна и чипова),

   - кривична дела против компјутерске опреме или подршке: неауторизовано модификовање, коришћење, или уништење компјутерског система, комуникационих веза или друге компјутерске опреме или подршке (компјутерске саботаже, оштећења софтвера, хардвера),

   - кривична дела против корисника рачунара: неауторизован приступ компјутеру, компјутерском систему, комуникационом систему и мрежама, или ускраћивање приступа ауторизованим корисницима компјутерских услуга,

[83] *UN Manual on the prevention and control of computer-related crime*.

[84] Дракулић, Мирјана, *Основи компјутерског права*, Друштво операционих истраживача Југославије, Београд, 1996, стр. 432.

- кривична дела против пружаоца компјутерских услуга и власника података: крађа сервиса, крађа информација, крађа новца и слично, као и компјутерска шпијунажа, компјутерске преваре, узнемиравања, изнуђивања;

2) повреде приватности помоћу компјутера:
   - производњом и коришћењем нетачних података,
   - недопуштеним откривањем или губљењем података,
   - недопуштеним скупљањем или чувањем података,
   - повреде формалности и права на информациону приватност и право приватности;
3) други облици злоупотреба:
   - кривична дела против државе и политичких интереса,
   - компјутерски тероризам.

Као типична дела у односу на компјутерски криминалитет у ужем смислу (криминалитет повезан с компјутерима), извршена, дакле, помоћу и против рачунара појављују се:

1) прављење и убацивање компјутерских вируса;
2) хакинг;
3) пиратство (софтвера, микрочипова, база података);
4) компјутерска саботажа;
5) компјутерска шпијунажа;
6) компјутерске преваре;
7) крађа компјутерских услуга“. [85]

Конвенција Савета Европе о сајбер криминалу класификује кривична дела сајбер криминала у пет група. Прва група састоји се од дела против поверљивости, интегритета и доступности компјутерских података и система, као што су илегалан приступ, незаконито прислушкивање, мешање података, систем уплитања.
Другу групу чине дела повезана с коришћењем рачунара као средство извршења кривичних делан– наиме као средство манипулације информацијама. Ова група укључује рачунарске преваре. Трећу групу чине кривична дела повезана са садржајем (садржај података) који су сачувани на рачунарским мрежама. Најчешћи пример из ове групе су кривична дела која се односе на дечју порнографију.
Четврта група обухвата кривична дела повезана с кршењем ауторских и сродних права. Пета

[85] Више о томе: Parker, D., *Fighting Computer Crime*, New York, Charles Scribneirs Sons, 1981, стр. 6.

група уведена је *Протоколом* уз Конвенцију о сајбер криминалу. Она прописује кривична дела расистичке и ксенофобичне природе извршена путем рачунарских мрежа.

Савет Европе је у *Извештају о организованом криминалу – Претња сајбер криминала из 2004. године,* под сајбер криминал прагматично сврстао следеће категорије дела:

- дела против поверљивости, интегритета и расположивости (доступности) података (енгл. *Computer data*) и рачунарских система (енгл. *Computer systems*) – у ту категорију, уопште узев, могу се сврстати сајбер напади (неовлашћен приступ неком систему, напади типа DoS, напади помоћу малициозних програма, фишинг итд.);
- традиционална дела извршена помоћу рачунара (енгл. *Computer related traditional crimes*) попут: превара, фалсификовања, злоупотребе кредитних картица, изнуда итд.;
- дела повезана са садржајем (енгл. *Content related offences*) – поседовање, дистрибуција, трансмисија и складиштење недозвољених садржаја (порнографских, расистичких итд.);
- дела повезана с кршењем ауторских и сродних права (неовлашћено репродуковање и дистрибуирање неауторизованих примерака аудио/видео-програма, банака података, дигиталних књига и, уопште, радова у електронском формату;

-дела повезана с нарушавањем приватности (неовлашћен приступ системима који садрже личне податке, прикупљање и дистрибуција личних података итд.).

Сваки од набројаних форми сајбер криминала може да се комбинује са другим па скоро да не постоји „чист" облик. Тако хакинг, осим неовлашћеног уласка у компјутерске системе и мреже, често обухвата и уништавање података или компјутерску шпијунажу (као што је то случај с упадима на веб-сајтове и уништавање или „преправљање" података на њима или хакинг пасворда и трговина њима). Измена компјутерских података и програма обухвата и „лансирање" компјутерских вируса црва, што је најчешће праћено заустављањем рада компјутерског система, или уништењем података. С тим у вези није могуће набројати све појавне облике сајбер криминала, и свако такво настојање биће илузорно и превазиђено.

3 КРИВИЧНО ДЕЛО ПРЕВАРА КАО МОДЕЛ ОСТВАРИВАЊА САЈБЕР КРИМИНАЛА

3.1. Појам превара као модел остваривања сајбер криминала

Од појаве интернета стварањем ARPANET-а, 1969. године трансформисан је начин на који функционишу комуникацијски системи. Иако се интернет врло брзо проширио на свет трговине и пословања, било је потребно скоро 30 година да се наметне као технолошка иновација која константно трансформише друштво и економију. Могућност коју пружа ова глобална мрежа, поред осталог, јесте спајање људи зарад међусобне комуникације и омогућавање кориснику да дели информације с осталим члановима глобалне мреже помоћу алаткама „лаким-за-коришћење" (*easy-to-use publishing tools*).

Почев од краја деведесетих година када се појавила друштвена мрежа Classmates.com, која је зачетник спајања људи преко имејл адреса, настаје експанзија друштвених мрежа које омогућавају корисницима стварање списка пријатеља и могућност тражења корисника са сличним интересовањима и њихово организовање по групама у којима ће износити своје ставове. Непресушна људска потреба за комуникацијом, контактом и социјализацијом заслужна је за велики успех друштвених мрежа орјентисаних на пословни карактер (*LinkedIn* и *Xing*), налажење старих пријатеља (*Friendster* і *Classmates*) или глобалног карактера, намењена дружењу и забави (*Facebook, MySpace, Twitter*). Све те друштвене мреже убрзо након оснивања и омогућивања повезивања људи постале су битан савезник сајбер преварантима.

Појава интернета, као и све већа, глобално распрострањена употреба информационих и телекомуникационих технологија утицале су на пораст илегалних активности у том простору. Употреба сервера који пружају опције анонимног коришћења интернета, могућност отварања веб-електронске поште, коришћења лажних електронских адреса, и постављање лажних интернет сајтова данас су основно оруђе у рукама извршилаца кривичних дела превара која се врше помоћу савремених информационих технологија. С појавом интернета традиционално кривично дело преваре попримило је широке димензије будући да се ради о релативно неистраженом облику криминалног понашања, а с обзиром на велику феноменолошку разноврсност ове појаве. Кривично дело преваре, које представља лажно приказивање или прикривање чињеница ради довођења у заблуду или одржавања у

заблуди неког лица, као и ради навођења неког лицада на своју штету или штету туђе имовине нешто учини или не учини, налази у сајбер простору плодно тло.

Број облика преваре, као и начина њихове реализације практично је неограничен и у пракси се сусрећу како оне врло примитивне и грубе, тако и преваре у којима починиоци испољавају велики стадијум вештине и рафинираности. Но, у шемама преваре увек се открије неки ранији облик, сличност, или елементи који су својствени и класичном видом преваре. Бројне шеме превара регистованих на интернету у ствари су прерађене и прилагођене верзије шема којима су некад и вековима обмањиване неопрезне, лаковерне и похлепне жртве. Компјутерске преваре карактерише то да оне далеко допиру због величине и приступачности интернета као тржишта, брзо се шире јер се с интернетом као медијем све дешава врло брзо, а сами трошкови извођења таквих врста превара јако су ниски.

Опасности које носи кривично дело преваре као модел извршења сајбер криминала постале су једне од најраспрострањенијих на интернету због врло честог мењања начина извршења и прилагођавања брзим променама у области информационих технологија.

Сајбер преваре представљају врсту високотехнолошког криминала чија је дефиниција дата у члану 2. Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала, који је ступио на снагу 26. јула 2005. године: „Високотехнолошки криминал у смислу овог закона 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.”[86]

Сајбер превара је облик сајбер и високотехнолошког криминала који представља облик криминалног понашања у ком се коришћење компјутерске технологије и информационих система испољава као начин извршења кривичног дела, или се компјутер употребљава као средство или циљ извршења, а ради тога да се себи или другоме прибави противправна имовинска корист или другом лицу нанесе штета, чиме се остварује у кривично-правном смислу релевантна последица.

[86] Закон о организацији и надлежности државних у борби против високотехнолошког криминала "Сл. Гласник РС", бр. 61/2005 и 104/2009 (члан 2)

Сајбер превара подразумева кривично дело преваре извршено у сајбер простору. Узимајући у обзир да се сајбер простор поистовећује с интернетом, сајбер преваре представљају коришћење интернет услуга или софтвера с интернет приступом са циљем прибављања имовинске користи себи или другом или наношења штете. Интернет је идеално место и средство за вршење преварних радњи јер омогућује да се без физичког контакта и без трошкова убеди жртва у истинитост приче.

Сајбер превара односи се на било коју превару при чијем извршењу лице које с намером прибавља противправне имовинске користи за себе и другога искористи једну или више компоненти интернета, као што су chat rooms (собе за ћаскање), веб-странице, електронска пошта да би створило услове за лажно приказивање или прикривање чињеница којим би се неко лице довело у заблуду или у њој одржавало, да би то лице учинило нешто на штету своје или туђе имовине тако што би, на пример, спровело неку финансијску трансакцију или пренело неке податке некој финансијској институцији која је мета напада.

Због непостојања правне регулативе која се односи на посебно кривично дело сајбер преваре, ово дело се погрешно поистовећује с кривичним делом „рачунарске преваре". У Кривичном законику који је ступио на снагу 1. јануара 2006. године, у поглављу XXVII, под називом „Кривична дела против безбедности рачунарских података", у ставу 1 члана 301. на следећи начин дефинише се радња извршења кривичног дела рачунарска превара: „Ко 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, казниће се новчаном казном или затвором до три године."[87]

Како сам назив превара каже, оне су усмерене на рачунар или компјутер, тј. електронски уређај који се користи за унос, обраду, спремање и дељење података према одређеној процедури. Дакле, рачунарска превара односи се на дела почињена над рачунаром, материјалима садржаним у њему (софтвером и подацима), при чему се рачунар користи као средство или циљ извршења кривичних дела, тј. за уношење нетачног податка пропуштањем да се унесе тачан податак или на други начин прикрије или лажно прикаже податак и тиме се

[87] Кривични законик Републике Србије („Сл. гласник РС", бр. 85/2005, 88/2005 – испр., 107/2005 – испр., 72/2009 и 111/2009).

утиче на резултат електронске обраде и преноса података. Овај вид преваре био је заступљен када глобалне мреже нису заживеле у пословној и приватној употреби.

Измена цифре на банковном рачуну, промена својства дужника/повереника је извршаване су без употребе глобалне мреже тј. сајбер простора. Рачунарске преваре имале су ограничен објекат, а то су били подаци складиштени у рачунаској меморији. Главно место извршења била је база података, која је садржала податке од интереса за рачунарске преваранте, а који су могли да буду промењени. Извршилац рачунарске преваре могло је да буде лице које је имало приступ тим информацијама, а најчешће запослено лице. С изумом малициозних програма и коришћењем интернета извршиоци, осим запослених, могу да буду и хакери, који убацивањем вируса добијају приступ бази података.

Време извршења рачунарских превара је врло кратко: активирање компјутерског система, налажење податка који се жели изменити и давање рачунару наредбе *insert, edit* или *delete*. Опције у рукама рачунарских превараната биле су убацити, тј. уписати податак, изменити га и обрисати. Тај противправни акт Кривични законик је регулисао, што није случај с комплекснијим сајбер преварама, које се битно разликују.

Сајбер преваре много су комплексније. Оне изискују најпре иновативност, смишљање техника социјалног инжињеринга које ће заинтригирати жртву, набављање или измишљање малициозног софтвера, проналажење жртве, остваривање и одржавање комуникације с њом и подизање новца с рачуна жртве (у случају банкарских превара). Начин извршења обухвата довођење жртве у заблуду и активно учешће жртве у извршењу (било пристајањем на „посао снова" и уплатом новца, било преузимањем заражених апликација). Дакле у сајбер преварама жртве пристају на ризик било изричито (уплатом новца на рачун превараната, преговорима), било прећутно (кликом на апликацију која је заражена). Управо је то *diferencia specifica* та два противправна акта. Док се рачунарске преваре изводе с намером да оштете „систем" (државу, фирму и др.), сајбер преваре усмерене су на појединце.

За разлику од облика рачунарске преваре, сајбер преваре карактеришу акти манипулације којима се људи наводе да одају поверљиве информације о себи. У извршењу те преваре, за разлику од осталих облика рачунарских превара, појављује се активно учешће жртве. Сајбер преваре је немогуће извршити без учешћа жртве и њеног деловања, а за рачунарске преваре нису потребни ни знање, ни воља жртве. У неким преварама, попут „нигеријске преваре", и саме жртве наседају на превару пристанком да учествују у

противправним радњама ради стицања противправне користи. Бабовић описује разлику између интернет и рачунарске преваре на следећи начин: „Интернет преваром се обмањује, пре свега, лице. Интернет превара није увек и обавезно рачунарска превара, јер неке Интернет преваре одговарају класичним преварама које за средство извршења имају Интернет без неког посебног утицаја на електронску обраду података или рад рачунара (обмањују се људи). Насупрот овоме, рачунарском преваром се обмањује рачунар и електронска обрада наводи на погрешан резултат који је усмерен на стицање противправне имовинске користи и то је *differentia specifica* ова два појма."[88]

Ова два вида превара разликују се и по месту извршења. Место извршења кривичног дела рачунарске преваре је један рачунар, а сајбер превара – интернет, који чине мреже које се међусобно повезују и тиме чине структуру од више од 150.000.000.000 рачунара с огромном количином информација.

Последњих година забележена је експанзија апликација за мобилне телефоне. Савремени мобилни уређаји постали су прави мали рачунари за понети. Уместо рачунара, за сурфовање интернетом или преглед вести на *Facebook*-у користи се смарт телефон. Тај тренд искористили су преваранти прилагођавајући се технолошким иновацијама. Угроженост малверима, спамовима и фишингом више није резервисана само за кориснике рачунара. Смарт мобилни телефони постали су објекат напада сајбер криминала, па и сајбер превара.

3.1.1 Други модели којима се остварује сајбер криминал

Поред сајбер преваре, у којој је мрежа окружење за извршење кривичног дела, постоје и други модели извршења сајбер криминала који су повезани с коришћењем мреже као средства или циља напада.

3.1.1.1 Злоупотреба мрежа за ширење недозвољеног материјала као модела за остваривање сајбер криминала

[88]Више о томе: Бабовић, М.: *Хакерска култура и компјутерски криминал*, „Правни живот – часопис за правну теорију и праску", бр. 9/2003, год. LIII, књ. 485, 1–1356, Удружење правника Србије, Београд, стр. 749–750.

Данас модерни криминалци користе све више компјутерске мреже као оруђе или средство за реализацију својих намера, тј. компјутерске мреже се користе као средство за извршење сајбер криминала. Злоупотреба мрежа за ширење недозвољеног материјала као модела за остваривање сајбер криминала нарочито је популарно кад се ради о:

- дечјој порнографији;
- злоупотреби интелектуалне својине;
- продаји недозвољене робе на мрежи (дрога, људски органи, невесте и др.);
- софтверској пиратерији.

Масовна примена рачунарске технологије директно је узроковала повећање потражње за рачунарским програмима. Самим тим софтверска технологија је врло брзо постала предмет злоупотребе на црном тржишту. Софтверска пиратерија постаје уносно занимање којим се, у релативно кратком времену и на прилично лак начин остварују велике материјалне зараде. Оваквом врстом злоупотребе оштећени су првенствено аутори, који губе економску добит на коју рачунају на основу дистрибуције софтверских програма. Оштећена је такође држава јер нелегалном дистрибуцијом софтверских програма губи огромне суме новца које јој припадају по основу наплате пореза.

Ширењу овог облика сајбер криминала умногоме доприноси и доскора неразвијена правна основа заштите рачунарских програма. У Кривичном законику републике србије у делу „Кривична дела против интелектуалне својине" прописује се кривично дело неовлашћено искоришћавање ауторског дела или предмета сродног права (члан 199.) и неовлашћено уклањање или мењање електронске информације о ауторском и сродним правима (члан 200).

3.1.1.2 Дечија порнографија

Моћ интернета имала је приличан утицај на тржиште дечије порнографије и омогућавање адекватног окружења за ширење ове појаве. Развој информационих технологија, као и доступност персоналних рачунара и пратећих медија за чување и пренос података условили су експанзију постојећих, али и појаву нових облика испољавања сексуалног искоришћавања деце. Разноврсне могућности злоупотребе интернета као најпопуларније глобалне рачунарске мреже, значајно су олакшале производњу, дистрибуцију, пренос и објављивање порнографских садржаја с децом. Деликти из сфере

сексуалне експлоатације деце врло су специфична кривична дела, која садрже тешка кршења основних људских права и слобода која услед примене психичког и физичког насиља као главних метода рада трајно ремете складан и неометан раст и развој личности, јер су жртве беспомоћне и тиме лако подложне различитим видовима психичке манипулације. Најчешће је реч о поседовању, али и ширењу путем интернета порнографског материјала на којем су деца и малолетици. Починиоци тих кривичних дела су из свих социјалних сталежа, различитих годишта и нивоа образовања. У иностранству су рађене многобројне студије на ову тему и ниједна није успела да дефинише која је то категорија друштва која се бави дечијом порнографијом путем интернета. Починиоци могу да буду политичари, физички радници, доктори наука, свештеници, као и обични грађани.[89]

Под дечјом порнографијом подразумевају се порнографски садржаји који визуелно представљају децу укључену у експлицитан сексуални однос уз ласцивно приказивање дечијих гениталија и околних делова тела.[90] Данас је обичном претрагом интернета немогуће пронаћи педофилске веб-странице или форуме. Такви сајтови заштићени су шифрама, имају више нивоа приступа, а заинтересоване особе морају и саме да понуде материјал да би постали чланови. Материјал који се размењује такође је заштићен неким од метода криптовања. Да извршиоци овог дела нису само настране особе измењеног сексуалног нагона, говоре нам карактеристике овог вида криминала, а то су добра организованост и затвореност група, као и уносност, јер су приходи који се остварују таквом злоупотребом деце огромни.[91]

Кривични законик Републике Србије у делу ,,Приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију" у члану 185. прописује санкције за ова дела:,,Ко малолетнику прода, прикаже или јавним излагањем или на други начин учини доступним текстове, слике, аудио-визуелне или друге предмете порнографске садржине или му прикаже порнографску представу, казниће се новчаном

[89] Више о томе: *Компјутерски криминал све опаснији*, http://www.vesti.rs/Hronika/Kompjuterski-kriminal-sve-opasniji.html, последњи пут приступили 12.04.2016.године.

[90]Више о томе: Кораћ, С., *Сузбијање дечије порнографије на Интернету: ЕУ стандарди*, „Ревија за безбедност –стручни часопис о корупцији и организованом криминалу", Центар за безбедносне студије, год. 2, бр. 11/2008, Београд, стр. 46.

[91] Више о томе: Ћировић, Д., Јанковић, Н., Лаћевић, М., *Cyber подземље у Србији*, „Репортер", 16. 11. 2005, стр. 12.

казном или затвором до шест месеци. Ко искористи малолетника за производњу слика, аудио-визуелних или других предмета порнографске садржине или за порнографску представу, казниће се затвором од шест месеци до пет година.Ако је дело из ст. 1 и 2.овог члана извршено према детету, учинилац ће се казнити за дело из става 1 затвором од шест месеци до три године, а за дело из става 2 затвором од једне до осам година.Ко прибавља за себе или другог, поседује, продаје, приказује, јавно излаже или електронски или на други начин чини доступним слике, аудио-визуелне или друге предмете порнографске садржине настале искоришћавањем малолетног лица, казниће се затвором од три месеца до три године. Предмети из ст. 1 до 4 овог члана одузеће се."[92]

На наведени начин створена је добра основа за регулисање кривичног дела дечије педофилије која се развојем технологије све више егзистира у сајбер простору и као таква представља модел остваривања сајбер криминала.

3.1.1.3 Упад у систем као модел остваривања сајбер криминала

Компјутерске мреже могу се користити и као циљ напада. У том случајју нападају се сервиси, функције и садржаји који се налазе на мрежи. Циљ овог модела остваривања сајбер криминала је крађа услуга и података, оштећење или уништавање сервиса или целе мреже и компјутерских система, као и ометање функција њиховог рада.

Ови модели сајбер криминала, који подразумевају спретно заобилажење заштитних механизама, не врше се из злонамерних побуда, већ ради демонстрирања својих информатичких вештина којима располажу или да укажу на постојеће слабости у механизму заштите компјутерских система. Зато су на мети таквих учинилаца компјутерске мрежи, за које се с правом очекује да су максимално заштићене од електронских провала као што су: војне компјутерске комуникације, информатички системи обавештајних служби, као и државних институција.

Овај облик сајбер криминала подразумева неовлашћен електронски упад у централни рачунарски систем и његову базу података. Учиниоци тих активности могу да буду само стручњаци у области информатичке технологије, јер улазе готово неопажено, заобилазећи

[92] Кривични законик Републике Србије („Сл. гласник РС", бр. 85/2005, 88/2005 – испр., 107/2005 – испр., 72/2009 и 111/2009) чл. 185.

заштитне механизме, обично у системе за које се очекује да су заштићени управо од тих активности и обезбеђени од било које врсте електронских провала. То је својеврстан изазов за таква лица и врло чест у пракси. Често се проваљивање у рачунарске системе постиже уношењем различитих вируса чија дејства могу да буду различита или се као последица проваљивања у систем може десити случајно или намерно убацивање вируса, чиме настаје потенцијална опасност од проузроковања, односно проузроковање штета, често и непоправљивих на виталним деловима рачунарских система и њихових елемената. Једну од најпознатијих електронских провала извршила је група немачких хакера, када су успели да коришћењем персоналних компјутера продру у компјутерску мрежу Главног штаба Северноатлантског војног савеза (НАТО пакта).[93]

Мада се те активности не врше из злонамерних побуда и мада је познато да је најчешћи мотив хакера управо самодоказивање и исказивање надмоћи над било којом врстом информатичке препреке, изазова и сл., не сме се изгубити из вида да се ради о нарушавању тајности рачунарског система, и да, чак и ако никаква штета није нанета систему, те активности производе потенцијалну опасност проузроковања непоправљивих штета, а могу узроковати повреду службене или војне тајне, што је у већини кривичних законодавстава предвиђено као кривично дело с одређеним значајем, последицама и санкцијама.

У Републици Србији овај облик сајбер криминала прописан је као „Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података" у члану 302. у ставу 1, на следећи начин: „Ко се, кршећи мере заштите, неовлашћено укључи у рачунар или рачунарску мрежу, или неовлашћено приступи електронској обради података, казниће се новчаном казном или затвором до шест месеци."[94] У случају да се сними или употреби податак добијен на начин предвиђен у ставу 1, починилац ће се казнити новчаном казном или затвором до две године. Уколико су услед овог дела настали застоја или озбиљан поремећај функционисања електронске обраде и преноса података или мреже или су наступиле друге тешке последице, Кривични законик предвиђа казну затвора до три године.

[93] Више о томе: Алексић, Ж., Шкулић, М., *Криминалистика*, Правни факултет Универзитета у Београду и Јавно предузеће „Службени гласник", Београд, 2007, стр. 392–393.

[94] Кривични законик Републике Србије („Сл. гласник РС", бр. 85/2005, 88/2005 – испр., 107/2005 – испр., 72/2009 и 111/2009).

Овакве моделе, којим се остварује сајбер криминал, не могу да врше лаици ослањајући се на своју способност елоквенције и уверљивости, као што је случај са сајбер преварама. Упад у системе могу да врше хакери, који се преко својих персоналних рачунара укључују у друге информативне системе, за шта је потребно стручно знање из области информационих технологија, што се разликује од превара који могу учинити лица са мањим информатичким знањем али уз помоћ маште и довитљивости.

3.1.1.4. Сајбер тероризам и сајбер ратовање

Овај модел остваривања сајбер криминала користи се и за вршење кривичних дела сајбер ратовања и сајбер тероризма.

Сајбер ратовање, у том смислу, представља релативно нов феномен, за који би се могло рећи да спада у категорију савремених војних, али и невојних, транснационалних и безбедносних претњи. Основна специфичност сајбер ратовања јесте да бојиште није физички, већ виртуелни свет. Сајбер ратовање, према томе, може се дефинисати као подврста информационог ратовања, којој није потребно традиционално бојно поље, већ се напади одвијају у сајбер простору и усмерени су ка противничким информацијама и информационо-комуникационим инфраструктурама.

Модерни терористи све више користе високу технологију како за шпијунажу и саботажу, тако и за пропагирање својих идеја. Њихови циљеви су банке података, рачунарски ресурси, владини комуникациони системи, електроцентрале којима управљају рачунари, рафинерије нафте и аеродромска постројења. Сајбер простор обилује предностима за остваривање сајбер тероризма због: лаког приступа, нерегулисаности, одсуства цензуре и владине контрое, потенцијално велике публике у целом свету, анонимности комуникације и децентрализација, брзог протока информација, ниских трошкова постављања интернет презентација, и критичне инфраструктуре као потенцијалног циља.[95] Најважнија подручја примене сајбер простора кад су терористи у питању јесу: планирање и координација, управљање операцијама, пропаганда, прикупљање средстава, публицитет, психолошки рат, прикупљање података, регрутовање и мобилизација, умрежавање, дељење информација,

[95] Кештеровић, Ж., *Интернет као оруђе теориста*, „Ревија за безбедност – стручни часопис о корупцији и организованом криминалу", Центар за безбедносне студије, год. 2, бр. 4/2008, Београд, стр. 38.

прање новца, сајбер рат, лажне куповине софистициране опреме, биотероризам (нпр., оглашавање фалсификованих и лажних лекова) итд. Терористи могу тројако да користе интернета: као оружје (сајбер тероризам), као начин комуникације међу активистима и као медиј за обраћање јавности. Сајбер тероризам као први начин на који терористи користе интернет односи се на смишљене, политички мотивисане нападе на компјутерске системе, програме и податке, чији су исход насиље и страх, а усмерени су на цивилне мете.[96]

Први терористички напад на компјутере забележен је још 1969. године у Америчкој држави Мичиген, где су припадници једне антиратне организације под именом *Beaver* 55 напали центар за електронску обраду података познатог хемијског концерна *Dow Chemical*, за који се тврдило да производи бојне отрове, напалм и друго хемијско оружје.[97] Терористи користе интернет као средство комуникације међу активистима. Пример је Осама Бин Ладен, који је комуницирао с припадицима Ал Каиде путем покретних компјутера и бежичне мреже енкриптованих порука. [98] Такође, терористи користе интернет за обраћање јавности путем глобалне рачунарске мреже. Бројне организације ушле су у интернет простор и створиле су своје веб-странице. Терористички напади често се врло пажљиво организују да би привукли пажњу електронских медија и међународне штампе. Узимање и задржавање талаца само појачава драму. Сами таоци не значе ништа терористима. Њихова циљна група су гледаоци, а не стварне жртве.

Садржај страница терористичких организација на интернету чине информације повезане с историјатом настанка организације и битних догађаја током развоја, политичко и друштвено одређење, биографски подаци лидера и истакнутих чланова организација, њихови говори и текстови, селективни описи значајних активности у прошлости, информације о политичким и идеолошким циљевима, као и вести које садрже обавештења о актуелним дешавањиима, такође селективно приказаним. Интернет је идеалан медиј за представљање једне терористичке организације у светлу у каквом она жели да буде представљена, а са

[96] Више о томе: Зиројевић, М., *Употреба нових информатичких и комуникационих медија у сврхе тероризма*, „Ревија за безбедност – стручни часопис о корупцији и организованом криминалу", Центар за безбедносне студије, год. 2, бр. 11/2008, Београд, стр.5.

[97]Више о томе: *Draft Board and Dow Chemical Raids (1969),* http://www.hippy.com/modules.php?name= News&file=article&sid=79, последњи пут приступили 12.04.2016.године.

[98] Више о томе: Зиројевић, М., *Употреба нових информатичких и комуникационих медија у сврхе тероризма*, „Ревија за безбедност – стручни часопис о корупцији и организованом криминалу, Центар за безбедносне студије, год. 2, бр. 11/2008, Београд, стр. 5.

циљевима које овим путем врло ефикасно остварује и чија је суштина обезбеђивање подршке што већег броја присталица, као и коришћење вешто урађених и прилично садржајних презентација и текстова ради оправдања насиља, а често и демантовања било какве употребе насиља приликом организовања.

Можемо закључити да за разлику од преваре као модела за остваривање сајбер криминала, ови модели усмерени су на безбедносну структуру. Овде појединац није циљ напада. С тим у вези социјални инжињеринг приликом извршења ових модела сајбер криминала не налази примену.

3.2. КЛАСИФИКАЦИЈА МОДЕЛА ПРЕВАРА У ОКВИРУ САЈБЕР КРИМИНАЛА

Тешко је одредити свеобухватну класификацију сајбер превара због њихове масовности и свакодневног проналажења све софистицираних начина да се изврше. Међутим, ради бољег сагледавања кривичног дела преваре као облика сајбер криминала, у раду ће бити приказане сајбер преваре које су највише уздрмале сајбер простор, на које је насело највише жртава, а самим тим су биле и најпрофитабилније њиховим извршиоцима.

Критеријум за класификацију је начин учешћа жртве у извршењу кривичног дела преваре као облика сајбер криминала. С обзиром на наведени критеријум, можемо направити следећу класификацију сајбер превара:

1. Нигеријска превара;
2. преваре ауторитета;
3. спам преваре;
4. преваре с наградама;
5. преваре са злонамерним апликацијама;
6. преваре из области електронског банкарства.

Ових 6 облика сајбер превара наведено је хронолошким редом, односно према времену појављивања. Оне су се развијале и усавршаван је начин њиховог извршења од појаве нигеријских превара, које су се прве догодиле, до софистицираних превара, које је, осим на рачунарима, могуће извршити и на ,,паметним телефонима".

Развој интернета допринео је да се комуникација људи широм света олакша. Многи корисници бесплатне комуникације путем имејла и *chat room*-а платили су велики цех за радозналост и читање порука непознатих пошиљаоца. „Свемогући интернет" не би имао то својство да не пружа својим корисницима прилику за бољи живот. Преваранти су се често служили бајковитим причама о великим добицима да би жртве населе на њихову превару. Уместо срећног краја, жртве су биле ојађене, њихови снови срушени, а мањак на рачуну био је подсетник на то да „ништа није бесплатно".

До сада наведени облици сајбер криминала махом су се базирали на социјалном инжињерингу, односно на комуникацију са жртвом уз њено активно учешће у извршењу преваре. Употребом злонамерних апликација, у прво време за рачунаре, а потом и за „паметне телефоне", жртве без знања и учешћа бивају оштећене. Малициозне апликације су нашле широку примену и у области е-банкарства, што представља посебан вид сајбер превара с обзиром на специфичности извршења и највећу материјалну корист превараната.

Када наводимо облике сајбер превара, можемо да запазимо еволуцију коју су доживеле и тенденцију да жртва све мање учествује у извршењу преваре. Пристанак, тј. учешће жртве, за разлику од превазиђених нигеријских превара, које су обухватале учесталу комуникацију, преговоре и уплате новца на рачун превараната, своди се на један клик, чиме сва финансијска средства жртве постају имовина превараната.

3.2.1. Нигеријска превара

„Нигеријска превара" представља специфичан начин извршења кривичног дела преваре као облика сајбер криминала. Ова превара настала је услед развоја и глобалне улоге интернета, који је својим корисницима понудио лакшу комуникацију. Појавни облици ове преваре подразумевају лажне пословне предлоге, с тим што је новчани износ који жртва треба да уплати, а који се током комуникације с преварантом испостави као неопходан, неупоредиво мањи од износа који би требало да добије након успешно обављеног посла.

Жртве (*mugus* – нигеријски назив) по примању такве поруке стичу утисак да им се срећа осмехнула и да им је указано поверење да по завршетку посла добију милионе. Од њих се једино тражи да уплате суму новца, и то у хуманитарне сврхе, као помоћ, а за шта ће

бити вишестуко награђени. Због тога се ,,превара 419" или ,,нигеријска превара" назива ,,авансна превара".

Сигуран начин зараде који преваранти нуде жртвама, који из перспективе жртве може деловати и као легалан и као илегалан, у сваком случају довољно је привлачан да жртва не може да га одбије. Заблуду о уложеном новцу, за који ће бити вишеструко награђена, прате углавном бајковите и срцепарајуће приче. Сајбер преваранти у извршењу нигеријске преваре били су упорни и уложили су месеце на активну комуникацију са жртвом, а да би је ,,омекшали" и да би придобили њено поверење.

Када жртва пристане да уплати новац, од ње се накнадно траже нове уплате услед нових трошкова и издатака, а уз стално указивање на то да милиони само што нису пристигли на њен рачун. За ову превару користи се зависност која се јавља код коцкара. Наивни корисници ризикују мали износ новца зарад могућности да зараде милионе. Увек постоји могућност да се све изгуби. Чак и кад се уплати одређени износ новца, и када преваранти у својству пословних партнера траже нове уплате за новонастале трошкове посла, код жртве преовлада убеђење да ће на крају уследити добитак.

Неки аутори нигеријску превару описују поделивши је у следеће фазе:

1. ,,наводно службено представништво стране владе или агенције шаљу писмо, мејл или факс;
2. писмо презентира пословни предлог за трансфер више милиона долара на жртвин лични банковни рачун, а њој се нуди известан проценат као ,,прва помоћ";.
3. писмо подстиче жртву на прекоокеанско путовање да би сазнала детаље;
4. писмом се такође тражи од жртве да обезбеди бланко меморандум компаније, информције о банковном рачуну и телефонске бројеве;
5. жртва прима различита документа са службеним маркама, печатима, логом и сл., а који доказују аутентичност понуде;
6. коначно, од жртве се тражи да унапред уплати новац за различите таксе, за регистрацију, дозволе и сл``.[99]

[99] Петровић, С., *Компјутерски криминал*, Војноиздавачки завод, Београд, 2004, стр. 148–150.

Први кораци у извршењу ове преваре повезани су с креирањем налога на бесплатним платформама *Gmail*, *Hotmail* ili *Yahoo* путем ког ће се контактирати мете. Имејл адреса смишља се тако да асоцира на ауторитативну особу или институцију, на коју ће жртве насести и неће проверавати у агенцији за привредне регисте да ли у њиховој земљи постоји таква компанија или да ли на интернету постоји неко претходно искуство корисника с њима. На пример: vangtc.state.gov@usa.com, info@willyjacklawfirm.gov-tg.com, fbi.gov@zing.vnus, military.gov@gmail.com,western_union_money_transfer@hotmail.fr,westernunionpaydepartment @videobank.it, kingsjack222222@sify.com, info@alegrete.rs.gov.br, и тд. Следећи корак је тражење жртве. Имена и имејл адресе узимају се приликом пријаве на бесплатне портале. На тај начин преваранти за неколико дана могу да прикупе неколико хиљада адреса.

Као пошиљалац може да се јаве лица која стварно постоје, али су њихови идентитети украдени без њиховог знања и извршиоци кривичних дела их користе да би прикрили свој прави идентитет, или да би се снагом ауторитета одређених лица улило поверење жртвама преваре и придобило њихово поверење. Електронске поруке насловљене су на било ког примаоца поруке и из њих се не може видети коме се пошиљалац обраћа, а њихов контекст је такав да прималац поруке лако може помислити да се порука односи управо на њега.

Текст порука углавном је писан енглеским језиком да би био разумљив људима широм света на чију адресу та порука пристигне. Садржина поруке увек је таква да гађа комбинацију емотивне и похлепне стране човекове природе. Увек се у позадини јавља срцепарајућа, романтична, бајковита фабула, у којој има места за споредну улогу која ће припасти жртви. Жртва се ту приказује као херој, као храбри помагач у великим делима. Ова врста преваре експлоатисала је примарни инстинкт људске похлепе, јер се израз хуманости богато награђује. У основи ове преваре је имагинарно решење проблема, примаоци доживљавају те предлоге као светло у тунелу, врсту спаса или позив на хуманост.

У првој поруци преваранти не спомињу да прималац треба да уплати одређени новац, већ се углавном њихове молбе односе на помоћ при пребацивању новца на рачун у њиховој земљи, а за шта ће бити награђен. Међутим, већ у наредној поруци извршилац преваре „неочекивано" се сусреће с разним ситним трошковима, које једино прималац поруке може да измири било због блокираног рачуна, било због немогућности плаћања у другој држави. Углавном се као изговор користе трошкови подмићивања, накнаде у банкама, трошкови адвоката и др.

Профит који може остварити адресант обухвата милионе долара које ће наводни инвеститори на крају посла поделити са жртвом преваре, а обећавани проценат зараде креће се и до 40% од суме новца која је предмет „посла".

Ако жртва преваре пристане на понуђени „посао", извршиоци ове преваре могу да се снађу у различитим околностима које комуникација са жртвом намеће. У кратком временском року могу креирати лажни налог, фотографије и обезбедити друге доказе који ће поткрепити њихову причу попут, фалсификованих докумената с лажним печатима, потписима, лажном садржином и сл. Да би се жртва убедила у истинитост посла, извршиоци комуницирају и путем мобилних телефона користећи припејд SIM картице, које лако могу да баце и потом купе нове ради даље комуникације. Преваранти зарад профита ангажују и адвокате, банкарске службенике и друга стручна лица, која се понекад укључују у комуникацију доводећи жртву још дубље у заблуду и одржавајући је у лажном уверењу да се заиста ради о правом, а не фиктивном послу.

Као оруђе за извршење ове преваре користе се: фалсификована документација, бежични трансфери новца за пренос противправно стечених новчаних средстава, техничка средства која им омогућују анонимну комуникацију, веб-базирана електронска пошта, електронски налози предходно преузети од правих корисника, факс-машине за слање факс-порука при размени документације са жртвама преваре, услуге телекомуникационих сервиса за директну комуникацију са жртвом преваре, као и лажне странице на интернету којима се оштећени доводи у заблуду да комуницира и сарађује с представницима легалних и легитимних институција.[100]

Лаковерни грађани, желећи да за веома кратко време зараде велику своту новца, пристају на то да пошаљу своје личне податке, па и број банковне картице. Од оштећених се најчешће тражи да новац уплате преко *Western Union*-а и *MoneyGram*-а због брзине преноса новчаних средстава и анонимности примаоца уплате, чиме се смањује могућност откривања извршилаца. Пошто оштећени уплати одређени новчани износ према инструкцијама извршилаца кривичних дела, следи одлагање новчаних трансакција повезаних с исплатом обећане суме новца. Стално се појављују нови трошкови за оштећеног на име реализације

[100] Dyrud, M. (2005), *I brought You a good news An analysis of Nigerian 419 Letters*, Proceedings of 2005 Annual Association for Business Communication, Convention Association for Business Communication, USA, стр. 11.

посла и нова одлагања, стално се обећава „експресна" исплата новца, а жртву преваре убеђују да ће јој се улагање у договорени посао вишеструко исплатити.

Психолошки притисак се на жртве преваре додатно врши и навођењем да је тајност „посла" неопходна, пошто би корумпирани званичници неке државе присвојили новац за себе уколико би сазнали да он постоји[101]. Такав притисак понекад жртва преваре додатно врши и сама над собом (нпр., када и, пошто сазнају да су преварене, жртве преваре наставе комуникацију да би повратиле новац, пронашле извршиоце и сл.). Извршиоци кривичних дела ослањају се на чињеницу да ће, за време које прође док жртва схвати да је преварена (тј. док схвати да обећани новац не постоји), новчани трансфер који је она извршила на њихове рачуне бити исплаћен, те да оштећени неће стићи да на време блокира трансфер.

Када жртва уплати тражени износ, преварант јој се више никада не јавља, а могућност да му се уђе у траг је минимална. Чињеница је да извршиоци тих кривичних дела користе информационе технологије да би сакрили свој идентитет и физичку локацију, да би осујетили напоре полицијских служби да их открију. Поруке се шаљу углавном из интернет-кафеа, при чему се губи сваки траг правог идентитета извршилаца преваре. У Нигерији, у областима као што су, нпр., Лагос или Фестак, постоје многи интернет-кафеи који су отворени управо у те сврхе, а радно време им је од 22,30 часова до 07,00 часова ради избегавања контроле коју спроводе државни службеници.[102]

За разлику од жртве, извршилац преваре је само на добитку. У време када је откривена, пре 15 година, новинар са Запада упитао је једног од превараната шеме 419 „Колико кошта извођење ове преваре?". На питање новинара преварант је одговорио: „Два долара. Долар да се плати сат интернета у кафеу и још долар да се попије кафа."[103]

Као најризичније државе из којих се врше ове врсте превара означене су државе западне Африке: Нигерија, Гана, Бенин, Обала Слоноваче, Того и Буркина Фасо. Ван

[101] Buchanan, J., Grant, A. (2001), *Investigating and Prosecuting Nigerian Fraud*, „U. S. Attorneys' Bulletin, vol. 49, no. 06, USA p. 39–47.

[102] Chawki, M. (2006), *Anonymity in Cyberspace: Finding the Balance between Privacy and Security*, Revista da Faculdade de Direito Milton Campos, Nova Lima, Brazil, vol. 11, p 39–64.

[103] N*igerian Cyber Scammers – LA Times*, http://www.latimes.com/la-fg-scammers20oct20-story.html, последњи пут приступили 12.04.2016.године.

територије западне Африке као најризичније државе са чијих се територија врше те врсте превара означене су Јужна Африка, Шпанија и Холандија.[104]

Због оваквих превара велику материјалну штету имају грађани који су се, вођени хуманим, емотивним или пословним разлозима, а понекад и похлепом, наивно упустили у комуникацију с имућним странцем и пристали су на то да пошаљу новац без претходне провере, верујући пошиљаоцима који користе „методе социјалног инжињеринга" да би их уверили у истинитост своје приче.

Сматра се да постоји велика „тамна бројка" када су „нигеријске преваре" у питању пошто оштећена лица или нису свесна да су преварена, или их је због околине срамота да пријаве да су оштећена. Оштећени се често плаше да пријаве такве случајеве пошто их извршиоци кривичних дела убеђују да су сами криви за то што посао није могао да се реализује, прете им да ће их тужити и сл.

Иако нигеријска превара постоји већ 15 година и на први поглед делује неозбиљно, подаци говоре да њоме преваранти добро зарађују. Према истраживањима холандске организације UAGI (Ultrascan Advaced Global *Investigationos*), губитак изазван нигеријским преварама до сада износи више од 82 милијарде долара, а само у 2013. години он износи 12,7 милијарди долара.[105] У Србији, према подацима Тужилаштва за високотехнолошки криминал, први случај нигеријске преваре пријављен је у 2009. години, а оштећење је било 2.500 долара.[106]

Приликом процесуирања ове врсте превара јавља се као проблем то што су углавном инициране с подручја Нигерије, Сенегала и Бенина, а међународна полицијска сарадња с наведеним државама до данас није довела до значајнијих резултата.

Током 2008. и 2009. године на територији Републике Србије оштећена лица пријавила су девет кривичних дела преваре с елементима „нигеријских превара", али су починиоци

[104] Више о томе: *Nigerian spam*, http://www.nigerianspam.com/people-affected-419-scam.htm, последњи пут приступили 12.04.2016.године.

[105] Више о томе: *419 Advance Fee Fraud Statistics 2013*, Released July, 2014

http://www.ultrascan-agi.com/public_html/html/ 419_statistics.html, последњи пут приступили 12.04.2016.године.

[106] Више о томе: http://www.telegraf.rs/vesti/1286463-obecavaju-vam-milione-evra-a-vi-se-lozite-evo-kako-pljackaju-srbe-foto, последњи пут приступили 12.04.2016.године.

непознати. Тим кривичним делима оштећени су држављани Републике Србије и предузећа с наше територије, а укупна имовинска штета износила је више од 60.000 евра. Оштећена лица су новац извршиоцима кривичних дела слала путем сервиса *Western Union* и *MoneyGram.*[107]

3.2.1.1 Најпознатији случајеви нигеријске преваре

3.2.1.2 Случај Miss Wumi Abdul

Преваранти приликом нигеријске преваре смишљено користе профил атрактивне усамљене богаташице да би призвали профиле тзв. електронских жигола који ће покушати да шармирају ову 26-годишњакињу на тај начин што ће бити џентлмени и прискочити у помоћ незаштићеној девојци која је већ у првом мејлу отворила душу и испричала потресну судбину своје породице. Бројне жртве су пале на причу младе девојке која је рано остала без оба родитеља с баснословном сумом на рачуну. Пошто је изгубила поверење у своје окружење, срећа јој се осмехнула када је уочила угледну и часну особу на интернету, тј. потенцијалну мету у коју може да има поверење. Свом саговорнику та млада девојка изражава молбу да јој помогне да пренесе свој новац у државу саговорника, за шта, заузврат, нуди 15% од целокупне суме новца као захвалност. Приликом сваког наредног мејла она ће истаћи да је вратила веру у људе и у част захваљујући свом саговорнику, а да би у њему изазвала сажаљење не би ли јој помогао. [108]

3.2.1.3 Случај Orient Bank Nigeria PLC

Често се садржај нигеријских превара односи на наследство. Из далеке земље жртве добијају мејл о особи која је умрла и поседује богатство, а потенцијалној жртви се нуди статус наследника. Примаоцу најпре стиже порука од легитимне институције, у овом случају *Orient Bank Nigeria*. Преваранти узимају идентитет финансијског менаџера умрлог лица господина Калед Алија (Khaled Ali), настрадалог у саобраћајној несрећи без наследника. Пошиљалац тражи странца који би наследио ,,плодове мукотрпног рада Калед Алија (Khaled

[107] *Internet prevare decenije*, http://www.informacija.rs/Clanci/Internet-prevare-decenije.html, последњи пут приступили 12.04.2016.године.

[108] Више о томе: *Wumi Abdul Nigerian Scam*, http://www.hoax-slayer.com/wumi-abdul-scam.shtml, последњи пут приступили 12.04.2016.године.

Ali), а да они не би доспели у руке корумпиране власти. Од примаоца се тражи да достави своје податке да би адвокати кренули да раде на том случају. За ову услугу мети се нуди 20% од укупног наследства за уложени идентитет и труд, при чему је тајност посла више пута наглашена. [109]

3.2.1.4 Случај charity distribution

Пример нигеријске преваре је и када се господин Питер Атах (Peter Attah) јави у нади да ће наћи особу која ће му помоћи да 15 милиона долара проследи хуманитарним организацијама. Преварант се не либи, да би придобио жртву, да измисли потресну животну причу наводног пошиљалаца, у овом случају 55-годишњака из јужне Африке који живи у Нигерији. Маштовитост преварантима не мањка. Свом измишљеном лику додељују статус председника нафтне компаније, некада ожењеног и оца двоје деце. Нажалост, чланови његове породице су преминули у саобраћајној незгоди пре 6 година. Вођен осећајем гриже савести што због посла није посветио време и пажњу својој породици, излаз тражи у помагању другима. Међутим, он је сада у болници, тешко је болестан и, по речима лекара, остало му је неколико месеци живота. Последња му је жеља да новац уложи у добротворне сврхе. Моли поштеног примаоца поруке да му помогне јер нема више поверења у своје пријатеље и рођаке, који су се окористили његовим богатством. При томе је прималац слободан да узме одређену суму за себе и своје залагање у целој мисији. У писму се наводи да је пошиљалац свестан да се ово писмо може схватити као изненађење и као неозбиљно, што може имати утицај на неприхватање, али ипак моли да се узме у обзир хуманитарни карактер који се жели постићи. [110]

3.2.1.5 Случај Use for the less privileged

Следећи је случај богате удовице којој су чланови породице преминули у цунами катастрофи приликом обиласка Шри Ланке, а којој је остало још неколико месеци живота. У писму нашироко описује свој живот испуњен само сакупљањем новца, без саосећајности и цитирањем библијских поука, као и надањима да ће њена душа завршити у рају, због чега она жели да целокупну имовину проследи хуманитарним организацијама.Особе које наседну

[109]Више о томе:Nigerijska šema (šema 419) http://www.prevara.info/ index.php? option=com_content&task=view&id=42, последњи пут приступили 12.04.2016.године.

[110] Више о томе:http://www.hoax-slayer.com/peter-attah-scam.shtml, последњи пут приступили 12.04.2016.године.

на ову превару и пошаљу своје податке, осим што губе новац који су послале за трансфер новца, отварање рачуна и др., постају и жртве крађе идентитета.[111]

3.2.1.6 Случај Mrs Tema Williams

Овај случај нигеријске преваре почиње учтивошћу, извињењем због ометања и изненађења услед неочекиваног јављања. У овом случају извршилац преваре није био превише речит и маштовит, већ је одмах циљао на предмет преваре, а то је пребацивање новца на рачун у држави примаоца мејла. Као награду пошиљалац за уложени труд нуди 2 могућности: 5% од укупне суме која се пребацује или партнерство приликом инвестиција тим новцем у држави жртве.[112]

3.2.1.7 Случај Johnson Savimbi

У овом случају, да би придобио поверење жртве, пошиљалац се одмах интересује како су прималац поруке и његова породица и нада се да су добро. Џонсон Савимби (Johnson Savimbi), који шаље мејл, жели да купи кућу у држави примаоца поруке. Поменути је син генерала кога је убила опозиција Владе председника Јозеа Едуарда дос Сантоса (Jose Eduardo Dos Santos). У мејлу се прималац моли да помогне на тај начин што ће пребацити новац на примаочев рачун у примаочевој држави, а све то треба да остане у строгој тајности. Напомиње се да је хитно потребан одговор и да у следећем мејлу треба написати телефон ради успостављања директног контакта.[113]

3.2.1.8 Случај Mother Sarah Alan Rowland

У овом примеру нигеријске преваре употребљава се вера и побожност ради добијања поверења жртве. Као пошиљалац се представља монахиња Сара Ален Роланд (Sarah Alan

[111] Више о томе:http://www.hoax-slayer.com/isabella-caromel-scam.shtml , последњи пут приступили 12.04.2016.године.

[112]Више о томе:http://www.hoax-slayer.com/tema-williams-scam.shtml, последњи пут приступили 12.04.2016.године.

[113]Више о томе: http://www.hoax-slayer.com/johnson-savimbi-scam.shtml, последњи пут приступили 12.04.2016.године.

Rowland), некадашња жена Алена Џорџа Роланда (Rev. Dr. Alan George Rowland), који је радио у немачкој амбасади у Дубајиу девет година и умро је након кратке болести. Нису имали деце. После његове смрти одлучила је да се не удаје и да не жели да има децу. У наследство је добила 48 милиона долара у Шпанској банци. По речима лекара, остало јој је још 3 месеца живота јер је оболела од рака дојки и има проблема са ходом. С обзиром на њено стање, одлучује се на овај корак у тражењу помоћи. Своје наследство жели да остави сиротиштима и удовицама али јој је потребно уверавање да ће сиротишта бити образована у складу с божјом речи да је „благословена рука која даје". Не жели да се њеног новца докопају неверници и да се тешко зарађени новац потроши на небожански начин. Њена сатисфакција је што је живот провела у хришћанству и благосиља примаоца поруке. Писмо је прожето хришћанским порукама и мотивима, чиме се жели одстранити свака сумња да је реч о превари. [114]

3.2.1.9 Случај Engr David Koni

Тражење пословног партнера, односно пословни предлог за партнера од поверења који ће суделовати у трансферу 11 милиона долара за инвестиције у држави примаоца. Од примаоца се тажи да асистира у трансферу ове суме у банку у својој држави, да посаветује о потенцијалним инвестицијама у држави и помогне да се све спровођењу пре инвестирања. За то се нуди 20% од целокупне суме. [115]

3.2.1.10 Случај Sgt. Joey Jones

Преваранти су свесни неповерљивости грађана према порукама с бајковитим могућностима, те зато у првом мејлу настоје да пруже наводне доказе о „истинитости" своје приче. Уплитање личности које су познате широким народним масама је само тактика превараната. Џој Џонс (Joey Jones) је амерички војник чији су партнери присвојили новац Садама Хусеина (око 24 милиона долара). Та средства чувају се у осигуравајућој кући чији линк прослеђује у мејлу. Желе да новац пренесу, при чему би помагач добио 30% целокупне суме. Тајност посла се напомиње, иако, по речима пошиљаоца, ризик не постоји.[116]

[114]Више о томе: http://www.hoax-slayer.com/sarah-alan-rowland-scam.shtml, последњи пут приступили 12.04.2016.године.

[115] Више о томе:http://www.hoax-slayer.com/engr-david-koni.shtml, последњи пут приступили 12.04.2016.године.

[116]Више о томе: http://www.hoax-slayer.com/sgt-joey-jones-scam.shtml, последњи пут приступили 12.04.2016.године.

3.2.1.11 Случај Mr. Wong Du

На први поглед, када кориснику интернета стигне порука с насловом „Партнерство” (енг. *Partnership*), то ће изазвати велико интересовање. Тешко је одолети знатижељи да се отвори мејл и прочита предлог господина Винга Дуа (Wong Du). Писац поруке на веома учтив начин приказује себе као банкара у Северној Кореји. Овај имагинарни банкар је вршећи свој посао открио рачун некадашњег председника господина Парка Чунг Хија (MR Park Chung Hee), који је владао 1963–1979. године. На његовом рачуну, који је остао без наследника, налази се 48 милиона долара. Предлог је следећи: као банкарски службеник Винг Ду предлаже да пребаци новац на рачун примаоца мејла, а који ће поделити на равне части. [117]

На основу приказаних примера нигеријских писама можемо спознати њихове заједничке црте :

– као пошиљалац писма јавља се имућна и угледна личност из удаљене државе;

– предмет мејла углавном привлачи пажњу, и то било да гласи „хитна помоћ” или „партнерство”;

– на почетку приче пошиљалац се представља детаљно приказујући своју трагичну судбину и појединости повезане с годинама, податке о својој породици, породичним трагедијама, чиме се жели постићи блискост с примаоцем поруке, а прича овог неочекиваног саговорника је у сваком случају веома бајковита;

– од примаоца мејла тражи се помоћ при пребацивању новца у његову државу пребивалишта, и то на његов или новоотворени рачун;

– пошиљалац поруке жели да остави утисак да послом никога не угрожавају или имовински оштећују, већ да ће се њиховом сарадњом избећи пропадање новца;

– такође, пошиљалац жели да увери да је реч о безбедном и лаком послу;

– преваранти се користе хуманошћу, жељом да се помофне и саосећајношћу примаоца поруке;

– предмет понуде је велика зарада, обично до 50% од целокупне суме, што обично износи неколико милиона долара;

– у сваком нигеријском писму траже се дискреција и тајност посла.

[117] Више о томе: http://www.hoax-slayer.com/wong-du-scam.shtml, последњи пут приступили 12.04.2016.године.

3.2.2. Преваре ауторитета (преваре с лажним профилима, тј. лажним и компромитованим профилима)

У најширем смислу ауторитет означава друштвени положај који се може приписати особи услед односа моћи и утицаја у друштвеним односима.[118] Ауторитет представља синоним за углед и на угледу засноване вредност, достојанство и утицајна снага која се стално гради и учвршћује. С особом која ужива ауторитет повезују се следеће особине: одлучност, компетенција, традиција и харизма. Услед експанзије интернета и друштвених мрежа, идентитет ових лица постао је параван сајбер преварантима за извршавање разних превара.

За извршење преваре кључан фактор је поверење жртве. Преваранти, да би убедили жртву, користе утицај и углед које особа поседује да би жртва занемарила безбедносне провере. Дакле, као мамац за извршење злоупотреба ауторитета користи се поштовање људи, репутација и широко прихваћен модел понашања. На тај начин отклања се сумња у постојање многобројних опасности, јер се комуницира или прати особе коју одликују част и поштење.

Ауторитет који одређена особа ужива користи се ради привлачења пажње жртава превара на друштвеним мрежама. Преварантима нарочито у прилог иде то што велики број људи некритички прихвата ставове и захтеве особе која ужива ауторитет. Најосетљивије групе су деца и млади, јер без велике опрезности прихватају информације на друштвеним мрежама, које наводно прослеђују ауторитативне особа.

Злоупотреба ауторитета личности на друштвеним мрежама може се извршити на 2 начина:

1) прављењем лажних профила особа које уживају ауторитет;

2) компромитовањем постојећих профила, хаковањем или на други начин преузимњем контроле над профилом особе која ужива ауторитет.

Лажно представљање је честа појава на друштвеним мрежама. Сакривање од закона, очување приватности, нелагодност услед изложености посматрању и процењивању других, недостатак самопоуздања, неповерење, шпијунирање, испитивање домета своје моћи и

[118] Више о томе: Милан Вујаклија, *Лексикон страних речи и израза*, Штампар Макарије, Београд, 2011.

воајеризам само су неки од разлога за прављење лажних профила. Кријући се иза лажног профила, преваранти имају слободу коју себи не могу да приуште у реалном животу. Најчешћи покретач за прављење лажних профила анонимних личности је радозналост и жеља да се завири у нечији живот. Међутим, при злоупотреби ауторитета лажни профил се прави под именом ауторитативне особе, а самим тим је посећенији и оставља веће последице као директни атак на репутацију жртве. Извршилац не мора лично да познаје особу која ужива ауторитет, већ информације о њој, које ће искористити као материјал за лажни профил може наћи на друштвеним мрежама или интернету. Преваранти за профилну слику, која ће се приказати приликом сваке претраге имена и презимена лица које ужива ауторитет, стављају професионалну слике високе резолуције. То и није тешко остварити јер бављење јавним послом изискује и давање интервјуа медијима који су пропраћени фото-сешном, када настају професионалне студијске фотографије високе резолуције.

На тим лажним профилима њихови администратори постављају слике које се већ могу наћи на интернету, или које може направити било ко на јавном догађају на ком присуствује позната личност. Одмах се може запазити недостатак приватних фотографија, које поставља како власник профила, тако и људи из његовог окружења. Постови других корисника с најавама догађаја, рекламама, честиткама, смешним сликама и шалама иду у корист преварантима, јер могу на њима да означе профил особе која ужива ауторитет и тиме дају до знања будућим пратиоцима да је профил активан, а самим тим и смањити вероватноћу да је лажан. Истраживање Barracuda Labs показало је да корисници лажних профила тагују фотографије 100 пута више него прави корисници (136 тагова на четири фотографије наспрам једног тага на четири фотографије).[119] Разумљиво је да ће личност која држи до свог угледа скинути ознаке с таквих слика, јер не жели да се приликом интернет претраге по упису њеног имена појављује слика компромитујућег садржаја. Такође, преваранти приступају с лажног профила разним групама, које се праве наменски, односно у вези с неким догађајима због обожавања.

Преваранти, желећи да постигну што већу уверљивост, попуњавају профил штурим информацијама о наводном кориснику (нпр., датум рођења, место рођења и пребивалишта, образовање, место запослења). Ради тога постављају статусе који су генерички, не односе се на конкретне животне ситуације и људе. Већина лажних профила лајкује свега неколико

[119] Више о томе:https://barracudalabs.com/2012/02/attackers-use-fake-friends-to-blend-into-facebook/, последњи пут приступили 12.04.2016.године.

страница док прави профили, који постоје годинама, приказују широк спектар интересовања власника профила. За разлику од лажних профила, прави профил лица које ужива ауторитет сведочи о остваривању контакта с истомишљеницима, и на њему та особа представља активности и предстојеће догађаје. Преко друштвених мрежа јавне личности, да би својим пратиоцима пружили увид у свој целокупан успех, промовишу нове пројекте, а осврћу се и на успехе и пројекте који су иза њих и значајни су за њихову каријеру. Особе, које уживају ауторитет, воде рачуна о комуникацији коју остварују на профилу и неће себи дозволити да се изражавају превише вулгарно, а особе које желе да искористе њихов профил за таква непримерена понашања – блокираће или пријавити. Супротно томе, ако се на профилу угледне особе пропагира вулгарност, насиље, представљање у негативном смислу, може се стећи утисак да је профил хакован или да је реч о лажном профилу, направљеном ради нарушавања угледа и популарности особе која ужива ауторитет.

Да би лажни профил био уверљив, преваранти имају задатак да привуку велики број пратилаца, тј. пријатеља. За многе славне и познате особе статус популарности данас се мери бројем „лајкова" на Фејсбуку, односно бројем пратилаца на Твитеру. Ради тога се преваранти служе разним триковима. Да би сакупили велики број пратилаца на друштвеним мрежама, преваранти често обећавају награде за верне пратиоце профила. Објаве следеће садржине: „сваки стоти пратилац добиће мобилни телефон нове генерације" само су један вид тих намамљивања. Уз њих постоје и нешто комплексније наградне игре, где се тражи да корисник тагује неколико пријатеља или да подели слику или линк, при чему на тај начин рекламира и представља својим пријатељима и пратиоцима лажни профил особе која ужива ауторитет, а све у погрешном уверењу да ће освојити награду.

Уз наведени метод прикупљања пратилаца, преварантима погодује опција друштвених мрежа да по аутоматизму повремено препоручују профил за праћење с обзиром на број заједничких пријатеља, а ради повезивања контаката и ширења мреже. На тај начин лажни профили сами од себе расту. Опција "*subscribe*" нуди могућност да профил прати више од 5.000 људи. Свако ко пошаље захтев за пријатељство постаје *subscriber* и прати све што се на профилу објави као јавно (енг. *public*). За кратко време „лажни профил" може стећи стотине, па и хиљаде пратилаца, чиме се одбацује свака сумња да је реч о злоупотреби ауторитета. Разумљиво је да јавне личности због своје популарности и присталица у реалности изазивају заинтересованост својих обожавалаца на виртуелним мрежама, који управо тамо могу да сазнају новости о својом миљенику, могу да прате његову временску линију, читају његове статусе и информишу се о будућим активностима у приватном и

пословном животу. Уколико, пак, профил постоји на друштвеној мрежи релативно кратко, а има превише пријатеља, оправдана је сумња да се ради о лажном профилу који из неког разлога гомила пријатеље.

Злоупотреба ауторитета, осим за прављење новог профила, може се извести и преузимањем контроле над постојећим профилом на друштвеним мрежама. Хаковање овде налази примену, јер се помоћу малициозних програма сазнају лозинке профила лица које ужива ауторитет. На тај начин преваранти се без проблема, редовним путем пријављују на налог и мењају профил или га допуњују новим објавама. Уз наведене начине, преузимање контроле над постојаћим профилом може извршити администратор задужен за ажурирање профила у име лица које ужива ауторитет, а злоупотребљавајући његово поверење. Када дођу у посед лозинке правог профила, преваранти могу да реализују своју жељу за омаловажавањем и понижавањем, остављањем непримерених објава на зиду профила те особе, објављивањем неприкладних фотографија, ширењем лажних вести и показивањем агресивног понашања у комуникацији. Заједнички именитељ оба начина извршења злоупотреба ауторитета је навођење корисника друштвених мрежа на то да помисле да угледна особа на коју гласи профил поставља објаве, комуницира, шаље захтеве за пријатељство и користи остале предности друштвених мрежа.

Мотиви злоупотребе ауторитета на друштвеним мрежама јесу:

1. омаловажавање и нарушавање угледа личности која ужива ауторитет;
2. стицање имовинске користи;
3. извршења других комплекснијих видова сајбер преваре (спам преваре, нигеријске преваре, фишинг и сајбер шпијунажа).

Прикривени велом анонимности, многи на интернету износе мишљења за која у стварном свету не би имали храбрости. Главни покретач свих дела повезаних са злоупотребом ауторитета узрокује анимозитет лица које управља налогом према лицу на које профил на друштвеној мрежи гласи. Имајући у рукама профил на име жртве коју желе да омаловажавају, преваранти износе мишљења која нису у складу са ставовима оних чија се имена налазе на насловницама налога. Циљ те објаве је да створи код посетилаца профила гнушање, негативне коментаре и одбојност према власнику профила.

Чести су случајеви да „хејтери”, да би омаловажили неку личност, у њено име постављају псовке, у негативном контексту коментаришу ситуације у политичком и јавном

животу, или слике неумесног садржаја. Све води томе да присталице лица изгубе осећај поверења, обожавања или одобравања. Посетиоци или пратиоци профила бивају згрожени понашањем које је изненађујуће и скандалозно за ту особу, а које без знања жртве може да потраје недељама, па и месецима. Вођени тим мотивом, преваранти остварују свој циљ када у свој круг уводе и дотадашње фанове и присталице лица које ужива ауторитет, а који почињу да негодују, да негативно коментаришу профил и блокирају га.

Други мотив лажног представљања и злоупотребе угледа и уважавања које неко лице поседује је стицање противправне имовинске користи. Један од примамљивих мамаца су добровољне акције за прикупљање помоћи. У име ауторитативне особе на профилима друштвених мрежа преваранти позивају присталице и пратиоце профила да се одазову прикупљању помоћи после катастрофа или за одређену особу у сврху њеног лечења и сл.

Преваранти се ослањају на рањивост посетилаца профила, њихову солидарност и хуманост, а поврх свега на поверење у особу која то објављује. Уместо рачуна угрожених, у објавама се даје рачун превараната, тако да новчани прилози завршавају у џеповима администратора лажних профила. Прављење лажних профила особа које уживају ауторитет су уносан посао преварантима због великог броја „лајкова" и пратилаца профила, а које могу да уновче. Велика посећеност и број пратилаца пресудни су за закључивање уговора у вези с рекламирањем или спомињањем неког бренда, производа или услуга на том профилу, тако да је на лажним профилима уочљиво рекламирање производа с „невероватним својствима", што може да буде алармантан сигнал за пријаву профила.

Лажни профили особа које уживају ауторитет исплатив су производ који се може уновчити на црном тржишту. Средином прошле деценије криминалци су били фокусирани на кредитне картице, да би затим своје криминалне активности проширили и на налоге корисника друштвених мрежа. Постоји 20 продавца на *eBay-у* и 58 сајтова које нуди Google Top 100 претрага, а на којима се продају лажни Твитер-профили.[120] Дилери стварају или преузимају постојеће профиле на друштвеним мрежама ауторитативних особа који могу да изазову интересовање и посећивање бројних корисника друштвених мрежа, а да би их продали особама које купују пратиоце или лајкове. Особа која купи профил, може само да промени назив профила и дотадашње пратиоце представити као своје. На тај начин купци

[120] Више о томе: https://www.barracuda.com/news/press_release/34#.VgR0a9Ltmkp, последњи пут приступили 12.04.2016.године.

тих профила стварају привид веће популарности, изазивају већу пажњу медија, добијају рекламу, а могу и да користе купљени профил за ширење малициозних програма. Према подацима истраживања *BarracudaLabs-a* из августа 2012. године, просечна цена лажних пратилаца је 18 долара за 1.000 следбеника, при чему 61% лажних Твитер налога није старији од три месеца, док је просечна старост лажних Твитер налога 19 недеља.[121]

Осим омаловажавања или стицања противправне имовинске користи, лажни профили особа које поседују ауторитет могу се искористити и за извршење других, комплекснијих облика преварних делатности. Пратиоци хакованог профила особе која ужива ауторитет јесу потенцијални примаоци спам поште, која се дефинише као порука маркетиншког карактера, а где непознати пошиљалац нуди своје услуге за које никада корисници нису изразили интересовање. Спам поруке на тај начин пристижу у име ауторитативне особе и тако обмањују примаоце да би они отворили мејл.

Фишинг се дефинише као врста напада у којем нападач путем електронске поште или лажних интернет страница покушава да дође до информација ради стицања финансијске користи: пин бројева, лозинки, бројева кредитних картица и других поверљивих информација.[122] За извршење фишинга увелико се користе лажно представљање и профили познатих особа ради привлачења пажње потенцијалне жртве, а да би заобишла традиционалне механизме безбедности. Представљајући се као угледна особа, преваранти покушавају да привуку пажњу корисника да отворе добијену поруку и кликну на линк у њој. На тај начин жртва, убеђена да комуницира с угледном личношћу, без дилеме отвара поруку и следи налоге саговорника. На тај начин жртва због уважавања и поверења у ауторитет бива изманипулисана, а њен рачунар заражен малициозним програмом и спреман за крађу података.

Злоупотребом ауторитета биле су поткрепљене и нигеријске преваре, које су у претходној деценији однеле милионе долара. Саставни део тих превара је добијање поруке од ауторитативне особе. Кључно је поверење жртве у ауторитативну особу, због чега преваранти отварају лажне профиле на друштвеним мрежама и на тај начин убеде жртву да

[121] Студија анализира случајаним узораком више од 70.000 лажних Твитер налога који се користе ради продаје у својству следбеника Твитера.

[122] Више о томе: Ранђеловић, Д., *Високотехнолошки криминал*, ,Криминалистичко-полицијска академија, Београд, 2013, стр 135,136

је заиста реч о правој особи. Представљајући се као ауторитативна особа, преваранти траже помоћ од жртве. Углавном се представљају као удовице владара које због промене режима имају проблем да пренесу наследство из државе, или као угледни функционери који траже нове пословне партнере. У тим случајевима тражи се од жртве да уложи мали износ новца, нпр. за трошкове преноса, адвоката, или отварања рачуна, при чему ће касније добити проценат од новца који је у питању. Наравно, тај добитак се никада не оствари. Чим жртве уплате тражени износ новца, лажни профил на друштвеним мрежама нестаје. Познати пример нигеријске преваре је порука од Сухе Арафат, супруге покојног палестинског лидера Јасера Арафата. У писму Суха описује како је тренутно вођство Палестинске ослободилачке организације излаже сталној тортури и понижавањима. У писму од примаоца тражи помоћ да с Арафатовог тајног рачуна пребаци 20 милиона долара. Да би то остварила, неопходно је да потенцијална жртва да број рачуна и шифру да би новац пребацила, након чега ће уследити богата награда особи која јој помогне.[123]

За извршење нигеријске преваре лажни профил на друштвеним мрежама прави се и у име бизнисмена или политичара који ће жртви предложити учествовање у нестварно уносном послу, и то било да је реч о куповини, градњи или сличним плановима. Такође, од жртве се тражи да уплати учешће у послу, при чему ће се након неког времена износ многоструко увећати. Углавном је реч о нелегалним пословима, тако да жртве, када открију да су преварене, и не пријављују случај у страху од гоњења. Постоји тамна бројка када је реч о овим преварама и постојања лажних профила ауторитативних личности уз које је вршена комуникација с оштећенима.

Злоупотребом ауторитета личности на друштвеним мрежама може се извршити сајбер шпијунажа. Шпијунажа се врши отварањем лажних профила војних заповедника и представљањем у њихово име. Познат је случај америчког морнаричког заповедника Адмирала Џејсма Ставридиса (Jamesa Stavridisa), познатог по активном коришћењу *Facebook*-а и Твитер-а и који је привукао „велики број заповедника и војника на друштвене мреже".[124] Његову популарност у сајбер простору искористили су преваранти коју су покренули профил на *Facebook*-у с његовим именом и онда се повезали с другим војницима, а потврђено је да су најмање један од тих лажних профила покренули кинески шпијуни који

[123]http://www.svbizlaw.com/nigerian.419.letters5.htm, последњи пут приступили 12.04.2016.године.

[124] https://www.facebook.com/james.stavridis, последњи пут приступили 12.04.2016.године.

су на тај начин шпијунирали Америчке заповедника и војнике.[125] Како војници верују да су потпуно сигурни на тој друштвеној мрежи јер се ослањају на подешавања приватности на *Facebook*-у, без опрезности прихватају позиве за пријатељство од наизглед познатих лица, а уопште не размишљају о томе ко би могао да буде иза тих профила. Осим самих војника, проблеме представљају и чланови њихових породица и пријатељи с којима војници деле информације о војним операцијама (поготово информације о локацијама на којима се налазе) и које онда они знају да деле на друштвеним мрежама. Пошто злоупотреба туђег имена и презимена, као и ауторитета на друштвеним мрежама представља кршење услова који су те друштвене мреже прописале, Фејсбук, Твитер и остале друштвене мреже одлучне су у намери да заштите жртве тих злоупотреба.

Да би се спречиле злоупотребе имена познатих личности и брендова, друштвена мрежа Твитер нуди могућност верификације налога плавим бецом који потврђује аутентичност налога пратиоцима профила. Следствено томе, Твитеров плави бец могу да добију утицајни људи и припадници значајних компанија, при чему ће бити одбијени захтеви „обичних корисника". На друштвеним мрежама корисници имају на располагању неколико апликација за откривање лажних профила да не би насели на злоупотребе ауторитета личности. Корисници друштвене мреже Твитер могу да користе апликацију *Fake Follower Check,* коју је развила компанија *StatusPeople,* а специјализована је за управљање друштвеним мрежама. Помоћу те апликације могу се детектовати спам профили и профили с купљеним пратиоцима.[126] Спам критеријум који користи апликација *Fake Follower Check* може указати на профил на Твитеру који има мало пратилаца на овој мрежи, али зато прати веома велики број особа. Такође, сајт *twitblock* пружа могућност испитивања пратилаца у потрази за лажним пратиоцима, који се након тога могу пријавити или блокирати.[127]

У случају сумње да још неко управља профилом на друштвеној мрежи, на друштвеној мрежи Фејсбук постоји могућност прегледа логовања с десктоп рачунара и мобилних телефона. На страници с подешавањима– *"Settings"* коришћењем опције "WhereYou'reLoggedIn" могуће је отклонити сумње.

[125]Више о томе: http://www.telegraph.co.uk/technology/9136029/How-spies-used-Facebook-to-steal-Nato-chiefs-details.html, последњи пут приступили 12.04.2016.године.

[126] Више о томе: https://fakers.statuspeople.com/, последњи пут приступили 12.04.2016.године.

[127] Више о томе: http://twitblock.org/, последњи пут приступили 12.04.2016.године.

Жртве злоупотребе ауторитета могу да пошаљу опомену власницима профила појединачно или путем адвокатских канцеларија. Да би жртва пријавила крађу идентитета и лажни профил на *Facebook*-у, потребно је кликнути на ”*Report/Block*” у доњем левом углу на *Timeline*-у лажног профила. Кликом на ту опцију појављује се мени с питањем због чега се профил пријављује и да ли је у питању особа која пријављује или познаник. Да би потврдио своје тврдње, од корисника се тражи да постави линк до оригиналног профила. На крају је неопходно дати сагласност о прихватању правила Фејсбука. Осим лица чији се углед угрожава постојањем лажног профила, и остали корисници могу да пријаве лажни профил у случају злоупотребе. Заправо, што више људи то уради, администратори Фејсбука озбиљније ће схватити пријаве, брже ће реаговати и лажни профил суспендовати.

Међутим, преваранти, да би прикрили своје активности, често блокирају прави профил ауторитативног лица, при чему лажни профил постаје невидљив за жртву чији се ауторитет злоупотребљава, чиме блокиран профил, у овом случају прави профил особе која ужива ауторитет, не може да пријави злоупотребу. Пошто нема увид у профил који га је блокирао, жртва о злоупотреби свог имена и угледа може да сазна од трећих лица, а не непосредно. Управо трећа лица у том случају могу да пријаве лажни профил и затраже његово уклањање. Оштећено лице након сазнања од трећих лица о злоупотреби свог ауторитета може да се обрати правној служби друштвених мрежа с кратиким образложењем поткрепљеним доказима. После одговарајућих провера, које трају у просеку од 3 до 10 дана, лажни профил биће обрисани с друштвене мреже.

Ко стоји иза спорног налога могуће је сазнати помоћу интернет провајдера, тј. телекомуникацијске компаније, које могу само у тачно одређеним ситуацијама да обелодане податке о својим корисницима. Тек када постоји основана сумња да је почињено кривично дело или постоји кривична пријава, провајдери морају да дају полицији податке који су јој потребни за истрагу. Ради тога Конвенција о високотехнолошком криминалу у члану 21. прописује да свака чланица треба да усвоји такве легислативне и остале неопходне мере да би омогућила својим надлежним органима да приморају даваоца услуга да у оквиру својих техничких могућности на територији те чланице прикупља или снима применом техничких уређаја или да сарађује и помаже надлежним органима у прикупљању или снимању у реалном времену података који се преносе путем компјутерских система. [128]

[128] *Конвенција о високотехнолошком криминалу*, члан 21, став 1.

Да би телекомуникационе компаније одговориле, потребно је испоштовати процедуру, тј. доставити захтев и разлоге због којих су подаци о кориснику потребни. На упућени захтев телекомуникационе мреже обелодањују IP-адресу компјутера на којима су креирани лажни профили, као и податке о власницима одређених бројева. Тим поступком утврђује се идентитет власника одређене интернет адресе, при чему та особа не мора увек да буде и извршилац злоупотреба ауторитета и администратор лажног профила. Одговорност корисника интернет адресе се претпоставља, при чему је могуће доказати супротно уз ваљане доказе. Наиме, извршилац може да буде и нека друга особа која је користила интернет мрежу тог корисника или се прикључила на мрежу бежичним путем без знања власника.

У многим земљама крађа идентитета на интернету је кривично дело, а висина затворске казне и других предвиђених казни зависи од тежине и природе самог дела, то јест од дужине периода током ког су идентитет и ауторитет лица злоупотребљавани, од тога да ли је то рађено због имовинске користи или због наношења нематеријалне штете, на пример – умањења угледа.

Када се сазна идентитет лица које је извршило злоупотребу ауторитета личности на друштвеној мрежи било прављењем лажних профила особа које уживају ауторитет или компромитовањем постојећих профила, хаковањем или на други начин преузимњем контроле над профилом особе која ужива ауторитет, оштећени може да покрене поступак за њено санкционисање. Оштећена лица могу да покрену приватну тужбу за надокнаду нематеријалне штете због повреде части и угледа. Кривични законик Републике Србије је у члану 172. у ставовима 1 и 2 прописао: „Ко износи или проноси штогод из личног или породичног живота неког лица што може шкодити његовој части или угледу, казниће се новчаном казном или затвором до шест месеци, а у случају да је ово дело учињено путем штампе, радија, телевизије или сличних средстава или на јавном скупу, учинилац ће се казнити новчаном казном или затвором до једне године.”

Ако је чињење злоупотребе ауторитета личности оставило теже последице по оштећеног, учинилац може да буде санкционисан и затвором до 3 године: „Ако је оно што се износи или преноси довело или могло довести до тешких последица за оштећеног, учинилац ће се казнити затвором до три године.” При томе, истинитост или неистинитост оног што се

износи или проноси из личног или породичног живота неког лица не може се доказивати.[129] На наведени начин може се санкционисати извршилац злоупотреба ауторитета на друштвеним мрежама. Међутим, чињеница је да ће злоупотребе ауторитета личности пратити експанзију друштвених мрежа и превазићи број правих профила.

3.2.3. Спем (*spam*) преваре

Спеминг (енгл. *spamming*) подразумева слање бројих незахтеваних порука електронске поште, најчешће комерцијалног карактера. Спемер (пошиљалац спема) шаље идентичне поруке на хиљаде имејл адреса. Те адресе су најчешће прикупљене аутоматски с веб-страница, из база података или су једноставно „погођене" насумичним коришћењем честих личних имена. У првих шест месеци 2005. године, према статистици корпорације "*Symantec*" ("*Symantec*" је светски лидер у производњи софтвера за заштиту рачунара и мрежа од сајбер напада), „спем" поруке су представљале 61% укупно размењених порука електронске поште у свету. Од тог броја, 51% потиче из САД.

По дефиницији, спем порука се шаље без дозволе примаоца, због чега се од стране ISP-а (*Internet Service Provider*) и већине корисника интернета сматра неприхватљивим понашањем. Анкете су показале да се спем сматра једном од највећих сметњи на интернету – слање тих порука у супротности је с Уговором о прихватљивом понашању корисника (*Acceptable Use Policy*) већине интернет-провајдера, те може да узрокује раскид уговора с пошиљаоцем. Спам или *junk mail* представља за примаоца нежељену електронску пошту која може да затрпа његово електронско сандуче за примање порука, а уз то је и безвредна и ненаручена. Постоје и друге врсте спама, попут спама у блогу, викијима или у чет собама (углавно на IRC-у), а може да буде реч и о имејл спаму, што је најчешћи случај. Особе, које се баве спамом, називају се на енглеском језику "*spammers*". Спам је анонимна, неочекивана, масовна електронска пошта – имејл еквивалент пошти коју добијамо „на врата", коју не очекујемо и која је потпуно безвредна.

Под спамом обично подразумевамо поруке маркетиншког карактера, у којима непознати пошиљалац нуди своје услуге за које никада корисници нису изразили

[129] Кривични законик Републике Србије, „Сл.гласник РС", бр. 85/2005, 88/2005 – испр., 107/2005 – испр., 72/2009, 111/2009, 121/2012, 104/2013 и 108/2014 (члан 172, став 3).

интересовање. Нажалост, велики број порука није само ”гњаважа" за примаочево сандуче, него је и потенцијална опасност, јер порука може да буде заражена вирусом, шпијунским или неким другим малициозним кодом. Спам је добио име по групи *Monty Python* која је рекламирала месну конзерву названу спам. Прималац спама обично из неког разлога и приступи линковима који му се нуде у спаму, а најчешћи разлози за то су знатижеља или „досада".

Данашњи забрињавајући податак да је три четвртине свих имејл порука на интернету спам последица је економије великих бројки. Наиме, послати много порука путем имејла постаје све лакше и јефтиније, а међу тих неколико милиона прималаца скоро сигурно ће се наћи неки који ће производ наручити или ће следити линк који некоме осигурава наплату рекламе. Током последње деценије коришћење и слање спам порука се раширило. У почетку се спам слао директно корисницима компјутера и било га је лако блокирати, али је у годинама које су уследиле брзо ширење интернета омогућило спамерима да јефтино и брзо шаљу масовну пошту, и то када су открили да модемима индивидуалних корисника може да приступи било ко, с било ког места у свету, и то због тога шта уопште нису били заштићени.

Слање циљаних спамова не треба мешати с обичним спамом. Кад се ради о обичном спаму, већ приликом првог погледа на мејл види се да га је послала нама непозната особа, а кад се ради о циљаном спаму, хакер се представља именом и имејл адресом нама познатих особе, фирме или владине установе. Циљани спам је дакле мејл за који прималац мисли да му га је послала њему позната особа која се наводи и као пошиљалац у оквиру имејл адресе, а у ствари је то урадио хакер користећи безбедносне пропусте мејл сервера. Важно је напоменути да је велика вероватноћа да хакер није отео тај мејл налог с ког је наводно послат спорни мејл, већ га је само виртуелно дуплирао и преко њега може да шаље мејлове, али на њега не може да их и прима.

Методе за слање спама су различите. Неки спамери траже да прегледавају имејл адресе на интернету, или „купују" имејл за људе које знају (нпр., неки журе на сајт, направе мејлове и позову кориснике да се пријаве на тај сајт). Овде су наведене две основне методе и трикови за слање спамова. Један њихов трик је стављање линка на крај поруке која изгледа попут ове: „Ако не желите да примате пуно оваквих порука, кликните овде за заустављање примања".Кад корисник кликне на линк, спамери траже корисника у адресару. Један од њих ставља списак особа које тренутно читају спам поруке. Даље, спамери траже списак и осталих спамера. Корисник тако може и да пошаље спам поруке на остале имејл адресе, које

други корисници најчешће и прочитају. Други трик спамера је стављање слике, која се не може видети. Кад корисник отвори спам поруку, захтев за отварање слике пошаље се серверу који је поседује. Кад добије захтев, корисник, читајући спам поруку, може исту такву поруку да пошаље на много других рачунара.

Спем поруке шаљу се невероватно брзо и једноставно. Помоћу обичног модема за сат времена може се послати на десетине хиљада порука. То је само једна страна трошка. Друга страна трошка је када се сав тај спам пребацује с једног пружатеља услуга на другог. Спамери знају да већина људи не желе да прима спам поруке. Због тога се користе разним методама да би натерали примаоца да отвори имејл. Тако ће у поље наслов (енг. *Subject*) ставити наслов који без отварања поруке уопште не даје до знања да се ради о спаму.

Неки спамери ослањају се на бот мреже, које претражују милионе веб-сајтова и с њих узимају све имејл адресе на које наиђу на страницама сајтова. Други се пак за помоћ обраћају сајбер-криминалном подземљу, а контакт се успоставља путем интернет форума који су у власништву криминалаца. Имејл адресе интернет корисника продају се и купују на милионе на отвореним тржиштима, а хиљаду имејл адреса коштаће вас свега један пени. LeadsAndMails.com, познат и као Buyemails.org, пример је једног таквог тржишта. Седиште је у Њу Делхију у Индији. Компанија која продаје имејл адресе тврди у својим рекламама да је њихово коришћење потпуно легално, а нема сумње да су неки од њених клијената преваранти из Нигерије.

Неки комерцијални спем сервиси укључују *botnet* мреже за слање ових порука, које помажу да се избегну антиспам мере на рачунарима корисника и заштите на серверима интернет провајдера, које функционишу на тај начин што се блокирају IP адресе које су стављене на „црне листе". Данас постоје бројне IP адресе с којих су слате те поруке и које су идентификоване као носиоци спем активности. „Црне листе" се врло често ажурирају, па извршиоци кривичних дела који користе слање оваквих порука за прибављање података морају да ангажују *botnet* мреже да би избегли блокирање њиховог пријема. Такав начин слања спем порука додатно отежава рад полицијских служби МУП-а Републике Србије, пошто корисници интернета на територији Републике Србије и не сумњају да поруке које им стижу могу да буду штетне. Сједињене Америчке Државе су прва земља која је криминализовала слање нежељених мејлова (спамова), сврставши их под одредбе тзв. CAN-SPAM закона о кривичној одговорности особа које се баве том активношћу.

Изгледа да оглашивачи полако одустају од спама и окрећу се разним врстама легитимног онлајн оглашавања која су сада доступна и која уз мање трошкове дају боље резултате од оних које може да понуди спам. Сталне апеле IT-стручњака упућене корисницима да морају редовно да ажурирају антивирусне програме на рачунарима криминалци су прошле године покушавали да искористе шаљући мејлове у којима су злоупотребљавали имена познатих произвођача антивирусног софтвера као што су *Kaspersky Lab*, *McAfee*, *ESET*, *Symantec* и др.

Чести су као спам мејлови у којима су нуде велики попусти на уређаје компаније *Apple*. Да би читава превара деловала веродостојно, преваранти су у поље „из" уносили име компаније *Apple*, иако имејл адреса није имала никакве везе с њом. Аутори тих мејлова наглашавали су да је количина робе на акцији ограничена и да је неопходно да се угради свој примерак што пре. Овај веома распрострањен трик користи се као подстицај купцима да се брже одлуче за одређени производ и кликом на линк га одмах наруче.Још једна од превара спамера била је понуда за пријем на америчке универзитете, као и понуда за онлајн образовање. Ови мејлови су често садржали линкове ка сајту са формуларима за пријаву на курсеве, а занимљиво је да адресе страница варирају од поруке до поруке и обично су направљене на сам дан слања спам поште. Ово је вероватно један од начина којима аутори масовних порука прикупљају личне податке корисника.

Злонамерни прилози пронађени су у 1,8% спам мејлова. Преваранти су често користили свој омиљени трик – слање обавештења у име познатих компанија.Лекови и производи и услуге из ове категорије и даље се углавном нуде на енглеском језику у спам мејловима. Овој врсти спам мејлова припада 30% укупног броја спам мејлова, мада је током друге половине маја овај удео порастао на 45–46%.Нежељена електонска пошта (спам) је свакодневница корисника интернета. Немали део те поште у служби је ширења малвера и то је за кориснике интернета много већи проблем од чињенице да су такви мејлови досадна напаст. Недавно истраживање, које је за потребе компаније *Halon*, која се бави безбедношћу електронске поште, спровео *TNS Global*, показало је да је већина испитаника (95%) бар једном добила спам мејл који је садржао шпијунски вирус или неки други злонамерни програм. Према подацима *TNS Global*-а, сваки једанаести корисник је отворио прилог у спам мејлу и инфицирао рачунар. Скоро трећина корисника је признала да су били на корак до отварања прилога у мејлу, али су одустали од тога после отварања спам мејла.

Спам мејлову неизоставни су део виртуелног живота корисника интернета. Иако су спамери све вештији у прикривању праве природе мејлова које масовно шаљу на адресе корисника, корисници су сада много више него раније свесни претњи сакривених у нежељеној електронској пошти. Филтери провајдера имејл сервиса нису савршени, па такви мејлови ипак успевају да пронађу пут до корисника.

Први корак који преваранти предузимају када желе да пошаљу спам поруку јесте проналажење мејл адресе циљане особе, што није толико тешко јер је то мање-више јавно доступан податак. У великом броју фирми и установа у Србији имејл адресе су обично у форми: име.презиме@називфирме.рс.Имејл адресе се такође могу открити и методама социјалног инжењеринга или упадима у базе података. Када се пронађе имејл адреса, приступа се писању и слању спама. У зависности од тога колико је хакер вичан, спам се може послати путем сајтова, који нуде такву услугу, као што је *Emkei's Fake Mailer* или програм који покреће са свог рачунара. Такви сајтови и програми обично су компромитовани и мејлове послате помоћу њих имејл сервери лако препознају као спам. Хакери који поседује веће знање упадају на веб-сервере и помоћу *php* скрипте за слање циљаних спамова, које су сами писали или је преузели са хакерских форума, шаљу спамове које мејл сервери веома тешко детектују. У зависности од умећа хакера, садржина таквог мејла може одмах да укаже на то да нешто није уреду или, што је много чешћи случај, да нас доведе у заблуду и у потпуности створи погрешну слику у вези с неком информацијом, догађајем или будућом активношћу. Тако, на пример, хакер се може циљаним спамом представити као непосредни руководилац, директор или декан и тражити од вас да отворите пратећи документ који је стигао уз мејл, а у ком се налази малициозни софтвер. Такође, фирма може да добије мејл, а да изгледа као да је добијен од фирме с којом тесно сарађује и којим је обавештена о „повољном" стању акција на берзи, те се тиме може довести у заблуду и претрпети штету због погрешне финасијске процене стања акција. Исто тако, као стратегија сајбер ратовања између две земље може да се примени циљано спамовање Владиних установа или медијских кућа лажним информацијама и саопштењима. У таквим ситуацијама хакер је обично само оруђе некога, криминалне организације, треће фирме или чак неке државе којима је интерес да на тај начин дођу до поверљивих информација, ослабе конкурентску фирму или да унесу пометњу.

Обично, док се схвати да је направљена превара, штета је већ начињена, а да се то не би догодило, потребно је озбиљно приступити овом проблему и на прави начин се заштити као појединац, фирма или Владина установа. Показатељ да се ради о спам превари може да

буде и заглавље мејла. Заглавље мејла садржи информације о томе како је тај мејл путовао од једног мејл сервера до другог и помоћу тога с великом сигурношћу можемо закључити да ли је мејл спам или није. У зависности од тога како је подешен програм за пренос мејлова MTA (engl. *Message Transfer Agent*), који мејл сервери користе за рад, у заглављу се мора видети прави пошиљалац потенцијално лажног мејла.

Програми за пријем и слање мејлова, и то како они инсталирани на рачунарима (*Outlook, Thunderbird, IncrediMail*), тако и они којима се приступа путем интернета (*Gmail, Hotmail, Yahoo!Mail*), не приказују заглавље мејла, већ се до њега долази избором кроз мените за сваки мејл посебно. Заглавље садржи већи број ставки које треба гледати и појединачно и као целину. Некада нетипичан распоред ставки у заглављу може да сигнализира да мејл није стигао с имејл адресе с које пише да је послат или да није стигао на регуларан начин.

У зависности од програма који користи и начина конфигурације, мејл сервер у заглављу треба да достави податке помоћу којих се с великом сигурношћу може утврдити веродостојност самог мејла. Ово је нестандардано поље заглавља, које генерише имејл сервер који шаље мејл и у њему се налазе подаци који служе имејл серверу који прима мејл да одлучи да ли је тај мејл спам или није спам. Ових поља у заглављу може да буде и више, а у зависности од тога како је подешен програм за пренос мејлова (MTA) који имејл сервер користи за рад. Нажалост, због непостојања стандарда којим би се дефинисало која поља треба да садржи хедер, сада имамо ситуацију да само MTA истог произвођача чита свој хедер, а остали MTA их занемарују и одмах прослеђују пристигли мејл као валидан.

Закон о оглашавању Републике Србије у члану 5. прописује: „Порука која представља огласну поруку мора бити препознатљива. Ако се Огласна порука појављује заједно са другом поруком, односно обавештењем, која нема огласну природу, огласна порука мора бити јасно означена. Забрањено је оглашавање усмерено на подсвест, као и препоручивање производа и услуга током емисија које нису намењене оглашавању и други облици скривеног оглашавања.” [130]

[130] Закон о оглашавању Републике Србије „Службени гласник РС", бр. 79/2005 і 83/2014,члан 5.

Истраживања бележе светски пад појаве спам мејлова у интернет саобраћају од почетка 2015. Године. У 2015. години САД и Русија су биле највећи извори спама. Кина је трећа држава по учешћу, а затим следе Вијетнам, Немачка и Украјина.[131]

3.2.4. Преваре с наградама – *scam* преваре

Појам игара на срећу одређен је у Закону о играма на срећу у члану 2: „Играма на срећу, у смислу овог закона, сматрају се игре у којима се учесницима, уз наплату, пружа могућност да остваре добитак у новцу, стварима, услугама или правима, при чему добитак или губитак не зависи од знања или вештине учесника у игри, него од случаја или неког неизвесног догађаја." У истом члану дефинише се шта се не сматра играма на срећу: „Играма на срећу не сматрају се игре које се приређују пред јавношћу, у којима се такмичи у знању и вештини из различитих области један или више унапред квалификованих учесника према правилима приређивача уз директно учешће учесника у игри (непосредно на месту приређивања игре или путем телефона), при чему крајњи исход зависи искључиво од постигнутих резултата из задате области."[132]

Игре на срећу налазе плодно тло на интернету. Бројне су лутрије и могућности за освајање награда, које, иако неуверљиво изгледају, привлаче велики број жртва, чиме и приход њиховим изумитељима постаје све уноснији. Први корак у извршењу ове преваре јесте слање жртвама мејла у име угледне компаније, тј. „добитницима" који никад нису уплатили тикет и који садржи информацију да су одабрани за награду као дуготрајни корисник њихових услуга. Порука је обично кратка, неколико реченица, без објашњења, уз истицање да се обрате особи за контакт. Углавном се наводи да је њихова имејл адреса одабрана, што их је учинило добитницима веома вредне награде. Награђени може да изабере између две опције исплате, а то је на „руке" или доставу на кућну адресу путем курира. Многа таква обавештења имају правописне грешке, што је поуздан знак да је реч о превари. Међутим, у неким случајевима лажне поруке немају правописне грешке, али су послате с јавних имејл сервера, као што су gmail.com, hotmail.com или yahoo.com. То може да буде показатељ да је у питању превара, јер угледне компаније увек шаљу мејлове с корпоративних адреса и неће себи дозволити коришћење преводиоца на интернет претраживачу.

[131] Више о томе: *Proportion of spam in email traffic*, https://securelist.com/analysis/quarterly-spam-reports/71759/spam-and-phishing-in-q2-of-2015/, последњи пут приступили 12.04.2016.године.

[132] Закон о играма на срећу („Сл. гласник РС", бр. 84/2004 i 85/2005 – др. закон), члан 2.

Након саопштавања о награди, ради убеђивања жртве, следе питања: "Како се осећате као победник?" и „Да ли сте некада добили на лотоу?" На крају поруке траже се скоро сви подаци о кориснику: адреса, бројеви телефона, као и имејл адреса, а наводи се и особа којој ће се „добитник" јавити. Наравно, уверавају да је све легално и да неће тражити ПИН-код. Ипак, побринули су се, док се испуњавају подаци на сајту, да се убаци вирус који ће само чекати да негде извршите плаћање картицом путем интернета и онда ће имати и ваш ПИН-код. Мејл се завршава печатом и потписом угледне компаније. Све те срећне вести имају нешто заједничко: добитник се обавештава да је освојио одређену новчану суму на некој лутрији и да мора да контактира представника лутрије да би добио освојени новац.

Ако жртва поверује да је „срећни добитник", и контактира наведену особу у мејлу, поставља јој се неколико услова. Да би жртва добила освојени новац, тражи се да најпре уплати одређену суму новца и тај се захтев креће у распону од неколико стотина хиљада долара. Такав захтев оправдава се наводним трошковима, као што су провизија за трансфер новца, порези, таксе за отварање рачуна у банци итд. „Срећни добитник" често захтевану суму за покриће наводних трошкова сматра безначајном у односу на ону коју ће добити. Међутим, када преваранти добију надокнаду за своје непостојеће трошкове, они нестају без трага и гласа, а преварени „добитник" има веома мале шансе да их икада пронађе. Радозналији „добитници" могу да потраже домен euroonlinelottery.com с ког је послата порука. Наравно, такав сајт не постоји. Уместо тога, браузер ће бити преусмерен на wn.com (*World News*). На том сајту не постоји знак за лутрију, нити га је икада било.

3.2.4.1 Најпознатији случајеви преваре са наградама

Преваре са наградама су део међународног ланца у којем криминалци с разних страна света шаљу примамљиве понуде, а заузврат траже новац да би оправдали трошкове поштарине.

Осим што би могла да остане без новца, жртва ће ризиковати своје личне и финансијске податке, које ће предати у руке преварантима наводно да би доказала свој идентитет. Такви подаци о жртви касније могу да буду искоришћени за крађу идентитета. Такве преваре још имају своју публику. Током једне такве кампање преваранти пошаљу на стотине хиљада мејлова рачунајући с тим да чак и мали проценат оних који буду насели и

послали тражене информације и новац значи да је покушај преваре успео и да се труд исплатио.

Да се преваре овог типа могу завршити веома лоше по жртве показује и прошлогодишњи случај када је 65-огодишњи држављанин Јужне Кореје заједно са својом ћерком отуптовао у јужну Африку да преузме милионе које је наводно освојио на једној таквој лутрији. Њих двоје, заједно с возачем који их је возио с аеродрома, били су тада киднаповани, а нигеријска банда која их је држала 4 дана. Тражила је од супруге „добитника" откуп од 7 милиона евра. Све се срећно завршило, отмичари су ухапшени, а таоци ослобођени, али је овај случај показао колико нас похлепа може учинити нерационалним и неопрезним и каквим се све ризицима излажемо верујући свему и сваком на интернету.

3.2.4.2 Случај фејсбукове наградне игре

У мејлу који шаље Facebook срећни „добитник" се обавештава да је победник *Facebook*-ове „међународне онлајн лутрије" за 2013. годину и да је освојио награду од 950.000 долара. Имејл адреса корисника је случајно одабрана и добитник треба да контактира „Одељење за исплате" да би преузео награду. Иако се кориснику *Facebook*-ова лутрија представља као новина и покушај компаније да захвали својим корисницима за коришћење друштвене мреже, тврдње из мејла немају везе с реалношћу. Они које заварају такве тврдње и који контактирају поменуто одељење, биће обавештени да морају да плате извесне трошкове да би им новац који су добили био пребачен на рачун. Те накнаде трошкова из правних разлога не могу да се одбију од награде, тако да корисник мора да уплати тражене новчане износе унапред, наводно на име пореза, осигурања, накнаде трошкова банке итд. Све док корисник буде спреман да плати, појављиваће се нови захтеви.

Још један пример Facebook преваре с наградама је када је путем Facebook догађаја, на који је већ позвано више од 50.000 људи, учесницима обећано да ће наводно бити подељено 300 рачунара *MacBookPro*. Било је потребно само да се придруже догађају, потврде своје учешће и поделе објаву, као и да „лајкују" слику која промовише догађај. Ништа од обећаног се неће десити. Учесници ове наградне игре нису постали богатији ни за цент, већ су остали без Facebook лозинке.[133]

[133] Више о томе: https://www.facebook.com/events/315343228636942/, последњи пут приступили 12.04.2016.године.

3.2.4.3 Случај prime lottery international

Овај пример преваре с наградама у сајбер простору приказује навођење жртве да одговори пошиљаоцу на имејл адресу која се разликује од адресе пошиљаоца с образложењем да треба послати мејл агенту или менаџеру. Уз то, овај случај је и пример како лажне поруке о добитку на лутрији увек имају неке противуречности.[134]

3.2.4.4 Случај Eu commonwealth lottery promotions

Захтев да се контактира извесни господин Маршал Елис из Нигерије, који из неког разлога користи јавни бесплатан сервис live.com, треба да буде довољан да укаже на то да је ту реч о превари. Организатори игара на срећу никад не траже од добитника да их контактирају слањем мејла на њихову личне имејл адресе. Целокупна комуникација у таквим случајевима била би обављена с пословних адреса. Најзанимљивије је следеће: ако је лутрија европска, зашто је господин Елис становник Нигерије? Фразе, као што су „Ваша емејл адреса је одабрана" (”*your email address was selected*”) или „ваша адреса је победила" ("*your address has won*") знаци су који одају преваранте. [135]

3.2.4.5 Случај Google наградне игре

Пример преваре са награђивањем је мејл који шаље наводно *Google*. *Google*-ов преводилачки сервис, *Google Translate*, олакшао је посао сајбер преварантима с интернационалним амбицијама. Некада су њихове жртве били само сународници, али сада они своје мејлове могу да шаљу на адресе корисника широм света. Ипак, коришћење онлајн сервиса за превођење је очигледно у таквим мејловима, који су препуни занимљивих лингвистичких креација које озбиљне лутријске организације никада себи не би допустиле. У овом случају се обавештава да је добитник извучен из базе података коју чини 250.000 адреса из свих држава света. Одмах у око пада нелогичност, јер је број од 250.000 мали с обзиром на

[134] Више о томе:https://en.wikipedia.org/wiki/Lottery_scam, последњи пут приступили 12.04.2016.године.

[135] Више о томе: *Congratulations, you've won! The reality behind online lotteries*, https://securelist.com/analysis/publications/36450/congratulations-youve-won-the-reality-behind-online-lotteries/, последњи пут приступили 12.04.2016.године.

укупан број корисника интернета, којих само у Србији има неколико милиона. За више информација жртва се упућује на тим за исплате, при чему треба да им достави личне податке попут: адресе, броја телефона, државе, занимања и места запослења, године старости, а имејл адреса се може, али и не мора дати.

Жртва ће лакше загристи мамац ако се у таквим порукама користе називи угледних компанија, као што су *Coca-Cola*, *Google*, *BMW*, *McDonald's*, *Microsoft* или *Yahoo!*. То жртвама улива поверење, јер је реч о мултинационалним компанијама с великим финансијским средствима, којима није проблем да награде своје верне кориснике. Нажалост, ове компаније не могу да ураде много да би спречиле да преваранти злоупотребљавају њихов углед и имена за остварење својих циљева. У наредним примерима биће приказана злоупотреба имена угледне компаније у сврху убеђивања жртве приликом преваре с наградама у сајбер простору.[136]

3.2.4.6 Случај UK national lottery

У вези с овом радосном вешћу превасходно је сумњиво то што је пошиљалац поруке Национална лутрија Велике Британије. Занимљив је део поруке у ком се каже следеће: „Онлајн извлачење спроведено је насумичним избором имејл адреса с ексклузивне листе имејл адреса појединаца и правних лица које су одбране напредном, аутоматизованом, насумичном компјутерском претрагом интернета. Иако није било продаје тикета, свим имејл адресама додељени су различити бројеви тикета..." Уз то, обећана сума од 150.000 долара делује нестварно, посебно уз једини постављен услов да се позове дати број телефона да би се договорило о преузимању награде.

3.2.5. Преваре са злонамерним апликацијама

Можемо поделити сајбер преваре по заступљености употребе малициозних програма, на:

[136]*Congratulations, you've won! The reality behind online lotteries*, https://securelist.com/analysis/publications/36450/congratulations-youve-won-the-reality-behind-online-lotteries/, последњи пут приступили 12.04.2016.године.

1) сајбер преваре без употребе малициозних програма;
2) сајбер преваре с употребом малициозних програма.

Сајбер преваре без употребе малициозних програма припадају прошлости. У сајбер преваре које су се базирале на социјалном инжињерингу без употребе малициозних програма спадају први облици нигеријских превара, превара ауторитета и лутријских превара. Доступношћу малициозних програма по приступачним ценама на интернету сајбер криминалци штеде труд и време у извршењу превара. Савремене сајбер преваре врше се комбинованим моделом, тј. употребом социјалног инжињеринга и малициозних програма. Сходно томе, раздвајање та два метода није могућа, јер се међусобно допуњују и чине преваре перфиднијим.

Преваре са злонамерним апликацијама, осим социјалног инжињеринга, користе и малициозне апликације за добијање поверљивих информација, као што су бројеви рачуна и пин-кодови. За разлику од лутријских и нигеријских превара, ту се не тражи директно новац који се правда разним трошковима, већ материјалну корист преваранти остварују помоћу података до којих су дошли управо употребом злонамерних апликација.

У последње време створен је криминални савез стручњака за фишинг (фишера) и такозваних спамера. Фишери могу да помоћу најновијих техника за масовно слање порука електронске поште, користећи банке података које садрже хиљаде имејл адреса (које су на располагању спемерима), контактирају огроман број корисника уз минималан ризик да буду идентификовани.

У питању је глобални проблем, и то нарочито због флуидности саме мреже и података који се путем ње могу размењивати, и то без обзира на стварну локацију преваранта и жртве. У ову групу превара спадају пецање (енгл. *Phishing*) и фарминг (енгл. *Pharming*), који представљају начине крађе поверљивих информација коришћењем лажних веб-сајтова, и то најчешће финансијског садржаја, где жртва уноси број рачуна и пин-код.

Први корак који предузимају сајбер преваранти јесте слање великом броју корисника (неколико десетина, стотина, па и хиљада) имејла којим се пошиљалац представља као препознатљив и веродостојан привредни субјект (банка, осигуравајуће друштво, трговинска организација итд.). У сваком случају, ове поруке су написане тако да делују као да су послате

из банака и других легитимних институција, а циљ им је да наведу примаоца да открије личне податке осетљиве природе.

У поруци се наводи да је прималац: потрошио велику количину новца, да ће картица бити укинута ако се не јави, да ће примаоцу наплатити енормну камату на износ који највероватније уопште не дугује. Порука обично садржи захтев да се хитно посети сајт дотичне организације, парадоксално објашњен као начин заштите поверљивих података корисника од нејасно аргументованих претњи. Порука, дакле, садржи адресу (*link*) чијом се активацијом жртва повезује с веб-сајтом који симулира оригинални сајт изабране организације. У следећем кораку жртва оставља личне податке на лажној (наизглед легитимној) веб-страници. Нападач настоји да усмери жртву ка одређеној веб-страници дизајнираној тако да имитира визуелни идентитет легитимне организације. Жртва даље, не сумњајући у аутентичност веб-странице, на њој оставља властите поверљиве податке.

У следећем кораку нападач користи прикупљене личне податке жртве, тј. преузима њен идентитет да би извршио незаконите финансијске трансакције. На тај начин жртве могу да претрпе значајне финансијске губитке или, у озбиљнијим случајевима, чак и губитак сопственог „електронског идентитета", који бива искоришћен за криминалне циљеве. Последице крађе извршене фишингом штетне су за жртву напада, која трпи губитак не само у економском смислу већ и у смислу репутације и кредибилитета пред различитим друштвеним институцијама (финансијским, административним, осигуравајућим итд.).

Фишинг напади функционишу зато што се ослањају на поверење људи. Претходних година ова свеприсутна друштвена платформа постала је одличан алат за нападаче, који су искористили њену популарност. Нападачи користе и страх људи да не изгубе податке да би им заправо украли те податке, и то тако што шаљу лажне захтеве за ресетовање лозинке, а који наводно долазе са *Facebook*-а.

Фарминг је много префињенија техника преваре с апликацијама, која веома личи на фишинг. У случају фарминга није потребно да жртва одговори на постављена питања да би преваранти могли да остваре своју замисао. Довољно је само отворити обавештење да би се у рачунар уселио злонамерни програм (енгл. *malware* – вирус, тројански коњ) или генератор (енгл. *key generator*), који ће красти информације с рачунара.

3.2.5.1 Најпознатији случајеви преваре са злонамерним апликацијама

3.2.5.2 Случај – верификација Твитера

Корисницима Твитера понуђена је могућност да верификују свој налог на овој социјалној мрежи. Међутим, предметни налог је успешно опонашао Твитеров званични налог ”*Verified Account*”. Заинтересовани корисник је ради тога морао да попуни образац с корисничким именом, имејл адресом, бројем пратилаца, да наведе зашто жели да његов налог буде верификован и да унесу лозинку за налог. За ту услугу корисник Твитера треба да плати надокнаду, а за шта је било потребно да унесе број своје платне картице, датум истека, име, адресу становања, број телефона и имејл налог на који ће примити потврду. На тај начин фишери су стекли могућност да хиљадама корисника украду налоге и информације о платним картицама. Они који су били толико неопрезни да су следили упутства превараната, вероватно нису ни приметили да сајт за плаћање није имао сигурну везу. Овај случај показује да креативност фишера нема границе – они ће увек пронаћи начин да преваре неискусне кориснике. Иако Твитер не прихвата захтеве за верификацију налога чак и када је налог прихватљив за верификацију, мање искусни корисници често верују да постоје начини да се заобиђу правила која су успоставили онлајн сервиси и друштвене мреже.

3.2.5.3 Случај – Твитер верификација плавим бецом

Твитер категорији утицајних људи и компанија даје се могућност верификације налога плавим бецом, којим се пратиоцима профила потврђује аутентичност налога. Да би се спречиле злоупотребе имена познатих личности и брендова, Твитер за верификацију профила плавим бецом не прихвата захтеве „обичних" корисника. Водећи се идејом да би обични корисници желели да имају плави бец поред свог твитер имена, чиме би добили на важности и утицајности, сајбер преваранти су смислили нову превару са злонамерним апликацијама. Наиме, сајбер преваранти направили су лажни твитеров веб-сајт на ком заинтересовани корисници могу да добију плави бец на свом твитер налогу без обзира на то да ли су познати или нису познати. На тој веб-страници корисник Твитера треба да унесе корисничко име и лозинку у за то предвиђена поља. Унесени подаци шаљу се криминалцима и све се то дешава у позадини, а жртва је усмерена на званичну Твитерову страну с најчешће постављаним питањима у вези с верификовањем налога. Лажна Твитер страница у овом тренутку више не постоји, или се корисницима саветује да буду опрезни када се од њих

тражи корисничко име и лозинка и да се информишу о услугама које пружа компанија на званичном сајту пре него што прихвате такве понуде.

3.2.5.4 Случај – онемогућен приступ фејсбук налогу

Пример фишинга је и када кориснику Фејсбука стигне обавештење да је онемогућен приступ његовом налогу с линком који упућује на фишинг страницу. Линк у мејлу води до странице на којој се потенцијална жртва обавештава да јој је онемогућено коришћење Фејсбук налога. Да би поново могао да користи налог, корисник у празна поља на страници треба да унесе имејл адресу којом се пријављује на Фејсбук, као и лозинку за приступ налогу. Поред тога, фишери траже од корисника и додатне информације: *webmail* адресу и припадајућу лозинку, датум рођења, сигурносно питање и одговор, као и назив земље у којој живи. Када унесе тражене податке, корисник треба да кликне на „*Confirm*". Међутим, када жртва унесе те податке, од ње ће на следећој страници бити затражени нови подаци под изговором да су ти подаци потребни када корисник купује Фејсбук кредите. Подаци које криминалци траже од корисника, између осталих, јесу име и презиме власника картице, број кредитне картице, датум њеног истека и сигурносни код. Тај део се не може прескочити, а када корисник кликне још једном на "*confirm*", отвориће се легитимна Фејсбук страница „Изјава о правима и обавезама". Уколико корисник при овој запањујућој вести остане присебан и сам унесе адресу сајта друштвене мреже у адресну траку *browser*-а, уместо да Facebook-у приступи кликом на линк у сумњивом мејлу, избећи ће превару и злоупотребу својих поверљивих података.

3.2.5.5 Случај – апликације које нуде могућност сазнавања ко посећује профил

Фишери често користе лажне апликације као мамац да би привукли потенцијалне жртве. Апликација која је привукла бројне жртве јесте она која омогућује кориснику Фејсбука да открије ко су најчешћи посетиоци његовог профила. То је већ доказано успешан метод за крађу корисничких имена и лозинки корисника. Ову малициозну апликацију могуће је активирати на два начина. Први начин подразумева преузимање софтвера који сакрива малвер који ће кориснику слати обавештење сваки пут када је Фејсбук профил посећен, као и ко га је посетио. Када се кликне на дугме "*Download*", за одобравање преузимања датотеке, преузеће се и тројанац *Infostealer* који краде информације са зараженог рачунара. Други начин односи се на уписивање корисничког имена и лозинке за Facebook налог.

3.2.5.6 Случај – промена боје фејсбук налога

Фејсбук апликација коју посете десетине хиљада корисника – *Facebook color changer* – пружа могућност промене боје фејсбук профила. Међутим, реч је о превари са злонамерним апликацијама. Када жртва кликне на линк за апликацију (apps.facebook.com/themsandcolors), директно се преусмерава на малициозни фишинг сајт. Преваранти могу да остваре своју замисао на следећи начин. Преваранти су изумели могућност крађе фејсбук токена за приступ тако што траже од корисника да погледају упуство за измену боја. У том процесу преваранти имају приступ токенима, што им омогућава повезивање са фејсбук пријатељима жртве. И ако жртва одбије да погледа упутство, њена безбедност је и даље угрожена, јер ће преваранти наметати разне начине да преузме злонамерни програм. Иако се чини да је ова превара превазиђена, преваранти су већ увежбаним мамцем успели да преваре много корисника. По објављеним резултатима истраживања компаније ”*Bitdefender*”, апликација за промену боје једна је од најраширенијих превара и налази се на другом месту топ 10 најраширенијих превара на Фејсбуку.

3.2.5.7 Случај – фишинзи усмерени на мобилне телефоне новије генерације

Преваранти, осим за класичне рачунаре, своју делатност усавршили су и за мобилне телефоне новије генерације. Засебна апликација Фејсбука, којом се приступа без претраге на интернет претраживачу, нуди многе могућности фишерима да се докопају поверљивих информација о кориснику.Фишери су дизајнирали лажну апликацију за Фејсбук, идентичну правој, где корисник треба да унесе корисничко име, имејл адресе, лозинку за фејсбук налог и да изабере сигурносно питање вероватно рачунајући на то да је корисник већ изабрао исто сигурносно питање и на неким другим сајтовима. Након уношења тих генералних података, преваранти траже уношење података о кредитној картици и на тај начин искоришћава се поверење корисника у респектабилне институције да би били украдени подаци као што су корисничко име, лозинка, имејлови или PIN-кодови.Лажна апликација Фејсбука за мобилне телефоне уочава се ако се обрати пажња на УРЛ адресу. Адреса праве Фејсбук мобилне странице је *https://m.facebook.com/login*, а поред ње је иконица катанца која је доказ да је сајт сигуран. Исти метод фишери користе када шаљу обавештења корисницима, који приступају Фејсбуку с мобилних уређаја, да су фејсбук профил пријавили други корисници и да ће бити трајно угашен. Да би се то спречило, дат је линк где корисник треба да попуни већ наведене поверљиве податке. Овака обавештења је најбоље игнорисати, а могу се проследити и на имејл адресу phish@fb.com, коју је корисницима друштвене мреже оставио Фејсбук да би

могли да пријављују случајеве као што је овај, када криминалци покушавају да дођу до њихових приватних информација. Као што се може закључити из наведених случајева, преваре са злонамерним апликацијама базиране су на недостатку безбедносне културе информатизованих маса. Већина корисника интернета није спремна да се самостално и на адекватан начин суочи с претњама у сајбер простору, иако свакодневно користи информационе системе. Милиони корисника свакодневно препуштају своје ресурсе, пословне и личне информације системима чији начин функционисања и рањивости не познају довољно.

На основу приказаних случајева превара са злонамерним апликацијама можемо приметити неколико заједничких карактеристика које се јављају у већини случајева. При извођењу превара са злонамерним апликацијама главно средство превараната је хакерска техника ”*drive-by download*”. Захваљујући функционисању те технике компјутер постаје заражен самом посетом веб-сајту на ком се налази штетни код, који је често у облику штетне скрипте. Посебно преварантима олакшава посао када су оперативни систем или апликација незаштићени, тј. када није преузет *Update*. Тада ће се штетни програм инсталирати аутоматски при приступу одређеном веб-сајту, прегледању HTML-а, мејла или кликом на *pop-up* прозор. Поред представљања у име банкарских и финансијских институција, у последње време доминирају фишинг напади на друштвеним мрежама.

3.2.6. Преваре из области електронског банкарства

Електронско банкарство је брз, ефикасан и поуздан систем који омогућава да се путем интернета приступи банци независно од времена рада банке, дакле 24 часа дневно, седам дана у недељи. На тај начин клијент банке може да приступа рачунима и да их прегледа, има увид у евиденцију трансакција, врши плаћања и трансфере новца с рачуна на рачун, мењати информације, наручује чекове и плаћа предефинисане рачуне (PTT, EDB, *Инфо стан*...).

Приступ е-банкинг сервису може се успоставити на два начина:

1. с тачно одређеног персоналног рачунара на који је претходно инсталиран софтвер који омогућује приступ серверу;
2. с било ког рачунара конектовањем на интернет, где је у оквиру веб-презентације банке посебна апликација намењена е-банкинг услугама.

Е-банкинг има бројне предности, као што су вршење трансакција без одласка у филијалу банке, уштеда времена, мања провизија и др. Међутим, нови век и нове технологије, осим предности које пружају у области е-банкарства, носе и бројне опасности. Једна од њих су и савремени пљачкаши банака – банкарски тројанци.

Успешно изведена е-банкинг превара састоји се из 4 корака.Први корак подразумева проналажење жртве. Нежељена пошта (спам) још увек је један од најефикаснијих начина да се допре до већег броја људи. Мејл мора да изгледа довољно уверљиво да жртва загризе мамац и тада је посао спамера завршен. Последњих година друштвене мреже су погодно тло за налажење жртава. Бројне апликације које нуде могућности сазнања о посетиоцима профила, промени боје профила, гледања разних снимака само су увод за е-банкинг превару. Дакле, као први корак корисников рачунар постаје заражен вирусом када несвесно кликне на злонамерни линк у фишинг мејлу, спам мејлу или можда током уобичајеног сурфовања интернетом.Други корак је куповина неког *exploit kit* пакета, који се може купити на интернету, а где их продају добро организоване групе. Пљачкаши рачунају, и то нажалост не без основа, на лоше навике већине корисника рачунара, који браузере и остале програме инсталиране на рачунарима не ажурирају редовно. То само значи да су лоповима наоружаним *exploit kit*-ом на располагању бројне добро познате рањивости које ће им омогућити приступ рачунарима жртава и потпуну контролу над њима. Треба само повезати спам мејл или апликацију с *exploit kit*-ом. Трећи корак обухвата функцију експлоита који отвара врата малверима. Инфицирање рачунара банкарски преваранти су завршили половину посла. Они могу да маневришу рачунаром, а још уз то и да инсталирају друге малвере који ће им обезбедити још могућности поред крађе поверљивих података који се односе на е-банкинг.

Тројанац специјализован за е-банкинг преваре *Zeus* од његове појаве 2007. године користи се за крађу података налога корисника е-банкинга и онлајн трговине. Овај комплексан и ефикасан малвер има много верзија, а чему је допринело јавно објављивање кода малвера Зевс, који се раније продаван по цени од 10.000 долара. [137]

Вирус Eurograbber (Еуроградбер), који је варијанта Зевса, намењен је преузимању контроле над рачунаром клијента и пресреће онлајн банкарске сесије. Појавио се 2012.

[137] Више о томе: http://www.informacija.rs/Vesti/Bankarski-Trojanac-Zeus-se-prodaje-na-Facebook-u.html, последњи пут приступили 12.04.2016.године.

године и изазвао је штету која износи више од 36 милиона евра. Пошто се жртва најпре зарази тим вирусом, нападач чека прву успешну е-банкинг пријаву жртве, приликом које излази лажна порука о провери података с молбом да клијент буде стрпљив. Током тог периода хакер је у стању да неовлашћено пренесе средства с рачуна клијента.

TSPY:BANKER.NJH је тројанац намењен за е-банкинг преваре који може да препозна када корисник укуцава било која од УРЛ-ова банака које су његови циљеви. Међутим банкама су *Banco de Brasil*, *Caixa* и *HSBC Brasil*. Он је у стању да затвори тренутно отворени прозор браузера, а ако је у питању *Google Chrome*, да прикаже поруку о грешци и да отвори нови лажни прозор *Chrome*-а. Све се то одвија тако да корисник не може да примети. У случају да корисник користи *Internet Explorer* или *Firefox*, оригиналан прозор остаје отворен, али се и тада појављује порука о грешци и лажни прозор. Ако корисник унесе корисничко име и лозинку у лажни прозор браузера, малвер путем мејла шаље те информације нападачу.[138]

Е-банкинг превара може се извести и путем СМС порука које су повезане с електронским банкарством, а помоћу малвера *ZitMo*. *ZitMo* добија команде од сервера за команду и контролу и прослеђује СМС поруке серверу који је под контролом нападача. На тај начин криминалци пресрећу *mTAN* бројеве (*mobile Transaction Authentication Number*) које банке шаљу кориснику, и то чим корисник започне трансакцију. Скоро половина заражених малвером *ZitMo* налази се у Кини. *ZitMo* тренутно угрожава и кориснике е-банкинга у Европи, посебно у Румунији и Немачкој.[139]

Корисник уопште није свестан постојања малвера који чека да се жртва пријави на свој е-банкинг налог. Када је остварена инфекција малвером, наступа четврти корак. Рачунар је под контролом пљачкаша, који га надзиру очекујући да ће заражени рачунар бити коришћен за е-банкарство. Након логовања клијента банке на е-банкинг систем нападач иницира на рачунару зараженом вирусом трансакције трансфера новца. Том приликом кориснику се појави лажни прозор за поновну идентификацију („провера података"), а ту

[138] Више о томе: http://www.informacija.rs/Sajber-hronika/Lordfenix-Prica-o-uspehu-20-ogodisnjeg-hakera-koji-prodaje-svoje-bankarske-trojance.html, последњи пут приступили 12.04.2016.године.

[139]Више о томе: Stručnjaci upozoravaju: „Bankarski" Trojanci i ransomware za Android u porastu, http://www.informacija.rs/Mobilni-telefoni/Strucnjaci-upozoravaju-Bankarski-Trojanci-i-ransomware-za-Android-u-porastu.html, последњи пут приступили 12.04.2016.године.

уписане податке нападач заправо користи за извршење трансакције. Напредни банкарски тројанци обављају своје задатке у реалном времену, у такозваним ”*man-in-the-middle*” нападима. Док корисник верује да је управо платио неки налог, новац намењен плаћању рачуна завршио је негде другде. Цео тај процес понавља се сваки пут када се корисник пријављује на свој е-банкинг налог. Да би се успешно реализовао један тако софистициран, вишеслојни напад, мора се развијти ”*Command & Control*” (C&C) серверска инфраструктура. Та инфраструктура је примала, чувала и управљала подацима које су доставили тројанци, она је и организовала нападе. Прикупљени подаци чували су се у SQL бази података за каснију употребу приликом напада. Да би се избегло откривање, нападачи су користили неколико различитих имена домена и сервера, од којих су неки били и прокси сервери да би се додатно отежала детекција. Ако би се открили, нападачи су могли лако и брзо да замене своју инфраструктуру, чиме би се обезбедио интегритет њихове инфраструктуру за нападе, као и континуитет њиховог рада и токови нелегалног новца. С техничке стране није постојала ефикасна директна заштита од такве врсте напада, па је било неопходно да клијент обрати посебну пажњу приликом уношења својих података (креденцијала) при коришћењу интернет банкарства.[140]

Корак четврти је и последње што треба да уради пљачкаши банака. Пошто прибави неопходне информације за приступ банковном рачуну жртве и изврши нелегалне финансијске трансакције, нападач се сусреће с проблемом пребацивања новца украденог електронским путем у властиту земљу будући да већина националних финансијских и безбедносних служби прати токове новца ка иностранству. Решење се најчешће проналази у коришћењу посредника који живи у истој држави као и жртва, и који често није ни свестан сопственог саучествовања у криминалној радњи. Такозвани ”*money mules*” (дословце – „мазге за пренос новца") јесу људи који на своје легитимне рачуне примају уплате украденог новца, који затим брзо пребацују на рачуне криминалаца уз занемарљиву надокнаду. Посредници, односно ”money mules” се налазе преко понуда наводно легитимне компаније за посао за радна места „агент за пренос новца", „финансијски менаџер", „менаџер продаје" итд. У огласу се наводи да се посао обавља од куће, да је радно време неколико сати недељно, а кандидат за посао треба да има само приступ интернету, док предзнање и искуство нису потребни.

[140] *Slučaj "Eurograbber": Kako je malver ukrao 36 miliona evra sa bankovnih računa evropskih korisnika*

http://www.informacija.rs/Vesti/Slucaj-Eurograbber-Kako-je-malver-ukrao-36-miliona-evra-sa-bankovnih-racuna-evropskih-korisnika.html, последњи пут приступили 12.04.2016.године.

Пример поруке чији је циљ проналажење посредника за транзит новца гласи овако: „Hello! We finding Europe persons, who can Send/Receive bank wires from our sellings, from our European clients. To not pay TAXES from international transfers in Russia. We offer 10% percent from amount u receive and pay all fees, for sending funds back. Amount from 1000 euro per day. All this activity are legal in Europe. Fill this form: http://XXX.info/index.php (before filling install yahoo! messenger please or msn), you will recieve full details very quickly.” [141] „Запослени" само треба да подигне 90% износа с рачуна и то пребаци на рачуне превараната, чиме посредник пред законом постаје саучесник у пљачки.

Е-банкинг преваре су у тој мери кулминирале да су постале врло уносан бизнис својим извршиоцима и творцима е-банкинг малвера. Статус најуспешнијег е-банкинг криминалца с правом носи *Lordfenix,* 20-годишњи студент рачунарства из Бразила. Он је у сајбер подземљу познат као један од водећих аутора више од 100 банкарских тројанаца, од којих сваки вреди више од 300 долара. Истраживачи кажу да је *Lordfenix* од априла 2013. године до сада створио више од 100 различитих банкарских тројанаца, као и друге малициозне алате. Сваки тројанац кошта око 320 долара, па је јасно колико се таленат исплатио овом младом криминалцу[142]. *Lordfenix* није једини соло играч у свету сајбер криминала. Истраживачи кажу да их има још – *Frapstar* из Канаде, *FighterPOS* из Бразила и *HawkEye* из Нигерије[143]. Међутим, све је већа појава умрежености и организованих група сајбер криминалаца у области е-банкинга.

Пример је група Анунак, која је започела нападима на малопродаје у САД, Аустралији и Европи са циљем да инфицира ПОС терминале малверима који могу да краду податке о платним картицама током трансакција. Група је напала најмање 16 таквих фирми, од којих су 12 у САД. Крађа информација о кредитним картицама потврђена је у три случаја. Група је такође компромитовала компјутере у три америчке PR имедијске организације, и то

[141]Више о томе: *'Money mules': Kriminalci ili žrtve bankarskih prevara na internet*, http://www.informacija.rs/Clanci/Money-mules-Kriminalci-ili-zrtve-bankarskih-prevara-na-internetu.html, последњи пут приступили 12.04.2016.године.

[142] Више о томе: http://www.informacija.rs/Sajber-hronika/Lordfenix-Prica-o-uspehu-20-ogodisnjeg-hakera-koji-prodaje-svoje-bankarske-trojance.html, последњи пут приступили 12.04.2016.године.

[143] Више о томе: http://www.informacija.rs/Sajber-hronika/Lordfenix-Prica-o-uspehu-20-ogodisnjeg-hakera-koji-prodaje-svoje-bankarske-trojance.html, последњи пут приступили 12.04.2016.године.

вероватно са циљем да стекне предности у трговању на берзи. Од 2013. годинеони успели су да добију приступ мрежама више од 50 руских банака и 5 платних система, а две од тих институција остале су без лиценце за обављање банкарских послова. До данас је укупно украдено више од милион рубаља (око 25 милиона долара), а већи део тога украден је у другој половини 2014. године.[144]

Група Анунак започињала је своје нападе инфекцијом рачунара запослених да би затим доспела унутар мреже. Главни алат групе је компјутерски тројанац назван Анунак, чији је код базиран на малверу *Carberp* који је дизајниран за крађу банкарских онлајн кредеиницијала. Нападачи су користили неколико метода за инфекцију рачунара тим тројанцем. То је обухватало *drive-by download* нападе коришћењем *exploit* пакета. Верује се да је група прошле године убацила малициозни код у сајт php.net да би инфицирала рачунаре посетилаца сајта. Осим тога, нападачи су користили и мејлове који су садржали малициозне фајлове, а који су изгледали као да их шаље Централна банка Русије. Малвер је инсталиран и помоћу других малициозних програма, а на основу такозваних „плаћање-по-инсталацији" договора. Просечно време које би протекло од тренутка када би група добила приступ интерној мрежи до крађе новца је 42 дана. Група је користила мрежне скенере, *keylogger*-е, *password cracker*-е, *SSH backdoorov*-е, програме за даљинску контрол, а често и *Metasploit framework* за пенетрацијско тестирање. Криминална група је у контакту с неколико власника великих бот мрежа које дистрибуирају њихов малвер масовно. Нападачи купују од власника бот мрежа информације о IP-адресама рачунара на којима власници бот мрежа имају инсталиране малвере и затим проверавају да ли те IP адресе припадају финансијским и државним институцијама. Ако је то случај, нападачи плаћају власницима бот мрежа за инсталацију својих малвера.

Званичници у САД тврде да је 1,78 милиона грађана Америке отворено признало да је преварено и да је путем електронског писма наведено да открије број платне картице, лични идентификациони број (ПИН-кôд) или друге личне податке, услед чега су претрпели материјалну штету. Процене су да је тамна бројка знатно већа – око три милиона случајева. Криминалци су „на име" недовољно опрезних Американаца зарадили скоро 1,5 милијарди долара, због чега су преваре фишингом постале уносна грана организованих криминалних

[144] Више о томе: *Ruski hakeri ukrali 25 miliona dolara od banaka i sa bankomata,* http://www.informacija.rs/Vesti/Ruski-hakeri-ukrali-25-miliona-dolara-od-banaka-i-sa-bankomata.html, последњи пут приступили 12.04.2016.године.

група. Број таквих напада непрекидно расте, и то по месечној стопи која се креће између 10 и 20%, а најчешће жртве су корисници услуга великих комерцијалних банака.[145]

Да би се сузбила ова опасност, корисницима, пак, стоје на располагању хардверска решења за борбу против злонамерних корисника информационих технологија, а ради заштите коришћења услуга електронског банкарства. Најпрактичнији су они који опонашају УСБ меморију, јер су компактни и лаки за преношење. Чим је један такав уређај укључен у УСБ прикључак рачунара, са своје платформе покреће и поставља сигурно окружење за онлајн банкарство. Иконе тих наменских апликација приказују се на посебној „радној површини", која је дизајнирана тако да заштити све апликације против логовања екрана (*screen capturing*) и кључних напада типа логера. Решење омогућава претраживање интернета (*browsing*) и вршење трансакција као и сваки стандардни претраживач, или уз додатну безбрижност коју пружа техникама софтверског учвршћивања (*software hardening*) заједно с *on-board* функцијом смарт картица. Решење је компатибилно са свим уобичајеним методама аутентификације корисника и трансакција. Такође, комбинује потписивање трансакције на екрану и *out-of-band* верификацију у једном уређају. То практично значи да се уређај прикључује у УСБ прикључак рачунара, он подиже своје заштићено окружење, преко ког се иницирају трансакције, а њихова ауторизација врши се уписивање, одговарајућег кода на самом уређају (има минијатурни дисплеј и тастатуру), који иначе користе и хардверску AEC-256 енкрипцију. Таквим решењем корисник је заштићен од заразе разноразним вирусима, ”*screen capture*” и ”*keylogger*” тројанаца. С аспекта безбедности, решење је добро, међутим с аспекта пословних лица, решење може да буде проблематично у смислу да применом оваквог производа клијенти увек морају са собом да имају дати уређај. Другим речима, ако је клијент на путу и није понео са собом уређај, неће му бити омогућена употреба услуге електронског банкарства, што у неким случајевима за одређена лица губи смисао идеје да се трансакције у сваком тренутку могу извршавати где год да је клијент, тј. корисник услуга.

3.3. ПОСЛЕДИЦЕ ПРЕВАРЕ КАО МОДЕЛА ОСТВАРИВАЊА САЈБЕР КРИМИНАЛА

Последице настале вршењем сајбер деликата могу се поделити на:

[145] Више о томе: Kerstein, P., *How Can We Stop Phishing and Pharming Scams?*, http://www.csoonline.com , последњи пут приступили 12.04.2016.године.

1. **финансијске или материјалне** – које могу да настану када учинилац врши дело ради стицања противправне имовинске користи, па ту корист за себе или другог заиста и стекне, или је не стекне, али својим делом објективно причини одређену штету, или када учинилац не поступа ради стицања користи за себе или другог, али објективно учини финансијску штету;
2. **нематеријалне –** које се огледају у неовлашћеном откривању туђих тајни, или другом индискретном штетном понашању;
3. **комбиноване последице –** које ће уследити када откривањем поверљивих информација путем злоупотребе рачунара или информатичке мреже наруши нечији углед, односно повреди морално право, а истовремено проузрокује конкретну финансијску штету.

3.3.1. Материјалне последице

Посматрано с историјске тачке, незаконита понашања усмерена на повреде или оштећења имовине, имовинских права и интереса увек су била у центру пажње у већини друштава и култура. Разлози за масовну распрострањеност сајбер деликта су многобројни, али их пре свега треба тражити у лошој економској ситуацији, недостатку сталног запослења, жељи за сигурном егзистенцијом без много рада и труда, паду моралних вредности, а све то води уласку у круг вршења сајбер превара којима се присваја противправно одузета имовина, а ради стицања неке користи за себе или другога. Како напредује технолошки развој друштва, напредују и идеје појединаца да што брже стекну што већи материјални добитак, и то без обзира на противправни начин стицања. Зато што се сматра једном од највећих вредности људског друштва (поред живота и људског тела), увек је била заштићена, а напад на њу је строго кажњаван.

Штетна последица испољава се као настала имовинска штета, али исто тако може да се испољи у виду губљења поверења у сигурност и тачност добијених информација из компјутерског система, што може узроковати различито третирање и нарушавање пословног угледа многих привредних и ванпривредних субјеката и изазвати страх од појаве нових криминалних радњи повезаних са свим нивоима функционисања компјутерског система.[146]

[146] Више о томе: Бановић, Б., *Обезбеђење доказа у криминалистичкој обради кривичног дела привредног криминалитета*, Виша школа унутрашњих послова, Београд–Земун, 2002, стр. 135.

Штете које наступају услед сајбер криминала изузетно су велике. Далеко надмашују износ штета нанетих класичним кривичним делима и могу се мерити стотинама милиона долара. Штете које наступају вршењем сајбер кривичних дела по правилу су веома велике, а често и тешко сагледиве, и обично се испостави да су и веће него што у првом тренутку сматрамо. Дакле, масовна распрострањеност финансијског пословања „из фотеље", заједно с неискуством корисника у области сајбер безбедности до сада су осигурали лаке зараде сајбер преварантима.

Експанзију сајбер криминала показују подаци компаније за рачунарску безбедност *Symantec*, произвођача антивирусног софтвера *Norton*. Према наводима у извештају *Symantec*-а, више од две трећине одраслих у свету користи интернет, или прецизније – 69% њих било је некад у свом животу жртва сајбер криминала, што значи да је милион људи дневно погођено тим незаконитим радњама. Према овом истраживању, сајбер криминалом у свету у 2011. години био је погођен 431 милион људи, уз финансијску штету од 14 милијарди долара.[147]

Верује се да је приход од сајбер криминала значајно премашио приходе од других кривичних дела, укључујући ту и трговину дрогом. Према подацима приказаним у јулу 2013. у заједничкој анализи америчког Центра за стратешке и међународне студије и компаније McAfee, годишњи губитак светске економије од сајбер криминала је већ достигао 500 милијарди долара: „Сајбер криминал глобалну економију годишње кошта око 445 долара милијарда, а штета од крађе интелектуалног власништва прелази 160 милијарди долара. Према подацима Центра за Стратешке и Међународне студије (ЦСИС) сајбер криминал је све учесталији и веома штети трговини, иновацијама и конкурентности. Глобални губитак износи између 375 и 575 милијарди долара."[148]

Највеће светске економије подносе највеће губитке. САД, Кина, Јапан и Немачка годишње губе око 200 милијарди због сајбер криминала. Губици који се односе на личне податке, попут хакованих података с кредитних картица, износе око 150 милијарди долара. Истраживања су показала и да је око 15 одсто или око 40 милиона становника Сједињених

[147] У САД је било више од 74 милиона жртава сајбер криминала, уз директне финансијске губитке од 32 милијарде долара.

[148] Више о томе: *Koliko svetsku ekonomiju košta sajber kriminal*, http://www.informacija.rs/Vesti/Koliko-svetsku-ekonomiju-kosta-sajber-kriminal.html, последњи пут приступили 12.04.2016.године.

Држава бар једном у животу било на удару хакера, при чему су им украдени лични подаци. У Турској је исти проблем погодио око 54 милиона становника, у Немачкој њих око 16 милиона, те више од 20 милиона у Кини.[149]

Истраживање, које је у јулу 2013. године спровео *Kaspersky Lab*, показало је да 41% жртава онлајн превара никада није успело да поврати новац који су им украли сајбер преваранти, иако у теорији постоји мишљење да би украден новац с онајлн рачуна банке или платни процесор требало да врате кориснику. Међутим, према подацима овог истраживања *Kaspersky Lab*-а, само 45% жртава успело је да поврати украдени новац, док је 14% успело да поврати део новца.У извештају *Kaspersky Lab*-а се даље наводи: „Трећина жртава су интернет корисници којима је новац украден током електронског плаћања, 17% током сесије e-bankinga, а 13% док су куповали на интернету. Тек сваком деветом купцу online продавница враћен је украден новац у целини. Када је реч о корисницима банака, само 15% њих је добило повраћај новца у целини."[150]

3.3.2. Нематеријалне последице

Нематеријалне последице сајбер криминала огледају се у неовлашћеном откривању туђих тајни, или другом „индискретном штетном поступању", које може да буде сајбер узнемиравање или сајбер прогањање, и то најчешће услед изостанка материјалне користи.

Поступци које карактерише сајбер узнемиравање прерастају у сајбер прогањање када се нежељена комуникација понавља, и то било да је директна, било да је индиректна, и када се врши у одређеном временском периоду, путем једног или средства интернета или више средстава интернета, као и неке друге врсте електронске комуникације. Онлајн узнемиравање може да буде директно или индиректно. Директно подразумева претње, застрашујуће поруке упућене жртви путем мејла или неким другим видом интернет комуникације, слање заражених порука или компјутерских вируса. Индиректно онлајн узнемиравање обухвата ширење гласина о жртви на различитим интернет форумима,

[149] Више о томе: http://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/, последњи пут приступили 12.04.2016.године.

[150] Више о томе: *Koliko svetsku ekonomiju košta sajber kriminal*, http://www.informacija.rs/Vesti/Koliko-svetsku-ekonomiju-kosta-sajber-kriminal.html, последњи пут приступили 12.04.2016.године.

потписивање жртве на нежељеним онлајн сервисима, као и слање порука другим корисницама у жртвино име.[151]

Неки аутори прихватају шире одређење прогањања, па сајбер прогањање сматрају видом конвенционалног прогањања, узнемиравања у неконвенционалном сајбер простору, које се врши посредством информационо-комуникационих технологија. Боциљи и сарадници сматрају да сајбер прогањање треба посматрати као независан проблем који не мора да буде ужи од појма прогањање.
Сајбер прогањање не искључује и друге уобичајне методе узнемиравањ које подразумевају физичку блискост. Информационо-комуникационе технологије не треба ограничити само на употребу рачунара и интернета. Према овим ауторима, оно што је заједничко сајбер прогањању и конвенционалном прогањању је континуираност у поступцима узнемиравања и изазивање страха код жртве.[152]

Психолошким злостављањем у сајбер простору сматраће се свака употреба психичке снаге којом починитељ повређује психички интегритет друге особе. Подразумева свако нељудско, негативно понашање према особи које се изражава наношењем душевних патњи мањег или већег интензитета.

Негативна понашања сајбер злостављача – лажно представљање, обмањивање и недозвољено саопштавање, оговарање и клеветање, вређање, узнемиравање и прогањање, као и искључивање, односно прогонство индикатори су самог психолошког злостављања у сајбер простору.Претварајући се да је неко други, злостављач може да шаље узнемиравајућу електронску пошту да би се веровало да поруке долазе од корисника налога. Поменути налог злостављач користи на основу лозинке коју му је у поверењу дао прави корисник тог налога, или на основу лозинке до које је дошао хаковањем самог налога. У сваком случају, злостављач с другим корисницама комуницира на негативан, немилосрдан или неприкладан начин претварајући се све време да изражава мишљење лица чији налог користи и чијим се

[151] Више о томе: Ellison, L., Akdeniz, Y. (1998), *Cyber-stalking: the Regulation of Harassment onthe Internet*,"Criminal Law Review", December Special Edition: Crime, Criminal Justice and the Internet, p. 29–48.

[152] Више о томе: Bocilj, P. (2003), *Victims of cyberstalking: An exploratory study of harassment perpetrated via the Internet, "*First Monday", vol. 8, no. 10, http://firstmonday.org/issues/issue8_10/bocij/index.html, последњи пут приступили 12.04.2016.године.

именом лажно представља. Поред лажног представљања, злостављач се може служити и обмањивањем, односно коришћењем лукавих трикова и обмана да би се друга особа довела у ситуацију да обелодани приватне, најчешће тајне и понижавајуће информације, које се затим даље, без знања те особе, онлајн прослеђују. Негативним понашањем сајбер злостављача сматраће се да недозвољено саопштавање личних информација о којима се нека особа поверила злостављачу.

Недозвољено саопштавање се најчешће врши јавним показивањем, постављањем или прослеђивањем туђих приватних слика или личне комуникације лицима којима те информације нису биле намењене. Међутим, недозвољено саопштавање може се вршити и путем мобилних телефона, када се другима показују или прослеђују туђе текстуалне поруке или слике начињене камерама мобилних телефона. Такође, читање сачуваних текстуалних порука с туђег телефоне може бити део овог процеса.

Оговарање и клеветање састоји се у слању или постављању увредљивих и неистинитих информација о другој особи с намером угрожавања њене репутације или пријатељстава. Те информације, у виду компромитујућих изјава или слика, могу да буду постављене на некој од интернет страница или се могу прослеђивати другим корисницима путем електронске поште или инстант порука.

Вређање је такође један од индикатора психолошког злостављања у сајбер простору. Подразумева кратку и жустру дискусију између две или више особа путем било које комуникационе технологије. Састоји се у намерном постављању или слању електронских порука с увредљивим, злобним, гневним, понижавајућим или вулгарним изразима.

Нешто другачији облик психолошког злостављања у сајбер простору који траје дуже од самог вређања, који је једностран, с најмање једним злостављачем и једном жртвом, јесте узнемиравање. Састоји се у слању увредљивих, провокативних и грубих порука једној особи или групи, и то у дужем временском периоду. Најчешће се јавља у персоналним каналима комуникације, као што је електронска пошта, али се узнемиравајуће поруке могу упућивати и путем јавних форума, као што су *chat*-собе и дискусионе групе. Узнемиравање се можев ршити како путем персоналних рачунара, тако и путем мобилних телефона, када једној особи један или више удружених злостављача шаљу на стотине или хиљаде текстуалних порука.

Индикатор психолошког злостављања који је тесно повезан с узнемиравањем јесте прогањање. Исто се односи на коришћење електронске комуникације у циљу прогањања друге особе путем узнемиравајуће и претеће електронске комуникације. Поруке које садрже претње повређивањем, оштро застрашивање и непријатне коментаре уобичајено се упућују персоналним каналима комуникације и изазивају осећај угрожености. У таквим ситуацијама индикатори психолошког злостављања се преплићу и чине издвојен догађај злостављања у сајбер простору, што узрокује страх да ће жеља за виртуелном осветом постати реалност, те су жртве уобичајено уплашене и страхују за своју безбедност. Овај облик психичког терора може резултирати психозом трајног страха и осећаја угрожености за кориснике електронских технологија свуда у свету. С тим у вези психолошко злостављање у сајбер простору представља глобалну појаву која превазилази границе свих држава света, чије се негативне последице не рефлектују само на угроженог појединца као корисника електронских технологија већ и на његово окружење и породицу, као и на друштво у целини.

Уобичајена средства електронске комуникације путем којих се испољава психолошко злостављање у сајбер простору су: текстуалне поруке или СМС-поруке које се упућују путем мобилних телефона, електронске поруке које се прослеђују у виду електронске поште, инстант поруке које се упућују у реалном времену путем бесплатних софтверских пакета, сајтови за социјално умрежавање,; онлајн причаонице које пружају могућност виртуелне комуникације између две особе или између више особа, блогови или веб-белешке као својеврсни онлајн дневници или часописи, веб-сајт као град или локација на светској електронској мрежи који садрже почетну страну и линкове за друге странице.

Једна од најшире прихваћених дефиниција сајбер прогањања је она по којој сајбер прогањање представља скуп поступака којима појединац или одређена група користећи комуникационо-информационе технологије узнемирава једну особу или више појединаца. Таква понашања обухватају претње, лажне оптужбе, као и намамљивање малолетника у сврх усексуалне експлоатације.[153]

Психолошко злостављање није нова појава, као што није ни ново понашање које овај појам описује. Као новост се једино може посматрати његова појава у тзв. сајбер простору

[153] Bocilj, P., McFarlane, L. (2002), *Online harassment: towards a definition of cyber stalking*, „Prison Service Journal", (139), p. 31–8.

условљена прогресивним развојем информационих технологија и интернет глобализацијом. Проблеми злостављања у сајбер простору производе негативне последице које се не рефлектују само на угроженог појединца већ и на његово окружење и породицу, као и на цело друштво.[154] Психолошко злостављање у сајбер простору подразумева испољавање негативних понашања према другим лицима, а која се врше уз коришћење електронских технологија као што су персонални рачунари и мобилни телефони. То даље значи да корисници електронских технологија могу да буду сталне мете психолошког злостављања у сајбер простору. Сајбер злостављачи могу да делују у било које време (24 сата током седам дана у недељи) и готово у сваком простору, јер сајбер злостављање није лимитирано физичком локацијом злостављача или жртве.[155]

Иако је значајна карактеристика психолошког злостављања понашање злостављача које се понавља током времена, у сајбер свету некада само једно негативно понашање које је извршио злостављач у сајбер простору може узроковати понављање виктимизације жртве у дужем временском периоду. Тако се, на пример, једна компромитујућа фотографија може електронским путем током одређеног временског периода прослеђивати многим различитим особама, што из перспективе сајбер жртве може да буде доживљено као поновна виктимизација. То нас даље упућује на чињеницу да онлајн комуникацију одликује постојаност у изражавању, тако да злонамерне текстуалне поруке, имејлови или фотографије, када се једном проследе у сајбер простору, постају тешко уништиви. Милиони посматрача могу такав материјал да сачувају на свом телефону или компјутеру и касније прослеђују другим корисницама. То даље означава да се психолошко злостављање у сајбер простору, као и већина традиционалног злостављања, одвија у присуству других особа које имају улогу посматрача или сведока, с том разликом што се код злостављања у сајбер простору публика може стално повећавати с протоком времена и не може се знати колико особа је, својом вољом или без своје воље, укључено у ову негативну појаву. Популарне апликације имају приступ информацијама о ГПС-локацији, тако да захваљујући томе нападачи могу да открију где корисник живи, ради и проводи већину времена.

[154] Више о томе: Б. Поповић-Ћитић, Вршњачко насиље у сајбер простору „Темида", ISSN: 1450-6637, vol. 12, no. 3. стр. 43–62, 2009, DOI: 10.2298/TEM0903043P.

[155] Више о томе: Baum, K., Catalano, S., Rand, M., Rose, K., *Stalking victimization in the United States*, Washington, DC: Bureau of justice report, US Department of justice, 2009, http://www.ojp.usdoj.gov/bjs/abstract/svus.htm, последњи пут приступили 12.04.2016.године.

У многим технолошки доминантним земљама света спроведена су истраживања која показују последице психолошког злостављања у сајбер простору, и то пре свега над школском популацијом (*cyberbullying*). Истраживање спроведено на 5.000 испитаника студентске популације у Јужној Кореји показало је да су чак 36% испитаника били жртве сајбер малтретирања током 2012. године, те да се они због тога осећају усамљено, беспомоћно и мање вредно. Статистичари британског „Телеграфа" дошли су до информације да је око 40% жена било жртва злостављања после договорених онлајн спојева, а да 20% злостављача наставља да трајно уходи жртве путем друштвених мрежа (*Facebook, MySpace, Twitter*).[156]

APA Media Psychology Division је објавио податке да прогонитељи све више користе врхунске технологије за праћење и узнемиравање својих жртава, као и да тек једна од четири жртве школског узраста пријављује неки од облика сајбер малтретирања, попут претећих мејлова или инстант порука. Процењује се да су током 2012. године чак 850.000 ученика и студената у САД били жртве (углавно женског пола). Елизабет Карл (Elizabeth Carll) наводи да сајбер злостављачи неретко откривају жртвине личне податке (право име, адреса, фотографије, радно место, школа, пријатељи, рођаци) на веб-сајту или форуму, а затим се лажно представљу са циљем објављивања материјала у жртвино име који их изврга руглу, клевеће или их исмева. Такав облик злостављања може изазвати тешке негативне последице, попут страха, поремећаја у спавањуи исхрани, као и престанак дотадашњег учествовања у различитим облицима друштвеног живота.[157]

На самом почетку било ког од форми психолошког злостављања у сајбер простору, прве последице се код жртве сајбер злостављања јављају у виду раздражљивости, анксиозности, несанице, неуобичајене аритмије, проблема с концентрацијом и проблема с органима за варење. Након одређеног времена, краћег или дужег, у зависности од самог психичког стања особе над којом се врши психолошко злостављање у сајбер простору, она почиње да сумња у своју способност, компетентност, осећа се разочарано, искључено из

[156] Више о томе: D'Ovidio, R., Doyle, R., *A study on cyber stalking: Understanding investigative hurdles*, FBI Law Enforcement Bulletin, ISSN 0014-5688, vol. 73, no. 3, p. 10–17, 2003, http://www.fbi.gov/publications.htm, последњи пут приступили 12.04.2016.године.

[157]Више о томе: Kowalski, R. M., Limber, S. P., Agatston, P. W., *Cyber Bullying: Bullying in the Digital Age*, John Wiley & Sons, ISBN: 978-14443-21-88-3, 2010.

средине.

Будући да жртва постаје емоционално рањива и да се повлачи у себе да би избегла конфликтне ситуације, јавља се њена емоционална изолација, те се жртва удаљава од људи, што даље доприноси доживљају бесмислености да се било шта предузме. На тај начин жртва сајбер злостављања се постепено искључује из реалног живота тако што све чешће касни с извршавањем својих свакодневних обавеза, и то како приватних, тако и пословних, односно одлаже завршавање започетог посла, а одбија да прихвати нове задатке, те на тај начин продужава ленчарење. Услови се компликује и појавом физичких симптома у виду хроничног умора, главобоља или безвољности. Често и сами симптоми могу да представљају додатно оптерећење, те тако узрокују апатију и губитак животних интереса. У тој фази јавља се исцрпљеност личних ресурса, жртва постаје депресивна и ничим мотивисана да било шта предузме, и то како у свом личном животу, тако и на послу. Жртва сајбер злостављања постаје цинична и равнодушна према својој околини и има потребу ижељу да побегне не само од пријатеља већ и од чланова своје породице.

Национално истраживање о прогањању у САД у 2006. години идентификовало је 3.424.100 жртава прогањања и дошло до следећих открића: „Свака четврта особа 26% била је изложена сајбер прогањању. У 83% случајева жртве су трпеле узнемиравање путем е-маил порука, а у 35% случајева путем инстант порука. Студија о сајбер прогањању у Великој Британији показала је да су жртве најчешће биле узнемираване путем е-маила и то у 79% случајева, путем инстант порука у 13% случајева путем соба за чет у 8% случајева, док су интерактивни сајтови коришћени у 2% случајева. У 92% случајева жртве су прогањане пута методом прогањања. У 83% случајева учиниоци су били мушкарци, просечног узраста од 24 године, најстарији је имао 53. године, а најмлађи 10. Жртве су у 52% случајева биле женског пола, а у 35% мушког пола. Жртве су биле просечне старости 32 године."[158]

На основу истраживања које је за предмет имало испитивање карактеристика „сајбер" прогонитеља и прављење типологије, на основу 24 случаја дошло се до података о карактеристикама жртава и учинилаца и њиховог међусобног односа, као и о поступцима „сајбер" прогањања: „У 91% жртве су биле женског пола, док је 85% било мушког пола. Жртве су биле просечно узраста до 32 године, при чему је најмлађа жртва имала 14 година, а

[158] Више о томе: D'Ovidio, R., Doyle, R.(2003), *A study on cyber stalking: understanding investigative hurdles*, „FBI Law Enforcement Bulletin", 73 (3), p 10–17, www.fbi.gov/publications, последњи пут приступили 12.04.2016.године.

најстарија 53. Учиниоци су у просеку имали 41 годину, при чему је најмлађи имао 18, а најстарији 67 година. Сајбер прогањање је у зависности од случаја до случаја трајало од 17 дана до 5 година, просечно 11,5 месеци. У највећем броју, односно у 10 случајева жртве су 'узнемираване' путем е-маил порука. У осталим случајевима узнемиравање је вршено путем '*usenet*' група и оглашивача, веб-сајтова за упознавање и *chat room*-ова пословних мрежа и друго. У 13 случајева 'он-лине' узнемиравање било је праћено '*offline*' узнемиравањем. У више од половине случајева прогонитељи су претили жртвама или њиховој породици/пријатељима. У највећем броју случајева ни жртве ни учиниоци нису били у браку/вези. Истраживање је показало да је 12 од укупног броја од 24 учиниоца имало истиорију 'сајбер' прогањања, од којих је три четвртине било процесуирано. Жртве су учиниоце у трећини случајева упознале путем информационо-комуникационих технологија. У 22% радило се о потпуним странцима, а у 12% о бившим партнерима и колегама. У три четвртине случајева ради се о мушко–женском 'сајбер' прогањању, а у преосталим случајевима оженско–женском или мушко–мушком 'сајбер' прогањању."[159]

3.3.3. Комбиноване последице

Комбиноване последице наступају откривањем одређене тајне, или повредом ауторског права. Злоупотребом компјутера или информатичке мреже нарушава се нечији углед, односно повређује се морално право а проузрокује се и конкретна финансијска штета. Учињена кривична дела, поред тога што проузрокују директну материјалну штету и друге посредне трошкове, све чешће код оштећених и жртви извршења кривичних дела изазивају бес, страх, нервозу и осећај личне несигурности и небезбедности.

Према истраживању које су спровели *Rand Corporation* и *Juniper Networks*, твитер налози се на црном тржишту плаћају више од украдених кредитних картица јер корисници твитер налога често користе иста корисничка имена и лозинке за различите налоге. Хаковање твитер налога криминалцима често открива вредне информације о другим налозима корисника, па и о налозима за е-банкарство и е-трговину. Крађа инфромација о налогу на једном сајту може да омогућити криминалцима приступ налозима на других десет сајтова. У децембру прошле године украдене информације о 40 милиона кредитних картица и 70

[159] Више о томе: McFarlane, L., Bocilj, P. (2004), *An exploration of predatory behaviour in cyberspace: Towards a typology of cyberstalkers*, „Firstmonday", no. 8 (9), p. 1–12.

милиона налога корисника америчког трговинског ланца *Target* појавиле су се у року од неколико дана на сајтовима који окупљају сајбер криминалце. Почетне цене за налоге кретале су се у распону од 20 до 135 долара по налогу, да би убрзо пале на 0,75 долара по налогу. Цене кредитних картица падају и због тога што је тржиште презасићено таквом врстом информација. Налози на друштвеним мрежама, пак, криминалцима отварају врата за приступ вреднијим подацима. Управо због тога је Твитер увео услугу двостепене верификације као додатни слој заштите за налоге.Поменуто истраживање показало је да се цене хакованих налога на друштвеним мрежама крећу од 16 до 325 долара, у зависности од врсте налога. Твитер налози на црном тржишту вреде много не само због тога шта омогућавају приступ другим налозима корисника већ због тога што за спамере, на пример, „прави" налози имају већу вредност.[160]

Комбиноване последице могу да буду и уцене о приватним информацијама до којих се дошло употребом тзв. полицијског малвера. Неретко је епилог тих случајева сајбер узнемиравања трагичан. Седамнаестогодишњи Џозеф Едвардс (Džozef Edvards) обесио се пошто је добио лажни мејл од полиције у ком се тврдило да је посећивао неке нелегалне веб-сајтове и да мора да плати 100 фунти да не би био покренут судски поступак против њега. Едвардс, који болује од аутизма, који је одиграо извесну улогу, поверовао је да је лажна мејл порука права претња. Истрага је открила да је Едвардсов лаптоп био инфициран малвером који је закључао уређај уцењујући Едвардса да плати 100 фунти путем *Ukash*-а, сервиса који отежава да се открије идентитет криминалаца који га користе да би изнудили новац од корисника. Едвардс се уплашио јер је поверовао у тврдње из мејла да су неке „непристојне" слике пронађене у његовом рачунару и да мора да плати да би спречио даље кораке полиције. Страхујући због бола који би сазнање проузроковало његовој мајци и сестри, Едвардс је одузео себи живот.[161]

Случај Џозефа Едвардса није усамљен. Тридесетшестогодишњи Марчел Датку (Marcel Datcu) из Румуније извршио је самоубиство зато што је поверовао обавештењу које је видео на рачунару, а којим му је због наводног кршења закона наложено да плати казну од 70.000 леја (15.519 евра) у замену за затворску казну у трајању од 11 година. Оно што се десило Марчелу Датку најгори је сценариј који је до сада виђен. Он је пронађен у дневној

[160] Више о томе: http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf, последњи пут приступили 12.04.2016.године.

[161] Више о томе: *Још једно самоубиство због „полицијског" малвера*. http://www.informacija.rs/Sajber-hronika/Jos-jedno-samoubistvo-zbog-policijskog-malvera.html, последњи пут приступили 12.04.2016.године.

соби обешен, са четворогодишњим сином у наручју, око чијег врата је такође био конопац. Он се на тај страшни чин одлучио пошто је у његовом браузеру била приказана лажна порука румунске полиције.

Полицијски малвери су претња с којом се корисници рачунара широм света релативно често сусрећу. Овај модел бизниса показао се до сад уносним за сајбер криминалце, јер немали број жртава поверује у истинитост упозорења које приказује малвер на зараженом рачунару. Они који наседну на овај познати трик криминалаца, плате казну која углавном не прелази износ од неколико стотина евра. Наводна казна од 7.0000 леја, колико је требало да исплати Датку криминалцима, није уобичајена, посебно у Румунији, у којој полицијски малвери обично траже мале суме, највише око 300 леја (66 евра).[162] Полицијски малвери се не повлаче са сцене зато што још увек постоји довољан број наивних корисника рачунара које ће те претње навести на то да направе корак у погрешном правцу, што сведочи и пример Данијела Периа (Daniel Pery), који је имао 17 година у тренутку када је извршио самоубиство ком су претходили бројни догађаји због којих је започео разговор на Skype–у с неким за кога је Данијел мислио да је девојка његових година. Онлајн романса се убрзо претворила у хорор за Данијела када му је запрећено да ће видео-снимак целог разговора с девојком бити послат његовим пријатељима и породици уколико на рачун отмичара не буде уплатио тражену суму новца.Сат времена касније, Данијел је скочио с моста. Преминуо је сат времена пошто су га спасиоци извукли из воде.[163] Према неким извештајима, неколико сати пред смрт Данијел је на Фацебооку и Твиттеру објавио своје корисничко име на *Skype*-у позивајући све, укључујући и непознате људе, да га контактирају. Могуће је да су криминалци, који су га касније уцењивали, тако дошли до његовог имена на *Skype*-у. Уобичајенији сценариј био би да девојка претходно постане пријатељ са жртвом на Фацебоок-у, да би касније жртва била увучена у разговор на скајпу уз веб-камере. Тај план обично подразумева да током разговора жена скине своју одећу и тако охрабри жртву да уради исто. Оно што жртва не схвата је да се цео разговор кришом снима, а ствари постају горе ако „разговор" оде у том правцу да се жртва охрабри да изведе неке сексуалне радње. Оно што следи је уцена, уз претњу да ће

[162] Више о томе: *Čovek izvršio samoubistvo zbog pretnje policijskog malvera*, http://www.informacija.rs/Sajber-hronika/Covek-izvrsio-samoubistvo-zbog-pretnje-policijskog-malvera.html, последњи пут приступили 12.04.2016.године.

[163] Више о томе: *Oprezno sa online „'romansama": Dečak zbog ucene izvršio samoubistvo posle razgovora na Skype-u*, http://www.informacija.rs/Vesti/Oprezno-sa-online-romansama-Decak-zbog-ucene-izvrsio-samoubistvo-posle-razgovora-na-Skype-u.html, последњи пут приступили 12.04.2016.године.

компромитујуће фотографије и видео-снимци бити достављени породици, пријатељима или објављени јавно на интернету. Број покушаја уцена који су познати полицијама непрестано расте, као и број деце која се јављају надлежним организацијама због тога шта су упали у исту замку.

3.4. ПРАВНА РЕГУЛАТИВА ПРЕВАРЕ КАО МОДЕЛА ОСТВАРИВАЊА САЈБЕР КРИМИНАЛА

Један од најважнијих предуслова за успешан, стабилан и одржив развој друштва свакако је и правна регулатива. Квалитет правих норми не зависи искључиво од правника. Приликом формулисања правних норми из области сајбер криминала неопходно је консултовати и стручњаке из других, ванправних области. Посебу улогу у том процесу имају стручњаци из области информационих технологија, као и економисти указивањем на могуће економске последице различитих нормативних решења, и то стога што се специфичност сајбер криминала огледа у последицама које проузрокује у виду економске штете која није лако мерљива и најчешће превазилази имовинску корист коју има појединац.Такође, с обзиром на врсту предмета којима се врше ова кривична дела приликом обликовања правних норми које прате ову област кривичног права, било би пожељно укључити и стручњаке који се баве различитим аспектима заштите животне средине, пре свега оне који се баве проблемом уништавања и рециклаже електронског отпада.

3.4.1. Правна регулатива превара као модела остваривања сајбер криминала у Републици Србији

Право реагује споро на нове технологије. С изузетком телефона и писаће машине, технолошка револуција из прошлог века није утицала на право. Право се бавило уопште технологијом стварајући нова правила у ваздушном саобраћају, у вези с генетским инжињерингом и слично.[164]

[164] Димитријевић, П., *Право информационе технологије*, Internet Law, Sven, Ниш, 2011, стр. 54.

Република Србија се с великим закашњењем укључила у област решавања проблема сајбер криминала. Од 1996. године је интернет у Србији користила најпре академска популација, а потом су се јавили и неакадемски корисници путем провајдера на комерцијалној основи. До 2003. године није постојала законска регулатива у овој области, па су учиниоци сајбер кривичних дела били изузети од кривичног гоњења, и пролазили су без било каквих последица, те су несметано вршили наведене облике компјутерског криминала.

Дана 18. 03. 2009. године у „Службеном гласнику Републике Србије", бр. 19–09 објављен је и Закон о потврђивању Конвенције о високотехнолошком криминалу. У члану 3. тог закона наводи се да су за њено спровођење задужени министарство надлежно за правосуђе, министарство надлежно за унутрашње послове и министарство надлежно за телекомуникације.

Први корак начињен је након ратификације Конвенције о сајбер криминалу и Додатног протокола марта 2009. године, када су иновирани Законик о кривичном поступку, а потом и Закон о организацији и надлежности државних органа за борбу против сајбер криминала и Кривични законик. На описани начин на територији Републике Србије створени су кривично-правни и институционални оквири за борбу против високотехнолошког криминала, а тиме и за борбу против кривичних дела преваре и рачунарских превара на интернету.

Основни материјални закон који регулише област сајбер криминала је Кривични законик Републике Србије, који је ступио на снагу 1. јануара 2006. године, а који у правни поредак Републике Србије уводи кривична дела повезана са злоупотребом компјутера у поглављу XXVII, и то под називом „Кривична дела против безбедности рачунарских података" (чл. 298–304).

Кривична дела против безбедности рачунарских података. – „Ко унесе, уништи, избрише, измени, оштети, прикрије или на други начин учини неупотребљивим рачунарски податак или програм или уништи или оштети рачунар или други уређај за електронску обраду и пренос података са намером да онемогући или знатно омете поступак електронске обраде и преноса података који су од значаја за државне органе, јавне службе, установе, предузећа или друге субјекте, казниће се затвором од шест месеци до пет година."

Прављење и уношење рачунарских вируса. – „Ко направи рачунарски вирус у намери његовог уношења у туђ рачунар или рачунарску мрежу, казниће се новчаном казном или затвором до шест месеци. Ко унесе рачунарски вирус у туђ рачунар или рачунарску мрежу и тиме проузрокује штету, казниће се новчаном казном или затвором до две године. Уређај и средства којима је учињено ово кривично дело одузеће се."

Рачунарска превара. – У ставу 1 члана 301. дефинише се и радња извршења кривичног дела рачунарска превара, и то на следећи начин: „Ко 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, казниће се новчаном казном или затвором до три године."

У ставу 2 тог члана наводи се да ће се учинилац казнити затвором од једне године до осам година ако је делом из става 1 тог члана прибављена имовинска корист која прелази износ од 450.000 динара. Ставом 3 предвиђено је да ће се учинилац казнити казном затвора од две године до десет година ако је делом из става 1 тог члана прибављена имовинска корист која прелази износ од 1.500.000 динара. Чланом 4. предвиђени су новчана казна или затвор до шест месеци уколико је дело из става 1 тог члана извршено само у намери да други буде оштећен.

Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података. – Ко се, кршећи заштите, неовлашћено укључи у рачунар или рачунарску мрежу, или неовлашћено приступи електронској обради података, казниће се новчаном казном или затвором до шест месеци. Ко употреби овако добијен податак, казниће се новчаном казном или затвором до две године.

Спречавање и ограничавање приступа јавној рачунарској мрежи. – Ко неовлашћено спречава или омета приступ јавној рачунарској мрежи, казниће се новчаном казном или затвором до једне године. Ако дело учини службено лице у вршењу службе, казниће се затвором до три године.

Неовлашћено коришћење рачунара или рачунарске мреже. – Ко неовлашћено користи рачунарске услуге или рачунарску мрежу у намери да себи прибави противправну или другом имовинску корист, казниће се новчаном казном или затвором до три месеца.

Гоњење за ово кривично дело предузима се по приватној тужби. У члану 119. и члану 304а новог закона о изменама и допунама кривичног законика, који је ступио на снагу дана 08. 09. 2009. године предвиђено је и ово: „Прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података". У ставу 1 тог члана начин извршења тог кривичног дела дефинисан је на следећи начин: „Ко поседује, прави, набавља, продаје или даје другом на употребу рачунаре, рачунарске системе, рачунарске податке и програме ради извршења кривичног дела из чл. 298 до 303 тог Законика казниће се затвором од шест месеци до три године." У ставу 2 предвиђено је да ће се предмети из става 1 овог члана одузети. На описани начин законодавац је омогућио кривично правну заштиту лица и имовине и створио је правне оквире за ефикасно спречавање кривичних дела рачунарске преваре.

Најчешће санкције које се изричу за дела компјутерског криминалитета углавном се крећу од новчаних и казни затвора до забране обављања делатности.Све кривичне санкције, када пресуда постане правоснажна, уносе се у казнену евиденцију, с тим што се у закону прописује коме се ти подаци и под којим условима могу давати и кад настаје брисање и којих осуда. За успешно праћење и сагледавање узрока, последица и најуобичајених дела и починилаца компјутерског криминалитета превасходно би требало обезбедити њихово систематско и континуирано евидентирање.[165] У већини информационо развијених земаља посебна тела и органи прате те податке (истражна комисија у Великој Британији, Национални центар за податке о компјутерском криминалитету, САД, Комисија експерата за праћење економског криминала у Немачкој и сл.), али се и у оквиру одређених међународних организација (OECD, специјализованој агенцији UN, EU) посебни подаци воде о тим делима. Осим тога, појединци–починиоци треба да знају да ће их и колико такви подаци пратити кроз професију и живот.

Институционални оквир за борбу против тих кривичних дела постављен је у Закону о организацији и надлежности државних органа за борбу против високотехнолошког криминала, који је објављен 15. 07. 2005. године у „Службеном гласнику Републике Србије", бр. 61/05. Како је Кривични законик морао да буде усклађен с Конвенцијом о сајбер криминалу, тако је Закон о организацији и надлежности државних органа за борбу против

[165] То су предвиделе и: Recommendation No. R (89) 9 on computer relating crime и Recommendation No. R (95) 13 of Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with Information Technology.

сајбер криминала морао да буде усклађен с иновираним Кривичним закоником, као и с новим законима о јавном тужилаштву, о уређењу судова и о седиштима и подручјима судова и јавних тужилаштава. Овим законом уређују се образовање, организација, надлежност и овлашћења посебних организационих јединица државних органа ради откривања, кривичног гоњења и суђења за кривична дела одређена тим законом. У члану 2. на следећи начин дефинише се високотехнолошки криминал: „Високотехнолошки криминал у смислу овог закона 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.”У члану 3. је одређена примена овог закона: „Овај закон примењује се ради откривања, кривичног гоњења и суђења за:

1) кривична дела против безбедности рачунарских података одређена Кривичним закоником;

2) кривична дела против интелектуалне својине, имовине, привреде и правног саобраћаја, код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже и рачунарски подаци, као и њихови производи у материјалном или електронском облику, ако број примерака ауторских дела прелази 2.000 динара или настала материјална штета прелази износ од 1.000.000 динара;

3) кривична дела против слобода и права човека и грађанина, полне слободе, јавног реда и мира и уставног уређења и безбедности Републике Србије, која се због начина извршења или употребљених средстава могу сматрати кривичним делима високотехнолошког криминала, у складу са чланом 2. став 1. овог закона."[166]

Наведеним Законом установљене су институције за борбу против високотехнолошког криминала: посебан тужилац за високотехнолошки криминал Окружног јавног тужилаштва у Београду надлежан за читаву територију Републике Србије, Савет за борбу против високотехнолошког криминала Окружног суда у Београду и Служба за борбу против високотехнолошког криминала у оквиру МУП-а Републике Србије.

3.4.2. Иностранa правна регулатива превара као модела остваривања сајбер криминала

Међународна конвенција која регулише питање сајбер криминала – Конвенција о сајбер криминалу Савета Европе, донета је у Будимпешти 2001. године. Конвенција је

[166] Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала „Службени гласник Републике Србије”, бр. 61/05.

ступила на снагу 2004. године и омогућава државама да развију легислативу у борби против сајбер криминала.

Доношење конвенција о сајбер криминалу представља свеобухватан покушај да се правно уобличи борба против високотехнолошког криминала на међународном нивоу. Конвенција о сајбер криминалу осмишљена је ради спречавања дела која су усмерена против интегритета, поверљивости и доступности компјутерских система, мрежа и података, а самим тим и спречавања злоупотребе тих система, мрежа и података. Основни значај ове конвенције је формирање посебних државних органа који су специјализовани за борбу против сајбер криминала, при чему ће се на унутрашњем и међународном нивоу олакшати откривање, истрага и гоњење за извршена кривична дела и омогућити да се обезбеде услови за брзу и поуздану међународну сарадњу. На овај начин постигла би се хармонизација различитих законодавстава и убрзала и унапредила међународна сарадња у области сајбер криминала.

Први део Конвенције састоји се у објашњењу основних појмова, као што су: „компјутерски систем", „компјутерски подаци", „давалац услуга", и „промет података". Конвенција о високотехнолошком криминалу дефинише укупно девет кривичних дела која су разврстана у четири групе. Прву групу чине кривична дела против поверљивости, интегритета и доступности компјутерских података и система. У ту групу кривичних дела спадају: неовлашћен приступ (члан 2), неовлашћено пресретање података (члан 3), мењање садржаја, брисање или оштећење података (члан 4), ометања нормалног рада рачунара (члан 5) и производња, продаја, дистрибуције или употреба уређаја пројектованих у сврху почињења неког од претходно наведених кривичних дела (члан 6). Другу групу чине кривична дела у вези с компјутерима, а која обухвата фалсификовање које је у вези с компјутерима, и преваре које су у вези с компјутерима. Затим следи група кривичних дела која се односе на садржај. Посебан акценат и предмет регулисања члана 9. ове конвенције су кривична дела повезана с дечијом порнографијом:

„а) Производња дечије порнографије у циљу њене дистрибуције преко компјутерских система

б) нуђење или стављање на располагање дечије порнографије преко компјутерских система

ц) дистрибуција или преношењедечије порнографије преко компјутерских система

д) добављање дечје порнографије преко компјутерских система за себе или за друга лица

е) поседовање дечје порнографије у компјутерском систему или на медијимаза смештање компјутерских података."

Четврти део су кривична дела која се односе на кршење ауторских и њима сличних права.

Поред наведеног прописивања кривичних дела која би свака држава потписница требало да предвиди у свом законодавству, Конвенција даје инструкције и у погледу других инструмената материјалног кривичног права. На пример, у члану 11. прописано је: „Свака држава чланица треба да усвоји такве легислативне и остале неопходне мере да би се у њеном националном праву као кривично дело оквалификовало намерно помагање или подстрекивање на извршење неког преступа дефинисаних конвенцијом, са намером да се такав приступ учини." Осим тога, у члану 12. указује се на обавезу држава потписница да се регулише и одговорност правних лица за кривична дела прописана конвенцијом, а која учини физичко лице које има одређену функцију у правном лицу. У члану 13. наводи се да: „Свака чланица треба да усвоји такве легислативне и остале неопходне мере да би се омогућило да кривична дела установљена Конвенцијом подлежу ефикасним, пропорционалним и одвраћајућим санкцијама које обухватају и лишавање слободе."

Одредбе Конвенције процесне природе односе се на: експедитивно чување ускладиштених компјутерских података (члан 16), експедитивно чување и заштиту и делимично откривање података о преносу (члан 17), издавање наредбе за предавање компјутерских података (члан 18), претраживање и заплену ускладиштених компјутерских података (члан 19), прикупљање информација о промету података у моменту њиховог настајања (члан 20), пресретање података који се налазе у садржају електронских комуникација (члан 21), као и на питања надлежности (члан 22) за гоњење извршилаца кривичних дела која су прописана Конвенцијом.

Конвенција дефинише опште принципе на којима ће почивати међународна сарадња путем договора склопљених на бази једнаке или реципрочне легислативе, а у складу с националним правима у сврху истраге или процедура које се односе на кривичне преступе у вези с компјутерским системима и подацима, или у сврху истраге или процедура које се односе на кривичне преступе у вези с компјутерским системима и подацима, или у сврху прикупљања доказа у електронском облику. Предвиђени су и принципи који представљају основ за екстрадицију извршилаца кривичних дела (члан 24), као и принципи за пружање узајамне правне помоћи.

Од велике важности за међународну сарадњу и подизање ефикасности у откривању и прогону извршилаца кривичних дела високотехнолошког криминала је члан 35, којим се предвиђа успостављање мреже „24/7" у свим државама потписницама. Сходно томе, свака чланица треба да одреди место за контакт које ће бити доступно 24 сата дневно свих 7 дана у недељи да би омогућила моменталну помоћ у истрагама и процедурама у вези с кривичним делима која се односе на компјутерске системе и компјутерске податке, или у прикупљању доказа за кривична дела у електронском облику. Ова врста помоћи требало би непосредно да омогући давање техничких савета, чување података у складу с одредбама Конвенције, као и прикупљање доказа, давање информација правног карактера и лоцирање осумњичених лица.

До септембра 2015. године 47 држава ратификовало је Конвенцију о високотехнолошком криминалу, док је још седам држава потписало конвенцију, али је није ратификовало. Списак држава потписница Конвенције о високотехнолошком криминалу приказан је у прилогу број 1.

Сајбер криминал својим наднационалним и транснационалним карактером снажно намеће унификацију законодавних решења, и то не толико због нужности успостављања свих облика међународне сарадње, колико због чињенице да правна наука нужно мора да прати логику развоја, употребе и злоупотребе информационих технологија које по својој егзактној, математичкој природи бинарног кода не допуштају различит приступ и разумевање у зависности од расе, културе или друштвено-политичког уређења. Списак правних прописа који регулишу област сајбер криминала приказан је у прилогу број 2.

3.4.2.1 Правна регулатива сајбер криминала у Немачкој

Немачко законодавство је у великој мери усаглашено с релевантном европском легислативом. Немачка је потписала Конвенцију о високотехнолошком криминалу 23. 11. 2001. године и она је ступила на снагу 01. 07. 2009. године. Корпус модерног кривичног права у вези са сајбер криминалом у Немачкој чине следећи правни извори: Закон о спречавању привредног криминалитета (*zweites Gesetz zur Bakampfung der*

Wirtschaftskriminalitat), Кривични законик и Закон о ауторском делу, Закон о заштити података, Закон о малолетницима и Закон о телекомуникацијама.[167]

Кривичним закоником у немачко законодавство уведена су следећа кривична дела:

1. крађа података (члан 202а);
2. рачунарска превара (члан 263а);
3. рачунарско фалсификовање (члан 269);
4. неовлашћено мењање података (члан 303а);
5. ометање рада рачунара (члан 303б).[168]

Рачунарска превара регулисана у члану 263. може се састојати од утицања на резултате процеса обраде података због неправилне конфигурације, употребе нетачне или непотпуне информације, неовлашћеног коришћење података или другог неовлашћеног утицаја на ток обраде. Изменама и допунама Кривичног законика из 2007. године хакинг је регулисан чланом 202. и представља тежњу прилагођавању немачког кривичног законодавства Конвенцији о високотехнолошком криминалу. За разлику од многих земаља, немачко кривично законодавство није експлицитно санкционисало кривична дела самог неовлашћеног приступа рачунарском систему и његовом неовлашћеном коришћењу. Овај недостатак отклоњен је помоћу богате тридесетогодишње праксу судова, која је екстензивним тумачењем наведених законских одредби обухватила и те врсте деликата. У члановима 106. и 108. Закона о ауторском делу регулисана је заштита ауторског права на рачунарским програмима.

3.4.2.2 Правна регулатива сајбер криминала у Аустрији

Све до 1987. године аустријско кривично законодавство није садржало посебне одредбе у погледу рачунарског криминалитета. Године 1985. предложена је допуна у смеру

[167] Више о томе: Weisser, B., *Cyber Crime – The Information Society and Related Crimes Section*, 2, Special Part National Report on Germany, University of Muenster, http://www.penal.org/sites/default/files/files/RM-8.pdf, последњи пут приступили 12.04.2016.године.

[168] Више о томе: *GERMAN CRIMINAL CODE Criminal Code in the version promulgated on 13 November 1998*, „Federal Law Gazette" [„Bundesgesetzblatt"], I, p. 3322, last amended by Article 1 of the Law of 24 September 2013, „Federal Law Gazette", I, p. 3671 and with the text of Article 6 (18) of the Law of 10 October 2013, „Federal Law Gazette", I, p. 3799, http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p1710, последњи пут приступили 12.04.2016.године.

да се у аустријски Кривични закон (*StrafGesetzburg*, StGB) уведу нова кривична дела: оштећење сачуваних података, рачунарска превара, рачунарско фалсификовање, крађа рачунарског времена, чињења недоступним сачуваних података. Предлог је делимично прихваћен, тако да су у коначну trafGesetzburg-a, која је ступила на снагу 1988. године, унета само кривична дела оштећење података (члан 126а) и преварне злоупотребе обраде података (члан 148а). Аустријско кривично законодавство определило се да на случајеве крађе или оштећења техничке основе хардвера примени постојеће инкриминације (члан 127 – крађа, члан 126 – тешко оштећење података) и у том сегменту увело је нову инкриминацију – оштећење података (члан 126а).[169] Кривично дело преварне злоупотребе обраде података из члана 148а. обухвата рачунарску превару и фалсификовање путем програма, уноса, брисања или измене података, као и свако друго деловање којим се утиче на ток обраде података.[170] Узимајући у обзир одредбе Конвенције о високотехнолошком криминалу, те усвојивши одговарајуће смернице, попут *E/Commerce Directive* 2000/31/EC, аустријски правни систем редовно санкционише појавне облике рачунарског криминала.

3.4.2.3 Правна регулатива сајбер криминала у Француској

Француска такође припада континенталном правном поретку, чије је кривично законодавство концентрисано око писаног законика који је донело представничко тело. Измене Кривичног закона бр. 2004-575 од 21. јуна 2004. године, које су ступиле на снагу 23. јуна 2004. године заједно с ратификованом Конвенцијом Савета Европе о сајбер криминалу (10. јануара 2006. године), чине основну правну регулативу из области сајбер криминала.

Француски *Code Penale* садржи сва кривична дела која је Конвенција о високотехнолошком криминалу предвидела:

1. неовлашћено прибављање података (рачунарска шпијунажа члан 182);
2. кривично дело неовлашћеног приступа (члан 323, ст. 1);
3. кривично дело мењања садржаја, брисања или оштећења података (члан 323, ст. 2);
4. кривично дело ометања нормалног рада рачунара (члан 323, ст. 2);

[169] Више о томе: Матијашевић, Ј., *Кривичноправна регулатива рачунарског криминала*, Универзитет привредна академија у Новом Саду, Нови Сад, 2013, стр. 192. и 193.

[170] Више о томе: *Regulation of criminal activities on the Internet in Austria (November, 25th, 2002),* http://www.juridicum.su.se/iri/masterIT/vls/rep/it-crime/Austria.htm, последњи пут приступили 12.04.2016.године.

5. кривична дела преваре и рачунарског фалсификовања (члан 323, ст. 3).[171]

3.4.2.4 Правна регулатива сајбер криминала у Великој Британији

Велика Британија је све до 1990. године била пример земље која је решавала питања из подручја рачунарског криминала путем постојећих прописа. То су били: 1) *Theft Act* (1968), 2) *Forgery and Counterfeiting Act* (1981), као и 3) *Data Protection Act* (1984). Постојао је и пропис о заштити ауторског права, као и сродних права, тзв. *Copyright, Design and Patents Act* (1988). Рапидна еволуција технологије и сајбер бизниса условила је доношење следећих аката: *Privacy and Electronic Regulations* (2003), *EC directive, The Police and Justice Act* (2006) и *The Serious Crime Act* (2007).

Copmuter Misuse Act из 1990. године је у кривично законодавство увео конкретна кривична дела рачунарског криминалитета.[172] С обзиром на то да је овај акт један од старијих прописа у овој области, садржи само три инкриминације. Међутим, њима су покривени бројни компјутерски деликти. Та кривична дела су следећа:

1) основно кривично дело хакинга (*Basic Hacking Offence* – члан 1).Ово кривично дело обухвата мењање или брисање података, њихово копирање или премештање, коришћење или исписивање с рачунара на којем се налазе на било коју локацију;

2) квалификовано хакерско дело (*Ulterior Hacking Offence* – члан 2).Ово дело надовезује се на претходно. Сам члан 2. примењивања санкције условаљава чињењем кривичог дела из члана 1, а с намером да се изврши или олакша извршење неког кривичног дела за које постоји законом тачно утврђена казна (превара, фалсификовање, изнуда итд.) и небитно је хоће ли се то ново дело извршити у исто време кад и дело из члана 1;

3) неовлашћено модификовање компјутерског садржаја (члан 3).Ово дело обухвата и било који вид онемогућавања или отежавања коришћења података, програма или рачунарског система, а може обухватити и санкционисати и деловање малициозних програма, рачунарских превара и саботажа.

Ови напади су они који могу узроковати губитак живота, тешке телесне повреде, социјалне поремећаје или оштећења привреде, животне средине или могу угрозити националну безбедност. Потребна је „значајна карика у Великој Британији" – тако и

[171] Више о томе: http://www.cybercrimelaw.net/France.html, последњи пут приступили 12.04.2016.године.

[172] Више о томе: Драгичевић, Д., *Компјутерски криминалитет и информацијски сустави*, Информатор, Загреб, 1999, стр. 160.

оптужени или циљни рачунар у вријеме извршења кривичног дела или узрок штете морају да буду у Великој Британији, а оптужени мора имати намеру да изазове озбиљну штету. Уједињено Краљевство је држава са *common law* правним системом, попут Сједињених Америчких Држава и других држава Комонвелта. Конкретна примена ових прописа зависи од судова који их примењују. Судови у *common law* системима имају улогу креатора, њихове одлуке су битан извор права. Иако је реч о држави битно различите правне традиције од наше, законодавство и пракса британског правосуђа ипак представљају значајан извор за компаративну анализу.

3.4.2.5 Правна регулатива сајбер криминала у САД

Будући да је интернет настао на тлу САД, а узимајући у обзир и чињеницу да најмоћније светске IT корпорације имају своје седиште у САД (*Microsoft, Oracle, Google, Apple, IBM* итд.), логично је да САД припадају групи земаља које су најдаље отишле у вези с питањем законске регулативе рачунарског криминала. [173]

По свом унутрашњем уређењу САД су федеративна држава, где свака од савезних држава има свој поредак и сет прописа, а за међудржавне (између савезних држава) и међународне спорове (САД и нека друга држава) начелно је задужено право федерације. САД су потписник Конвенције о високотехнолошком криминалу. Што се кривичног права тиче, у федерални домен често спадају и понашања за која је законодавац сматрао да су превише битна да би била препуштена системима савезних држава. Таква понашања санкционисана су на два начина, уврштавањем у Општи кривични законик (*Federal Criminal Code*, који је део јединственог законика – "*United States Code*") или доношењем новог закона (нпр., Закон о пристојности у комуникацији из 1995. године, *Communications Decency Act*, Закон о унутрашњој безбедности из 2002. године – *Homeland Security Act* и др.).

У општем кривичном законику, у члану 1030. (глава 18, део 1, поглавље 47 Федералног законика) санкционисано је кривично дело превара и сличне активности у вези с

[173] Николић, К., Гвозденовић, Р., Радуловић, С., Милосављевић, А., Јерковић, Р., Живковић, В., Живановић, С., Рељановић, М., Алексић, И., *Сузбијање високотехнолошког криминала*, Удружење јавних тужилаца и заменика јавних тужилаца Србије, Београд, 2010, стр. 151.

рачунаром. [174] Поред ове врсте преваре, у законику су регулисане и следеће преварне делатности:

– неправедне или преварне радње или праксе (члан 45);

– лажни огласи (члан 52);

– преваре с кредитним картицама (члан 1644);

– преваре у вези с идентификационим документима и информацијама (члан 1028);

– преваре у вези с приступним уређајима (члан 1029);

– превара у вези с компјутерима (члан 1030);

– поштанске и банкарске преваре (члан 1341);

– прање новца (чланови1956. и 1957).[175]

У члану 1362. (глава 18, део 1, поглавље 65 Федералног законика) санкционисано је кривично дело ометања нормалног функционисања система (државне управе) –комуникационе линије, станице и системи.[176] У члану 2511. (глава 18, део 1, поглавље 199 Федералног законика) санкционисано је кривично дело неовлашћеног прибављања података: , Пресретање и обелодањивање неовлашћено прибављених податакастечених путем класичне, усмерене или електронске комуникације."[177]У члану 2701. (глава 18, део 1, поглавље 121 Федералног законика) санкционисано је кривично дело неовлашћеног приступа: неовлашћени приступ сачуваним комуникацијама. [178]

Поред општег кривичног законика, потребно је истаћи и два веома битна законска текста из ове области, а то су: Закон о превари и злоупотреби помоћу рачунара, из 1986. године – *Computer Fraud and Abuse Act* и Закон о контролисању агресивног и нежељеног рекламирања и порнографије, из 2003. године – *Controlling the Assault of Non-Solicited*

[174] U. S. Code § 1030 – Fraud and related activity in connection with computers, https://www.law.cornell.edu/uscode/text/18/1030, последњи пут приступили 12.04.2016.године.

[175] U. S. FEDERAL CYBERCRIME LAWS, http://digitalenterprise.org/governance/us_code.html, последњи пут приступили 12.04.2016.године.

[176] U. S. Code § 1362 – Communication lines, stations or systems, https://www.law.cornell.edu/uscode/text/18/1362, последњи пут приступили 12.04.2016.године.

[177] U. S. Code § 2511 – Interception and disclosure of wire, oral, or electronic communications prohibited, https://www.law.cornell.edu/uscode/text/18/2511, последњи пут приступили 12.04.2016.године.

[178] U. S. Code § 2701 – Unlawful access to stored communications,

https://www.law.cornell.edu/uscode/text/18/2701, последњи пут приступили 12.04.2016.године.

Pornografhy and Marketing Act – CAN-SPAM Act. Треба споменути да је у кривичном законодавству САД заступљена и заштита права приватности у сфери рачунарског криминала у виду Закона о заштити приватности за време електронске комуникације, из 1986. године – *Electronic Communication Privacy Act*. Напредак информационих технологија мора да праи адекватна законска регулатива. У Сједињеним Америчким Државама и судска пракса и законодавство су до сада били значајни извори података и искуства, и то не само за *common law* правне системе већ и за остале правне системе.

3.4.2.6 Правна регулатива сајбер криминала у Јапану

Јапан спада у државе највише угрожене сајбер криминалом. Према Токијском Националном институту за информисање и комуникационе технологије, забележено је 12,8 милијарди сајбер напада у 2013. години, највише икада у историји те земље.[179] Јапански парламент ратификовао је Конвенцију о високотехнолошком криминалу. За ову област најзначајнији прописи су Кривични законик, који је претрпео измене и допуне ратификацијом наведене конвенције, као и нови закон о неовлашћеном приступу из 1999. године – *Unautorized Computer Access Law*.

Кривични законик садржи следеће инкриминације:

1. кривично дело мењања садржаја, брисања или оштећења података – оштећење приватних података (члан 259);
2. кривично дело мењања садржаја, брисања или оштећења података – оштећење јавних података (члан 258);
3. кривично дело фалсификовања (члан 161, ст. 2);
4. кривично дело преваре (члан 246, ст. 2);
5. кривично дело мешања у пословну трансакцију путем рачунара (члан 234, ст. 2).

Закон о неовлашћеном приступу, из 1999. године, обухватао је кривично дело неовлашћеног приступа (члан 3) и кривично дело омогућавања неовлашћеног приступа (члан 4). Прописана дела обухватају и ширење и коришћење малициозних програма, као и одавање информација које могу омогућити неовлашћен приступ.

[179] *CYBERCRIME IN ASIA: A CHANGING REGULATORY ENVIRONMENT*, http://asia.marsh.com/Portals/59/Documents/Cybercrime%20in%20Asia%20-%20A%20Changing%20Regulatory%20Environment_EN.pdf, последњи пут приступили 12.04.2016.године.

Заштите ауторског и сродних права – *Copyright Law*. – Оно што је овде посебно интересантно, уз стандардан ниво заштите који се пружа свим ауторским и другим заштићеним делима, јесте члан 120а, који предвиђа новчану казну у износу од милион јена или казну затвора до једне године за сваког ко поседује, изнајмљује или продаје уређаје чија је главна сврха заобилажење техничких метода којима су ауторска и друга дела заштићена.

3.4.2.7 Правна регулатива сајбер криминала у Кини

Последњих година Кина је усвојила неколико прописа и управних мера којима је циљ забранити нападе на рачунарске система, неправилну употребу рачунара и коришћење интернета да би се починила кривична дела из области рачунарског криминала. Главни законски текст је Кривични законик – *Criminal Code*, који садржи одредбе о кажњавању повреда повезаних с рачунарском сигурношћу, у члану 2/85. одређује кривично дело неовлашћеног приступа заштићеним рачунарима.[180] Године 1994. усвојен је Закон о заштитити рачунарских информационих система (*Regulations on Safeguarding Computer Information Systems*) који садржи кривична дела повезана с рачунарским системима и мрежама, али и нека специфична кривична дела искључиво су повезана с кинеским политичким системом, попут повреде обавезе пријаве и регистрације међународно умрежених система. Три године касније, 1997, усвојен је нови пропис Закон о заштити рачунарских мрежа и интернет безбедности (*Computer Information Network and Internet Security Protection and Management Regulations*), који је обухватао нова кривична дела, својствена кинеском систему: искривљивања истине и ширење гласина ради поткопавања државног поретка, угрожавања рапутације државних органа, као и коришћење мрежа и мрежних ресурса без одговрајуће дозволе. Овај пропис увео је и кривична дела предвиђена Конвенцијом о високотехнолошком криминалу: стварање и ширење вируса и онемогућавање исправног рада рачунара и рачунарских мрежа, као и брисање, оштећење и мењање података.[181] Закон под називом Административне мере у циљу превенције и контроле рачунарских вируса – *Measures for Administration of Prevention and Control of Computer Viruses*, донет 2000. године, установио је одговорност државних органа за предузимање мера

[180] Више о томе: http://www.cybercrimelaw.net/China.html, последњи пут приступили 12.04.2016.године.

[181] Више о томе: *Reporting and Policing Internet Crimes in China*, http://www.hg.org/article.asp?id=22958, последњи пут приступили 12.04.2016.године.

против ширења вируса, и могућност да запослени у државним органима буду кажњени за непредузимање мера које унапређују рачунарску сигурност.

3.4.2.8 Правна регулатива сајбер криминала у Бразилу

С обзиром на то да је општа стопа криминала у Бразилу врло висока, не чуди много што постоје и организоване криминалне групе које се баве рачунарским криминалом. Управо је бразилско подземље једно од најнапреднијих. Разлог за такву ситуацију је спој неодговарајућег правног оквира и недовољно опремљене и увежбане полиције и истражних органа. Бразилски закони не садрже одредбе у складу с Конвенцијом о високотехнолошком криминалу, а једини закон који делимично покрива нека кривична дела из ове области јесте Закон бр. 9983 из 2000. године, који садржи кривична дела неовлашћене промене и оштећења података и информационих система. Иако бразилска пракса садржи случајеве када су за кривична дела учињена путем интернета одређена и затворске казне, реч је углавном била о кривичним делима превара. Постоји 40 додатних закона који се односе на борбу против сајбер криминала, а који чекају одобрење у бразилском конгресу.

3.4.2.9 Правна регулатива сајбер криминала у Шведској

Кривична дела рачунарског криминала су у шведском кривичноправном систему садржана у Кривичном закону. Поглавље 4 Кривичног закона садржи кривична дела: 1) неовлашћено прибављање података (рачунарска шпијунажа), 2) неовлашћен приступ подацима или рачунарском систему, 3) мењање садржаја, брисање или оштећење података. Поглавља 12 и 13 Кривичног закона садрже класичне кривичноправне одредбе о делима против имовине и кривичноправној одговорности за штету. То се посебно односи на поглавље 13, које садржи кривична дела против државе и добробити грађана. Одредбе се могу применити и на оштећење и уништење телефонске/радио-станице и друге телекомуникацијске инфраструктуре, па тако и на учиниоце кривичних дела онемогућавања правилног функционисања рачунарских система. У уводном делу истакнуто је да је Шведска једна од ретких држава која је у својим законодавним решењима отишла и даље од стандарда који су Конвенцијом о високотехнолошком криминалу успостављени. Намера законодавства је да нова кривична дела подведе под постојеће законске одредбе, што се, према упоредним анализама, цени као економичнији, али не тако квалитетан метод као што је усвајање нових

прописа који ће регулисати одређену материју, или издвајање нових одредаба у посебне одељке постојећег законодавства.

3.4.2.10 Правна регулатива сајбер криминала у Доминиканској Републици

У Доминиканској Републици је 23. априла 2007. године донет посебан закон против високотехнолошког криминала, и то после годину дана израде нацрта и 2 године чекања да га Конгрес потврди.[182] Иначе, прва хакинг истрага у овој држави била је 2003. године. Овај закон регулише следећа кривична дела: незаконит приступ (члан 6), незаконито пресретање (члан 9), ометање података (члан 10), ометање система (члан 11), злоупотреба уређаја (члан 8), фалсификовање употребом рачунара (члан 18), дечију порнографију (члан 24), кршење ауторских права (члан 25) и одговорост правних лица (члан 60). Закон против високотехнолошког криминала Доминиканске Републике посветио је чланове 13, 14, 15. и 16. регулисању кривичног дела преваре употребом рачунара. Важећи законик о кривичном поступку допуњује Закон против високотехнолошког криминала Доминиканске Републике тако што садржи одредбе о чувању рачунарских података у рачунарском саобраћају (члан 53), откривању рачунарских података у рачунарском саобраћају (члан 56), налогу за предају рачунарских података (члан 54) и надлежности органа (члан 65).

3.4.2.11 Правна регулатива сајбер криминала у Индонезији

Индонезија није потписница Конвенције о високотехнолошком криминалу. Најважнији законски прописи који регулишу област високотехнолошког криминала у Индонезији су Закон о телекомуникацијама (*UU Telekomunikasi* No. 36/1999) и Закон о информацијама и електронским трансакцијама (*Information and Electronic Transaction Act UU ITE* No. 11/2008).[183] У Закону о информацијама и електронским трансакцијама регулисана су кривична дела незаконит приступ (члан 30), незаконито пресретање (члан 31), ометање података (члан 32), ометање система (члан 33), злоупотреба уређаја (члан 34),

[182] Више о томе: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900 0016802 f259a, последњи пут приступили 12.04.2016.године.

[183] Више о томе: Setiadi, F., *An Overview of the Development Indonesia National Cyber Security*, „International Journal of Information Technology & Computer Science" (IJITCS, ISSN No: 2091–1610), vol. 6: Issue on November/December, 2012. p. 108., 109.

фалсификовање употребом рачунара (члан 35), превара употребом рачунара (члан 36), дечија порнографија (члан 27). Овај закон садржи и процесне одредбе повезане с чувањем рачунарских података (члан 43, ст. 3), откривањем рачунарских података (члан 43, ст. 4), као и с налогом за предају рачунарских података (члан 43, ст. 3).

3.4.2.12 Правна регулатива сајбер криминала у Малезији

Малезија је област сајбер криминала регулисала бројним правним актима: *Communications and Multimedia Act*, 1998, *Computer Crimes Act*, 1997, *Copyright Act* (*Amendment*), 1997, *Digital Signature Act*, 1997, *Electronic Commerce Act*, 2006, *Electronic Government Activities Act*, 2007, *Payment Systems Act*, 2003, *Personal Data Protection Act*, 2010, *Telemedicine Act*, 1997, *Penal Code* (*including Chapter on terrorism & cyber-terrorism*), *Communications and Multimedia Content Code*.[184] Закон о компјутерском криминалу, који је есенцијалан у овој области, донет је 1997. године, а ступио је на снагу 1. јуна 2000. године. Тај закон чине 3 дела: Уводни део, Прекршаји, Опште и помоћне одредбе. У другом делу се правно регулишу следећи прекршаји: неовлашћен приступ рачунарском материјалу, неовлашћен приступ с намером да се почини или олакша извршење другог кривичног дела, неовлашћена модификација садржаја било ког рачунара. [185]

3.4.2.13 Правна регулатива сајбер криминала у Португалији

Материју сајбер права у Португалији чине Закон о рачунарском криминалу и Кривични закон. Закон о рачунарском криминалу 109/91 од 17. августа 1991. године спроводи *Препоруку* Р 89 (9) Савета Европе и регулише кривична дела у вези с рачунарима и кривичним делима на интернету: фалсификовање употребом рачунара, оштећења, преваре,

[184] Више о томе: *Cyber Law in Malaysia*, http://malaysiancyberwarriors.blogspot.rs/2013/03/introduction-of-cyber-law-acts-in.html, последњи пут приступили 12.04.2016.године.

[185] Више о томе: LAWS OF MALAYSIA REPRINT Act 563 COMPUTER CRIMES ACT 1997 Incorporating all amendments up to 1 January 2006 PUBLISHED BY THE COMMISSIONER OF LAW REVISION, MALAYSIA UNDER THE AUTHORITY OF THE REVISION OF LAWS ACT 1968 IN COLLABORATION WITH PERCETAKAN NASIONAL MALAYSIA BHD 2006, http://www.agc.gov.my/Akta/Vol.%2012/Act%20563.pdf, последњи пут приступили 12.04.2016.године.

илегалне приступе, илегална пресретања и кршења ауторских права.[186] У овом закону одређује се и одговорност правних лица за вршење наведених кривичних дела.

3.4.2.14 Правна регулатива сајбер криминала у Русији

Русија није потписница Конвенције о високотехнолошком криминалу. Материја високотехнолошког криминала регулисана је у поглављу 28. „Компьютерные информационные преступления" Кривичног законика Руске Федерације. Незаконит приступ регулисан је чланом 272. Кривичног законика Руске Федерације: „Неовлашћени приступ заштићеним информацијама у рачунару, њиховим системима или мрежама које је резултирало брисањем, блокирањем или копирањем рачунарских информација, нарушавајући рад електронских рачунара, њихових система или мреже биће санкционисано новчаном казном од двеста до пет стотина износа минималне плате, плате осуђене особе или других прихода у року од два месеца до пет месеци, друштвено корисним радом у трајању од шест месеци до једне године, или казном затвора у трајању до две године."[187] У истом члану у 2. ставу одређује се да, ако је ово кривично дело извршила група лица по претходном договору, организована група, или лице које има приступ и електронским рачунарима, њиховим системима или мрежи злоупотребљавајући свој службени положај биће кажњени новчаном казном од пет стотина до осам стотина износа минималне зараде осуђене особе или неког другог прихода у року од пет до осам месеци, друштвено корисним радом у року од једне до две године, притвором у року од три до шест месеци или казном затвора у трајању до пет година.

У Кривичном законику Руске Федерације регулисани су производња, коришћење и ширење штетних електронских компјутерских програма: „Производња електронских компјутерских програма или увођење промена у постојеће програме које је резултирало брисањем, блокирањем, модификовањем или копирањем информација, нарушавајући рад електронских рачунара, њихових система или мрежа и коришћење или ширење тих програма казниће се казном затвора до три године, новчаном казном од двеста до пет стотина износа минималне зараде или плате осуђеног лица или неког другог прихода у року од два до пет

[186] CYBERWELLNESS PROFILE PORTUGUESE REPUBLIC, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Portugal.pdf, последњи пут приступили 12.04.2016.године.

[187] *Уголовный кодекс РФ*, http://www.uk-rf.com/, последњи пут приступили 12.04.2016.године.

месеци."[188] У колико је извршење наведеног облика високотехнолошког криминала изазвало тешке последице, казниће се казном затвора од три до седам година (члан 273, ст. 2).

Повреде електронског рачунарског система или мрежних оперативних правила регулисане су на следећи начин: „Лице које има приступ електронским рачунарима, њиховим системима или мрежи, а направило је повреду електронског рачунарског система, или мрежних оперативних правила, што је опет узроковало брисање, блокирање или мењање поверљивих информација и изазвало знатну штету, биће санкционисано укидањем посебног положаја или привилегија у року до 5 година, друштвено корисним радом у року од сто осамдесет до две стотине сати или ограничењем слободе у трајању до две године."[189] Ако је то дело изазвало тешке последице, казниће се казном затвора до четри године (члан 274, ст. 2).

3.4.2.15 Правна регулатива сајбер криминала у Републици Словенији

Првим реформама из 1995. године, када је донет нови закон о ауторском праву, почео је процес усвајања кривичноправних стандарда у кажњавању појавних облика рачунарског криминала. Појавни облици рачунарског криминалитета у законодавству Републике Словеније концентрисани су у Казненом законику. [190] Кривична дела, која се базирају на злоупотреби рачунара, рачунарске технологије, информационих система или мрежа, или имају додирних тачака с тим, регулисана су у оквиру више поглавља Казненог законика. У оквиру групе кривичних дела против људских права и слобода законодавац је предвидео кривично дело злоупотреба личних података (члан 143). У оквиру групе кривичних дела против имовине законодавац је предвидео кривично дело напад на информациони систем (члан 221). У оквиру групе кривичних дела против привреде, кривично дело из области рачунарског криминала је упад у пословни информациони систем (члан 237).

Последњом променом Закона о ауторском праву из 2004. године Словенија је увела још строже мере у циљу даљег смањења стопе пиратерије. Доношењем потребних прописа и њиховим адекватним примењивањем у пракси Република Словенија испунила је све захтеве Конвенције о високотехнолошком криминалу.

---

[188] *Уголовный кодекс РФ*, http://www.uk-rf.com/, члан 273, став 1, последњи пут приступили 12.04.2016.године.

189 *Угловный окодекс РФ*, http://www.uk-rf.com/, члан 274, став 1, последњи пут приступили 12.04.2016.године.

[190] *Kазнени законик* (КЗ-1), „Урадни лист Републике Словеније", шт. 55/2008, issn 1318-0576, година XVII.

3.4.2.16 Правна регулатива сајбер криминала у Републици Хрватској

Кривична дела у вези с рачунарским криминалом у законодавству Републике Хрватске регулисана су у Казненом закону.[191] Кривична дела која се базирају на злоупотреби рачунара, рачунарских технологија, информационих система или мрежа или имају додирних тачака с тим, као и у Законику Републике Словеније, регулисана су у оквиру више поглавља. У оквиру групе кривичних дела против полне слободе и полног морала, законодавац је предвидео кривично дело дечја порнографија на рачунарском систему или мрежи (члан 197а). У групи кривичних дела против имовине налазе се следећа кривича дела: 1) повреда тајности, целовитости и доступности рачунарских података, програма или система (члан 223), 2) рачунарско фалсификовање (члан 2223а) и 3) рачунарска превара (члан 224а). Улагање напора да се кривичноправна законска решења ускладе с одредбама Конвенције о високотехнолошком криминалу јасно представља могућности злоупотребе рачунарске технологије у различитим виталним сферама друштва и издваја Републику Хрватску у круг земаља које су одлучне у супротстављању овој врсти криминала.

Можемо закључити да су анализирана законодавства других држава начиниле неке кораке ка успостављању регулативе у области сајбер криминала, која и ако није задовољавајућа представља добар почетни корак. Многе државе би требале да се угледају на наведене државе било ратификацијом Конвенције о сајбер криминалу, или увођењем одредби о сајбер криминала у домаће законодавство, како подручје сајбер простора не би био полигон за некажњено вршење сајбер криминала.

[191] *Казнени закон*, „Народне новине Републике Хрватске”, бр. 110/97, 27/98, 50/00, 129/00, 51/01, 111/031, 190/03, 105/04, 71/06, 110/07, 152/08.

4. НАЧИН ИЗВРШЕЊА ПРЕВАРЕ КАО МОДЕЛА ОСТВАРИВАЊА САЈБЕР КРИМИНАЛА

4.1. СОЦИЈАЛНИ ИНЖЕЊЕРИНГ

Социјални инжењеринг у ширем смислу јесте дисциплина у друштвеним наукама које се односи на напоре да се утиче на ставове и популарна друштвена понашања и управљање ресурсима, и то било владе, било медија или других група.

Социјални инжењеринг није нова појава, већ датира из времена у којима интернет и рачунари нису били ни у зачетку. Сходно наведеној дефиницији социјалног инжењеринга, први „социјални инжењер", по историчару Андресу Региани (Andres Regiani) , био је грчки филозоф Аристотел, који је тада усмерио и научио Александра Великог да примени социјални инжењеринг, помоћу ког је постигао успешна освајања и друштвене реформе, уз континуирано спровођење египатске идеологије.[192] Године 1894. немачки индустријалац Jacques van Marken (1845–1906) први пут је употребио назив „социјални инжењер" приказујући идеју о томе да страни послодавци ангажују „друштвене инжењере" да би се ефикасније утицало на људске ресурсе, попут техничке експертизе повезане с производном машинеријом.[193] Две године касније социолог Едвин Ерап (Edwin L. Earp) у свом делу *Друштвени инжењер* анализирао је друштвене односе и уочио потребу за стручњацима који ће управљати друштвом помоћу важних информација и техника манипулисања. Први примери таквог типа управљања јавили су се уско и то у вези с остваривањем ауторитативне власти Јозефа Гебелса Josepha Goebbels-a, који је помоћу техника манипулисања управљао народом[194].

Можемо рећи да је пандан социјалног инжењеринга – политички инжењеринг као уметност изградње, пројектовања датог друштва заснованог на утврђеним принципима психологије имајући на уму да одлучивање може да утиче на безбедност и опстанак

[192] Више о томе: W. H. G. Armytage, *A social history of engineering*, University of California, , 1961,p. 25.

[193] Више о томе: MARKEN, Jacob Cornelis van, https://socialhistory.org/bwsa/biografie/marken, последњи пут приступили 12.04.2016.године.

[194] Више о томе: *Društveni inženjering – Stoljeće medijske manipulacije čovječanstva*,

http://blog.vecernji.hr/ratko-martinovic/drustveni-inzenjering-stoljece-medijske-manipulacije-covjecanstva-3948, последњи пут приступили 12.04.2016.године.

милијарде људи. Присталица политичког инжењеринга, немачки социолог Фердинанд Тонис (Ferdinand Tonnies) у својој студији истицао је да друштво не може више да функционише користећи превазиђене методе социјалног управљања. Решење је видео у политичком инжењерингу као ,,средству за постизање интелигентног управљања државним ресурсима с највишим нивоом слободе, просперитета и среће у оквиру популације"[195]. Као вид социјалног инжењеринга ("*piecemeal social engineering*") који ће донети благодат друштву постоји демократски друштвени инжењеринг. Разлика између демократског друштвеног инжењеринга (*democratic social engineering*) и утопијског социјалног инжињеринга (*Utopian social engineering*) описана је на следећи начин: „То је разлика између разумног начина да се побољша маса људи, и метода који може лако да узрокује неподношљиво повећање људске патње. То је разлика између методе која се може применити у било ком тренутку и методе чије залагање може лако постати средство одлагања акције до неког каснијег датума, када су повољнији услови. То је такође разлика између начина да се побољша ситуација која је до сада била веома успешна, у било ком тренутку, и на сваком месту, и методе која је, где год да је покушана, узроковала употребу насиља."[196]

У области информационо-комуникацијских система социјални инжењеринг је врста напада на компјутерске системе са циљем навођења особа да испуне захтеве нападача. Ту се првенствено ради о начину прикупљања података до којих нападач легалним путем не би могао да дође, при чему се не искоришћавају пропусти имплементација операционих система, протокола и апликација, већ се напад усмерава на људски фактор. Човек који приступа мрежи представља потенцијалну рањивост информационих система. Социјални инжењеринзи користе ову најслабију тачку безбедносног система информационих технологија тако што своје нападе усмеравају на природну тежњу људи ка сарадњи, добронамерности и индивидуалној несигурности, а ради добијања специфичних информација. Дакле, социјални инжењеринг у сајбер простору представља сакупљање личних података различитим савременим техникама са циљем манипуисања префињеним акцијама прикупљања и давања (продавања) информација.

Социјални инжењеринг се дефинише као нетехнички хакинг: ,,Социјални инжињеринг је ништа друго него добијање информација преваром, под изговором, крађом

[195]Више о томе: Tönnies, F., *The Present Problems of Social Structure*, „The American Journal of Sociology", vol. 10, 1905, no. 5, p. 569–688.

[196] Више о томе: Popper, K., *The Open Society and Its Enemies*, vol. I, „The Spell of Plato" ,1945.,p 23

идентитета користећи за то позната имена особа или чак лажног представљања на интернету и имена веб страница, потом искоришћавања тих података за продају или куповину, или пак понуду трећим особама.” [197]

Социјални инжењеринг представља основно средство сајбер криминалаца при извршењу сајбер превара. Без коришћења информатичких техника, и то превасходно малициозних програма, ова техника базира се на комуникацији са жртвом. Преваранти путем социјалног инжењеринга покушавају да придобију поверење жртве, а када то остваре, жртве убеђене у валидност приче превараната крше безбедносне норме или процедуре, и одају информације за приступ мрежи или систему. Преваранти се служе овом техником, јер није потребно пробијати корисникову сигурносну заштиту, користити рањивости његовог софтвера и сл. Дакле, овде је присутан тзв. ефекат лептира, тј. Одлука, чак и она најмања, може имати огромне последице. Без обзира на циљ употребе социјалног инжењеринга, који може да буде новац, крађа идентитета, или увид у приватну преписку између запослених у компанији, све почиње наизглед безазлено.

Социјални инжењери користе одвраћање од систематичног размишљања које се у психологији објашњава овако: „[...] при систематичном обрађивању, пажљиво и рационално размишљамо о захтеву пре него што донесемо одлуку. Када информације обрађујемо хеуристички, правимо менталне пречице у доношењу одлука. На пример, у таквој ситуацији могли бисмо одговорити на захтев узимајући у обзир то како се подносилац захтева представља, а не осетљивост информација које је он затражио. Трудимо се да радимо у режиму систематичног размишљања када нам је та ствар битна. Међутим, кратко време за доношење одлуке, ометеност или јаке емоције могу нас пребацити на хеуристичко размишљање.”[198]

Преваранти употребљавају различите методе којима приморавају жртве да изађу из систематичног режима знајући да ће људи у хеуристичком режиму ретко посегнути за својим психичким одбрамбеним механизмима. Мања је вероватноћа да ће бити сумњичави, постављати питања или приговарати. Преваранти теже да жртвама прију док су у хеуристичком режиму и да их у том режиму задрже. Могућа тактика је контактирање жртве

[197] Бабић В., *Компјутерски криминал*, Рабић, Сарајево, 2009, стр. 139.

[198] Више о томе: Kevin D. Mitnik, Vilijam L. Sajmon, Умеће провале, Микро књига, Београд, 2005, стр. 251.

пет минута пре краја радног времена. Нападач рачуна на то да ће нестрпљење због скорог одласка с посла навести жрву да испуни захтев који би иначе одбила.[199]

Све методе социјалног инжењеринга засноване су на специфичним особинама људског одлучивања, познатим као когнитивне пристрасности. Предрасуде, које се понекад називају „грешке у људском хардверу", с тим да циклус омбане обухвата следеће фазе: истраживање о жртви преваре, развијање добрих односа и поверења – употреба интерних информација, лажно представљање, молба за помоћ или позивање на ауторитет, злоупотреба поверења – тражење информација или услуга од жртве и употреба информација.

Друштвене мреже најчешће су место за извршење социјалног инжињеринга где преваранти налазе и контактирају жртву. Захваљујући друштвеним мрежама преваранти могу да сакупљају податке о лицу чији идентитет преузимају, као и о жртви коју су одабрали. Друштвене мреже попут Facebook-a или Twitter-a јесу непресушан извор вредних информација у извршењу сајбер превара. Разлог томе је то што се људи слободније понашају на друштвеним мрежама него у реалном свету, не проверавају идентитет својих наводних виртуалних пријатеља, те спремно откривају детаље из свог живота које нападач лако може да злоупотреби за своје намере. Потенцијалне жртве су пре експанзије друштвених мрежа тражене у старијим облицима друштвених заједница, као, на пример: theGlobe.com 1994. године, GeoCities.com 1994. године и Tripod.com, 1995. године, које су укључивале игрице за више играча на мрежи, блогове, групе за вести, мејлинг листе и причаонице (engl. *chat rooms*). Све то створило је окосницу нових модерних интерактивних друштвених медија који омогућавају корисницима стварање властитих веб-страница, тема, група, фото-галерија и онлајн пријатеља (који не морају обавезно да буду пријатељи у реалном животу), уз висок степен међусобне повезаности свих елемената друштвене мреже и бригу за самостално одређивање степена приватности сваког појединца. Ове друштвене заједнице фокусиране су на спајање људи и охрабривања корисника да деле информације и идеје путем личних интернет страница. Ово је постало лако-за-коришће алаткама за објављивање (*easy-to-use publishing tools*) и бесплатним интернет простором. Друштвена мрежа Classmates.com је зачетник спајања људи путем адреса њихових електронских пошти. Неколико година касније кориснички профили постају централна карактеристика друштвених мрежа, омогућавају корисницима стварање списка пријатеља и тражења корисника са сличним интересовањима и њихово организовање по групама у којима ће износити своје ставове. Годину 2002.

[199] Више о томе: Kevin D. Mitnik, Vilijam. L. Sajmon, Умеће провале, Микро књига, Београд, 2005, стр. 251.

обележио је процват друштвених мрежа с појавом Friendster.com, који је преовлађајући правац интернета (*mainstream of Internet*). Спокео (енгл. *Spokeo*) као претраживач за повезивање људи, који користи податке скупљене агрегацијом, један је од најчешће коришћених сајтова за проналажење жртве сајбер превара. Сајт садржи информације као што су старост, статус везе, имућност, информације о ближим члановима породице, као и адресе људи. Те информације сакупљене су помоћу података који већ постоје на интернету или у другим јавним евиденцијама. Трендови се из дана у дан мењају, а с њима и популарност одређене друштвене мреже варира. Главна предност друштвених мрежа је размена листе контаката једног корисника с другим корисницима те друштвене мреже. На тај начин остварује се сајбер социјализација на друштвеним мрежама, која је оријентисана или на пословни карактер, налажење старих пријатеља или је глобалног карактера, намењена дружењу и забави. Можемо закључити да је за велики успех дрштвених мрежа заслужна непресушна људска потреба за комуникацијом, контактом и социјализацијом, па макар само у виртуелном облику. Друштвене мреже, пак, имају и своје негативне стране и представљају идеално место за извршења свих облика сајбер криминала. Уочавајући негативне стране које друштвене мреже носе, поједине државе су их цензурисале. Пример можемо наћи у Кини, која је цензурисала Youtube и Facebook, али је својим веб-корисницима понудила замену у виду локалних мрежа, попут Youkou-a (кинеска верзија Youtube-a) и QQ (комбинација Skype-a и Facebook-a).[200] Осим у Кини, Фејсбук је цензурисан и следећим државама: Северна Кореја, Иран, Куба, Египат, Сирија, Пакистан и Вијетнам.[201]

Лака мета социјалних инжењера су асоцијалне лаковерне особе које у сајбер свету траже бег од реалности. Жеља за доказивањем, прихваћеношћу и представљањем у бољем светлу жртве нагони да се не придржавају опција заштита приватности, па личне информације чине доступним: име, презиме, датум рођења, град и државу пребивалишта, образовање, радно место и друге битне информације. Откривање наизглед небитних информација на друштвеним мрежама, које се чине не толико битним и сасвим безазленим, може да буде од велике користи сајбер преварантима. И када корисник сакрије личне информације, листа корисникових пријатеља може одати важне информације попут: похађане средње школе и факултета, главног предмета на студијама (смера), родног града,

[200]Више о томе: https://en.wikipedia.org/wiki/Websites_blocked_in_mainland_China, последњи пут приступили 12.04.2016.године.

[201] Више о томе: https://www.indexoncensorship.org/2014/02/10-countries-facebook-banned/, последњи пут приступили 12.04.2016.године.

године дипломирања и чак и информације о студенстком дому у ком су можда живели. Истраживање које су спровели стручњаци с Max Planck Institute for Software Systems у оквиру Northeastern University показала је да се само 5% људи сетило да заштити листу пријатеља. Што се тиче осталих корисника, 58% објавило је који су универзитет похађали, 42% је приказивало радно место, 35% интересовања и 19% омогућило је јавни приступ информацији о свом пребивалишту.[202] Када имају информације на основу којих могу сазнати о каквом профилу жртве се ради, преваранти без већих проблема могу смишљати тактике обмане. Уз то, недостатак редовног ажурирања оперативног система, антивирусног решења и осталих програма на рачунару даје сајбер преварантима „одрешене руке" за коришћење слабости софтвера које открију на систему у процесу сајбер превара.

4.1.1 Елементи социјалног инжењеринга

Социјални инжењеринг, који се користи за остваривање сајбер превара, обухвата:
– лажно представљање;
– стварање одговарајуће ситуације као предуслова за напад;
– наговарање и
– коришћење људских слабости попут радозналости или похлепе жртве.

4.1.2 Лажно представљање

Успостављање кредибилитета је први корак у већини напада лажним представљањем, оно је темељ онога што следи. Обмањивач испољава неколико начина понашања повезаних с улогом коју је преузео. Улога може да буде IT техничар, клијент, нови запослени или друга особа која ће одговарати датој ситуацији. Психолози ову методу објашњавају на следећи начин: „Обмањивач користи технике убеђивања које и ми свакодневно користимо. Прихватамо улоге. Трудимо се да изградимо поверење. Рачунамо на узајамно помагање. Али, у лажном представљању те технике се користе за манипулисање, обмањивање. Обмањивач се њима служи изузетно неетички, често са разорним последицама." [203] Ову технику, стару хиљадама година, преваранти су искористили за продор у добро заштићене системе и ван сајбер простора.

[202] Више о томе: *On Facebook, You Are Who You Know*, http://www.psmag.com/books-and-culture/on-facebook-you-are-who-you-know-10385, последњи пут приступили 12.04.2016.године.

[203] Више о томе: Kevin D. Mitnik, Vilijam. L. Sajmon, Умеће провале Микро књига, Београд, 2005, стр. 237.

Pretexting, познат у Великој Британији као *blagging* или *bohoing*, вид је социјалног инжењеринга у ком се злоупотребљава ауторитет који неко лице ужива (нпр., сарадници, полиција, банке, порески органи, истражитељи осигурања). У неким случајевима све што је потребно је глас који звучи ауторитативно, способност убеђивања и поседовање информација о жртви. За прикупљање информација нападачи обилато користе интернет мрежу, која пружа лак приступ детаљним информацијама о директорима компанија (име, број телефона, позиција у компанији, изводи из трговинских и привредних регистара, финансијски биланс, ажурирани статуси за компаније, записници са састанака и сл.). На мрежи се могу наћи и додатне информације, као што је лого компаније, њена организациона структура, информације о запосленима, чак и изјаве председника компаније. Да би се боље упознали са свим детаљима битним за ту компанију, информације, које нису доступне и јавно публиковане, криминалне групе купују од професионалаца који се баве индустријском шпијунажом или директно од запослених који пристају на одавање поверљивих података уз надокнаду. Након информисања о фирми и лицу чији идентитет узима, преварант контактира финансијског директора неке компаније и покушава да га убеди да изврши уплату на страни банковни рачун, што се правда гаранцијом за инвестирања, предстојећом пореском ревизијом или јавним тендером. Том приликом објашњава да уплате морају да остану потпуно тајне и поверљиве и да ће са жртвом бити у контакту адвокатска канцеларија да би им пружила потребне информације. Упркос многим камапањама и едукацијама које компаније предузимају за подизање свести, криминалне групе константно се прилагођавају и мењају иницијални модус операнди, те стварају нове сценарије за нападе. Осим што се представља као руководилац, сајбер криминалац се представља и као пословни партнер компаније која је жртва преваре. Преваранти контактирају одељење за рачуноводство или менаџера компаније путем електронске поште и обавештавају га да је промењен банковни рачун за промет или услуге које треба да се плате и да убудуће трансфер новца мора да се изврши на други рачун пословног партнера, који се налази у иностранству, а не у држави где се до тада вршило плаћање. Том приликом криминалне групе путем електронске поште достављају податке о новом банковном рачуну користећи исти лого, стил и фонт писања које користи компанија чији идентитет је украден. Уколико се користи електронска пошта за доставу информација о новом банковном рачуну, криминалне групе креирају електронски налог веома сличан налогу компромитоване компаније.

4.1.3 Стварање одговарајуће ситуације као предуслова за напад

Међу различитим методима који се користе за навођење једне особе да изврши одређену радњу у корист неке друге особе, основни метод своди се на формулисање директног и личног захтева – молбе. Иако овај метод, по правилу, има низак процент успешности, он је најједноставнији и директан: жртва тачно зна шта се од ње тражи. Сложенији приступ укључује потенцијалну жртву у добро осмишљен сценарио. У присуству наизглед објективних разлога и морално прихватљиве мотивације, имајући на располагању више елемената у односу на једноставну молбу, нападач повећава шансе да се циљана особа понаша по његовој жељи. Коришћење таквог приступа изискује бољу припремљеност агресора. Он готово увек мора добро да познаје жртву и околности у којима се она налази, тј. контекст ситуације у којој напада.

Фингирана ситуација мора се заснивати на реалистичним елементима, тако да се степен неистине смањи на минимум. Уколико се одређени практични аспекти на прави начин уклопе у осмишљени сценарио, повећава се и могућност успеха нападача:

1. жртва мора да буде убеђена да одговорност за извршену радњу неће пасти искључиво на њу (тзв. начело поделе одговорности);
2. жртва може да буде убеђена да ће, уколико поступи по захтеву, моћи да оствари неки вид личне користи (на пример, да напредује у послу);
3. жртва може да буде убеђена да је њена морална обавеза да поступи по захтеву, тј. да ће уследити осећање гриже савести уколико не поступи тако.

Пример социјалног инжењеринга када сајбер преварант ствара одговарајућу ситуацију као предуслов за напад је метод *Quid pro quo* – нешто за нешто (енг. *something for something*). Ова превара има следећи сценарио: нападач контактира компанију тврдећи да је из техничке подршке и обавештавајући о постојању проблема за који ће му жртва бити захвална ако га отклони. Нападач ће „помоћи" жртви да реши проблем и током тог процеса инсталираће вирус или ће украсти поверљиве информације с рачунара жртве. Овде се користи психолошки отпор приликом одузимања права избора. Ту негативну реакцију преваранти покрећу обавештењем да жртва неко време неће моћи да приступа датотекама на рачунару и навођењем периода који је потпуно неприхватљив. Када жртва почне да се понаша емотивно, нападач нуди помоћ да се датотеке брже врате, само му требају корисничко име и лозинка жртве. Жртва, којој је лакнуло што постоји начин да се избегне губитак, обично радо испуњава захтев. На тај начин жртве су довлачене на веб-презентацију на којој се могу

украсти њихове информације за пријављивање или подаци о кредитној картици. Сајбер преваранти искористили су ту технику 2013. године када се догодио пораст посебних превара са „СЕПА" трансферима (*Single Euro Payments Area*) и када су компаније, јавна администрација и банкарски сектор одлучили да успоставе „СЕПА" стандард да би ускладили електронске уплате унутар земаља евре зоне. У пробном периоду преваранти су преузели идентитете запослених у оштећеним банкама и контактирали су рачуновође компанија уз изговор да ће их током обавезног преласка у „СЕПА" систем контактирати техничари ради обављања тестова. Поступајући по примљеним инструкцијама, рачуновође су се конектовале на своје веб-сајтове и преузимале су наменску апликацију која омогућава даљинску конекцију с другим веб-сајтом.

Други облик је када преварант жртвама у телефонском разговору тврди да је из IT-подршке, да је интернет провајдер или из техничке подршке *Microsoft*-а. Преварант објашњава да су примећена чудна понашања рачунара, да је инфициран рачунар позиваног лица и да, на пример, шаље спам електронску пошту, поводом чега је техничка подршка добила инструкције да истраже случај. Да би жртву лишили сваке сумње, преваранти се служе различитим техничким изразима и фразама, као и захтевом за провером да ли на рачунару постоје одређени фајлови. Када жртва лоцира тражене фајлове, преварант ће их окарактерисати као заражене иако су то, у ствари, фајлови који су уобичајени за нормално функционисање рачунара (на пример, разне врсте драјвера). Након „установљавања" зараженост компјутера следи убеђивање да се купи безбедносни софтвер, њихових умова дело, који је заправо штетан вирус или најчешће да дозволе да се даљински приступи „зараженом" рачунару ради поправке.

Сајбер-криминалци такође користе поруке типа: „Кликните на линк или ће вам налог бити блокиран", „Уколико не пошаљете СМС на овај број у наредних 10 минута након што будете прочитали овај е-маил, ваш налог биће обрисан". Те претње и застрашивања играју на карту страха и брзоплетости. Под притиском хитности жртва неће имати у виду да ниједан провајдер неће блокирати налог на такав начин, нити ће тражити да се кликне на линк у мејлу да би се оставили лични подаци. По правилу, ниједан легитиман сервис неће пожуривати и захтевати да се нешто уради наврат-нанос. Без размишљања и одлагања жртве испуњавају захтеве превараната и упадају у њихову клопку.

4.1.4 Наговарање

Лично убеђивање жртве неопходно је за успех напада социјалног инжењеринга. Жртва не сме да се осети присиљеном да реализује директиву нападача, већ њена перцепција ситуације треба да поприми перспективу „добре воље и ваљаних чинова". Иако се жртвом управља, неопходно је да она мисли да има потпуну контролу над ситуацијом. Битно је, дакле, да жртва верује да је самостално донела одлуку да жртвује део свог времена и енергије у алтруистичке сврхе или за остваривање конкретних бенефиција.

Обмањивачи често користе чињеницу да ће се радије потврдно одговорити захтевима које постављају симпатични и допадљиви људи. Људима се допадају сличне особе, оне које имају слична интересовања у каријери, образовању и хобије. Обмањивачи своју допадљивост могу повећати и додавањем комплимената и ласкањем, а физички привлачни нападачи могу искористити своју атрактивност да би се више допали жртви. На тај начин утицање на његову може наивну жртву преобразити у помагача. Када особа прихвати ту улогу, тешко јој је и нелагодно да се из ње извуче. Лукав обмањивач покушава да предвиди у којој ће се улози жртва добро осећати. Људи радо прихватају улоге које су позитивне и због којих се после осећају добро.

Да би наговорили жртву, преваранти се не устручавају да користе многобројне алатке, као што су: техничка средства која им омогућују анонимну комуникацију, веб-базирана електронска пошта, електронски налози претходно преузети од правих корисника, факс-машине за слање факс-порука при размени документације са жртвама преваре, услуге телекомуникационих сервиса за директну комуникацију са жртвом преваре (са жртвама кривичних дела извршиоци комуницирају и путем мобилних телефона, када користе припејд SIM картице, које лако могу да баце и потом купе нове ради даље комуникације), лажне странице на интернету којима оштећене доводе у заблуду да комуницирају и сарађују с представницима легалних и легитимних институција, фалсификована докумената с лажним печатима, потписима, лажном садржином да би преузели новац који им је оштећени уплатио, бежични трансфери новца за пренос противправно стечених новчаних средстава, фотографије других лица које су прикупили с интернета да би се лажно представили оштећенима приликом уговарања пословних састанка.

4.1.5 Коришћење људских слабости

Свака обмана и тактика коју користе сајбер преваранти усмерена је на људске слабости. Похлепа је сигурна карта за остваривање замисли сајбер превараната. Ретко која људска природа је имуна на лако стечен новац, добитак на лутрији или сличне могућности добијања новца без труда. Све те преваре осмишљене су на исти начин, темеље се на принципу „уложите мали износ новца да би сте стекли милионе". Такође је примамљива понуда набавка лекова, реплике дизајнерских производа и других производа по нереално ниским ценама. И у сајбер свету, као и у стварном животу, свакоме се понекад може десити да поступи ирационално. Од свих особина, радозналост је слаба тачка многих интернет корисника.

Први примери социјалног инжењеринга заснованог на радозналости жртава је изазивање или *Baiting*. У том нападу нападач оставља дискете, CD ROM, или USB *flash drive* заражен вирусом тамо где ће их жртва сигурно наћи (купатило, лифт, тротоар, паркинг, хол циљане компаније) и која ће их, у жељи да открије њихов садржај, спојити с рачунаром. Тада корисник несвесно инсталира тројанца, што омогућава нападачу неометан приступ рачунару жртве и унутрашње рачунарске мреже циљане компаније.

Изгледа невероватно, али људи понекад преварантима шаљу новац из радозналости. Чак и ако не разумеју у потпуности шта пише у мејлу, и заправо не очекују да ће добити стотине хиљада или милионе долара, понекад су само радознали и желе да знају шта би се могло десити уколико би кликнули на линк. Facebook корисници из чисте радозналости пристају на анкете, дељења и лајковања веб-сајтова да би гледали снимке, као и на инсталацију ажурирања која је услов за преглед видеа, а што је метод извршења сајбер превара ма колико безазлено деловало. Ова људска слабост била је кључни фактор успеха популарне преваре на Фејсбуку која се односила на обећање корисницима да ће моћи да виде ко им гледа профил. Наводно, Фејсбукова „официјелна" апликација нудила је приказ профила корисника који најчешће посећују дати профил. Апликација "*Profile Viewers*" само је била маска за *Trojan.JS.Carfekab*, који, осим што шпијунира *browsere* жртава, има могућност да шаље поруке у име зараженог корисника, као и да шаље приватне податке жртава на сервере превараната. [204]

[204]Више о томе: *Najuspešnije Facebook prevare u 2014*,. http://www.informacija.rs/Drustvene-mreze/Najuspesnije-Facebook-prevare-u-2014.html, последњи пут приступили 12.04.2016.године.

Све популарнији мамци које користе преваранти јесу видео-снимци ужасних призора, као што су мучења животиња, деце и жена. То није изненађење с обзиром на то да су нека истраживања открила да се током последњих 30 година емпатија код деце драстично смањила, док се толеранција према насиљу значајно повећала. Видео-снимак жене коју је убио муж коришћен је за инфицирање рачунара корисника *adwareom-a* и *malverom*-а. Слика одсецања главе Азијаткиње заинтригирао је хиљаде корисника Фејсбука да погледају лажни видео-снимак жене коју је муж убио због пољупца с другим мушкарцем. Иза обећање да ће видети голишаве видео-снимке својих пријатеља с друштвене мреже, а уз лажно инсталирање *Adobe Flash Player*-а, крио се *Trojan.FakeFlash*. Највећи број тих инфекција забележен је у Великој Британији, Италији, Француској, Немачкој и Румунији.[205]

Исти је случај и са смешним видео-снимцима пријатеља са Фејсбука. Након клика на видео корисници би доспели на лажну YouTube страницу, која би их преусмеравала на малициозни фајл *Flash Player.exe*. Уместо смеха и забаве, жртве су биле забринуте јер је тројанац преузео велике количине података из њихових меморија.Преваре с лажним компромитујућим видео-снимцима неке познате личности никада не јењавају. Преваранти користе скандал са цурењем голишавих фотографија и снимке познатих. И ова превара је иза себе оставила инфициране рачунаре оних које је радозналост натерала да кликну на малициозне линкове. Пошто би кликнули на линк, од корисника је тражено да надограде свој *Flash Player* да би погледали обећани видео. Фајл који су жртве преузимале крио је тројанце *Trojan.JS.Facebook.A* и *Trojan.Afent.BFQZ* који мењају конфигурацију *browser*-а и онемогућавају приступ жртвама списку екстензија, активностима на Facebook-у и подешавањима налога.

Најзаслужнији за популаризацију социјалног инжењеринга у сајбер простору је несумњиво Кевин Митник (*Kevin Mitnick*). Он је најпознатији осуђени хакер због упада у велике рачунарске системе Мотороле, Фуџија, Нокије и Сан мајкросистемса. Интересатан детаљ је то да Митникова стручност спада пре у домен манипулације (*social engineering*) него у способност рада на рачунарима. Социјални инжењеринг је касније постао његов примарни метод добијања информација.

[205] Више о томе: *Da li postoji tipičan psihološki profil žrtve Facebook prevara?*,

http://surfujbezbedno.com/zanimljivosti/da-li-postoji-tipican-psiholoski-profil-zrtve-facebook-prevara/, последњи пут приступили 12.04.2016.године.

Митник је заступао теорију да је лакше обманути особу која има кључне информације, и добити их од ње, него провалити у комплексни рачунарски систем у ком су смештене. Уз популаризацију рачунара и интернета, као и ширење канала комуникације, лични подаци постали су много доступнији, а могућности социјалних инжињера све веће. Кевин Митник одлучио је да своје умеће подели са широким масама да би младим хакерима пренео своје искуство, а ширу популацију упозорио чега да се чувају приликом крстарења интернетом. Уједно, он је писац који је на најсвеобухватнији начин описао социјални инжењеринг. Он је између осталог обелоданио технике којим се користе социјални инжењеринзи и који су сигурни знаци који упозоравају на могући напад, а то су:

„– неко одбија да вам каже број на који га можете позвати
– необичан захтев
– наглашавање високог положаја
– наглашавање хитности случаја
– претња негативним последицама у случају одбијања сарадње
– нелагодни разговор при испитивању
– спомињање познатих особа
– дељење комплимената или ласкање
– флертовање."[206]

Допринос Кристофера Хаднагија огледа се у дефинисању физичких и психичких принципа социјалног инжењеринга у његовим делима *Social Engineering: The Art of Human Hacking, Unmasking the Social Engineer: The Human Element of Security* и бројним чланцима који се базирају на сигурности која се стиче едукацијом (*a free online SE resource*). Он је креатор *DEFCON Social Engineer Capture the Flag and the Social Engineer CTF for Kids*.

Познати социјални инжењери су и браћа Ramy, Muzher и Shadde Badir. Иако слепи од рођења, тај хендикеп их није омео да успоставе велику телефонску и рачунарску превару у Израелу 1990. године користећи социјални инжењеринг, гласовно лажно представљање и *Braille-display computers*.

[206] Више о томе: Kevin D. Mitnik, Vilijam. L. Sajmon, *Уметност обмане: утицај људског фактора на безбедност*, Микро књига, Београд, 2003, стр. 335.

У области е-банкинга с правом можемо поменути JB Snyder, главног консултанта за *Bancsec, Inc.* и познатог социјални инжињера. Његов успех представљају упади у више од 50 америчких банака, а који су окарактерисани као „најефикаснији социјални инжењерски напади у историји". Ти напади пре свега се заснивају на коришћењу електронске поште и лажном представљању, а самим тим и малој вероватноћи откривања и након тога санкционисања.

Пит Херцог (*Pete Herzog*) је неуро-хакер и признати истраживач социјалног инжењеринга који је створио прву методологију тестирања безбедности од утицаја социјалног инжењеринга за OSSTMM 2.1 у 2002. години (означен као „Процес безбедност"). До 2003. године створио је начин мерења количине поверења на квантитативан начин за OSSTMM 3 у 2010. години. У 2009. години Херцог је почео да ради са *brainwave* скенерима и tDCS ради проучавања мождане манипулације и сазнања како људи уче и усредсређују пажњу.

Комбиновањем поверења, неуро-хакинга и истраживања социјалног инжењеринга закључио је да су људи неуролошки рањиви и због тога наседају на технике манипулације. Он је представио "How We Are Broken" у SecTor у 2010. години, а касније у 2014. години побољшање свести о безбедности са *5 тајни за изградњу изузетне безбедносне културе у вашој организацији* (*5 Secrets to Building an Amazing Security Culture in Your Organization*). Користио је технику *Security Awareness Learning Tactics* (SALT) *project* да би створио свест о сигурности на основу неуро истраживања.[207] Он је такође показао да социјални инжењеринг може да се користи за попуњавање радних места за незапослене у чланку *Hacking Human Resources Is a Thing*. Херцог је применио те манипулативне технике у оквиру пројеката за подизање безбедности намењеним специјално тинејџерима.

Технике социјалног инжињеринга се свакодневно развијају, обухватају све сфере коришћења интернета, а вектори нових напада користе малициозни софтвер да би комуницирање са жртвом свели на минимум. Корисницма сајбер простора не преостаје ништа друго до најједноставнијег начина одбране од напада социјалним инжињерингом, а то је коришћење здравог разума.

[207] Више о томе: *Your favorite IT-Security Conference*, https://www.troopers.de/events/troopers15/461_the_science_of_security_awareness_building_a_better_awareness_program/, последњи пут приступили 12.04.2016.године.

4.2. УПОТРЕБА МАЛИЦИОЗНИХ ПРОГРАМА

Под злонамерним или непожељним програмом подразумева се сваки програм који може да се усели у рачунарски ситем без знања и воље корисника, а направљен је с намером да угрози рачунарски садржај или мрежу. У ту групу спадају софтвери креирани за *Windows* и *Linux* оперативне системе и *Macintosh* и *Palm* рачунаре, а који за своје ширење користе интернет, посебно имејл и *World Wide Web* (WWW).

За успешно спроведен малвер напад потребне су 3 компоненте:
– мотивисан нападач;
– недостатак одговарајуће заштите;
– погодна мета (може да буде било која особа или имовина над којима нападач жели да преузме контролу).[208]

Након инфицирања рачунарског система неауторизованим и за корисника неочекиваним процесима, малициозни софтвер користи се за:

1) нарушавање перформанси система и довођење система у нестабилно стање. Првобитни облици малициозних програма у 80-им и 90-им обично су били облик вандализма или неслане шале која се користила за онемогућавање или отежавање извођења појединих операција на рачунару. Међутим, „апетити" сајбер превараната убрзо су порасли, па су малициозне програме, осим за шалу и вандализам, искористили за стицање профита. Малициозни програм коришћен је за успостављање контроле над *dial-up* модемом и позивање скупих телефонских бројева (*premium-rate*), те корисник на крају месеца добија огроман телефонски рачун за који су заслужни преваранти;

2) неовлашћен приступ систему рачунара.

Када се успостави контрола, заражени рачунари користе се да раде за аутора малициозног софтвера. Тако се споменути рачунари користе као *proxy* за слање спам порука. То су зомби рачунари (*zombie computers*). Предност коришћења заражених рачунара за слање спам порука је анонимност коју пружају.

[208] Више о томе: Bossler, A., Holt, T., *Malware Victimization, A routine activities framework*, CRS Press, Taylor and Francis Group,Unitet States of America, 2011, стр. 320–321.

3) прикупљање информација које узрокује њихову злоупотребу и губитак приватности корисника. Користећи малвер, сајбер преваранти прикупљају све информације које су им потребне за напад, тј. превару, као што су, нпр., списак пословних партнера, бројеви рачуна, досадашње трансакције, пословна преписка, администраторске шифре овлашћених особа које обављају трансакције, корисничка имена и лозинке и др.;

4) остале злонамерне активности.

4.2.1 Класификација злонамерних малициозних програма

По критеријуму самосталности, тј. потребе за програмом у ком ће малициозан програм бити сакривен, малвере можемо поделити на:

1) оне којима је неопходан носилац, тј. програм у ком ће бити сакривени (тројански коњи, вируси) и
2) самосталне, тј. оне којима није неопходан носилац (црви, шпијунски програми).

По критеријуму могућности реплицирања, можемо направити поделу на:

1) малвере који се реплицирају (вируси, црви) и
2) малвере који се не реплицирају (тројански коњи).

Једна од најобухватнијих класификација, ако се има на уму њихово свакодневно увећавање и тежња да број малициозних програма претекне број оних легитимних, јесте класификација на:

1) заразне, чији су типични примери вирус и црв;
2) сакривене, чији су типични примери *trojan horse* и *rootkit*;
3) користољубиве – чији су типични примери *spayware*, *adware* и *dialer*.[209]

Црви и вируси су најпознатији типови малициозних софтвера. Они су карактерисани као заразни малициозни софтвери јер стварају проблеме инфицираном рачунару тако што отежавају његово функционисање. Разликују се по начину ширења: црв се шири преко мреже

[209] Више о томе: Ранђеловић, Д., Поповић, Б., *Злонамерни програми*, „Техника”, 5/2010, „Електротехника” (59), бр. 5, Београд, 2010, стр. 19–24

са циљем да зарази друге рачунаре, а вирус инфицира извршни програм, који, када се покрене, почиње да се шири и на друге програме. Уз то, вирус, да би се ширио, користи корисникову интервенцију, док црв аутоматски влада рачунаром. С обзиром на наведено, може се закључити да црви могу направити већу штету због мрежног промета који генеришу приликом ширења интернетом.

4.2.2 Црви

Црви су самостални малициозни програми који се шире путем електронске поште, *web*-а і *instant messenger*-а. Први црв који су се ширили мрежом били су намењени за *Unix* уређаје. Тадашњи *Internet Worm* појавио се 1988. године и угрожавао је SunOS і VAX BSD саставе. Електронске поруке које садрже црв обично користе технике социјалног инжењеринга да би навеле примаоца да отвори прилог. У највећем броју случајева назив и екстензија приложеног фајла дозвољавају црву да се камуфлира као неизвршни програм (фајл, на пример, има екстензију слике или филма). Поједини црви искоришћавају софтверске грешке (енгл. *bug*) најпопуларнијих програма за размену електронске поште (попут програма *Microsoft Outlook Express*), тако да се аутоматски активирају у тренутку приказивања инфициране поруке. Примери тих црва су: *Netsky*, *MyDoom* и *Sasser.a*.Сви напреднији црви фалсификују адресу пошиљаоца и на тај начин стварају непријатан колатерални ефект ширења инфицираних порука – антивирусни програми инсталирани на серверу враћају заражену поруку на адресу с које је послата, али, с обзиром на то да је лажна, заражена порука стиже неком другом, а не правом пошиљаоцу поруке електронске поште (*Mailer* и *mass-mailer*).

Црви се могу преносити путем:

• е-поште (тзв. имејл црви). Имејл црви користе методе социјалног инжињеринга да би натерали корисника да покрене програм који се налази у прилогу или да приступи хиперлинку. Поруке су често следеће садржине: „an important thing about you”, „critical windows update”, или „meet the love of your life”. Када корисник приступи предложеној вези или покрене послат програм, црв се активира. Након инфицирања рачунара црв ће своје копије послати на имејл адресе меморисаних на зараженом рачунару;

• инстант порука (IM црви). Ови црви користе сервисе за комуникацију попут *Microsoft* MSN-а, *Skype*-а, *Yahoo Messenger*-а, ICQ-а, AOL AIM-а и друге. У овом случају црв ће се ширити када корисници приступе инфицираној веб-локацији или датотеци предложеној путем порука овог типа;

• интернета. Ово је најлакши начин да се искористе рачунари који немају сигурносне програме или *firewall*, као и искоришћавање отворених портова;

• дељења датотека (*file-sharing* црви). Црв ће у овом случају тежити да се ископира у дељени фајл под именом које ће асоцирати корисника на то да се ради о услужној апликацији која је неопходна за рад рачунара;

• P2P мреже. Тада се црв копира у P2P дељени фајл. P2P мрежа након тога помаже даље ширење црва тако што информише друге кориснике о постојању новог ресурса и обезбеђује преузимање дељеног фајла.

Апсолутна звезда у свету малициозних програма је компјутерски црв *Stuxnet*, први малициозни програм направљен да нападне индустријске системе као што су електране и нуклеарни реактори. Тај црв направљен је са циљем да успорава и убрзава центрифугу, тј. шупље цеви које се окрећу великом брзином и користе се за физију изотопа У-235 у У-238, а који се налази у природном уранијуму. *Stuxnet* је откривен у јуну 2010. године када је његова мета био Иран, који је свој пројекат гасних центрифуга започео 1987. године њиховом инсталацијом у подземном постројењу *Natanz* у централном Ирану. *Stuxnet* је погодио компјутерске системе широм Ирана, укључујући и оне који нису критични за рад нуклеарних реактора. За описане координисане акције усмерене против иранског нуклеарног програма оптужене су западне земље и Израел.[210]

4.2.3 Вируси

Термин „вирус" је у информатичком смислу први употребио Фред Коен (*Fred Cohen*), студент Универзитета Јужне Калифорније, у чланку објављеном 1984. године под насловом *Експерименти с рачунарским вирусима* (*Experiments with Computer Viruses*). [211] Вирус сам по себи није програм који се аутономно инсталира, као што и његов биолошки имењак није сам по себи облик живота. Информатички вирус не користи мрежне ресурсе, већ убацује своје

[210] Више о томе: *The Real Story of Stuxnet How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program,* http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet, последњи пут приступили 12.04.2016.године.

[211] Више о томе: Cohen, F., C*omputer Viruses Theory and Experiments*, „Computers and Security", vol. 6, 1987 p. 22–35.

копије у инсталациони програм. На тај начин, када корисник активира програм, прво се неприметно активира вирус, а затим и програм.

Вирус је део сложенијег кода који се шири унутар једног рачунара или рачунарске мреже копирајући се унутар других програма или у одређеном делу хард-диска рачунара, тако да се може активирати отварањем инфицираног фајла. Након инсталирања софтвера вирус само репликацијом инфицира остале фајлове у рачунару или мрежи, и то најчешће без знања корисника. Вирус обично садржи неколико „инструкција" које се могу односити на произвођење сопствених копија и ширење епидемије. Међутим, вирус може садржати и много штетније инструкције, попут брисања или уништавања фајлова, форматизовања хард-диска, или отварања споредних врата.

Пре веће доступности интернета вируси су се ширили тако што би заразили *boot* сектор или дискету. Ти вируси били су написани за *Apple* II и *Macintosh,* али су се почели ширити с појавом IBM PC-а и MS-DOS-а.[212] Године 1981. и званично је потврђено постојање рачунарског вируса *Elk Cloner*.[213] Годину 1988. обележило је харање вируса Јерусалим, који је брисао све покренуте програме.[214] Следећу годину, осим што је обележила експанзија вируса *Datacrime,* који је био способан да изврши *low-lewel* формат нулте стазе на диску, карактерисало је и то што се први пут појавила фирма вируса у Бугарској.[215] Раније верзије вируса биле су написане да делују као шала, тј. као безопасни и досадни програми. Вируси *David* и црв *Melissa*[216], који су инфицирали укупно 20% тадашњих корисника интернета, представљали су експеримент њихових твораца, без икакве штетне намере вандализма.[217]

---

[212] Више о томе: *History of Mac malware: 1982 – 2011,* https://nakedsecurity.sophos.com/2011/10/03/mac-malware-history/

[213] Више о томе: *6 Computer Viruses That Changed The World*, http://www.makeuseof.com/tag/6-computer-viruses-changed-world/, последњи пут приступили 12.04.2016.године.

[214] Више о томе: *VB – Virus Bulletin*, https://www.virusbtn.com/pdf/magazine/1990/199003.pdf, последњи пут приступили 12.04.2016.године.

[215]Више о томе: *Computer Virus History I,* http://www.mindpride.net/root/Extras/Viruses/computer_virus_history_1.htm, последњи пут приступили 12.04.2016.године.

[216] Више о томе: *Melissa (computer virus),* https://en.wikipedia.org/wiki/Melissa_(computer_virus), последњи пут приступили 12.04.2016.године.

[217] Више о томе: *Top Ten Most Destructive Computer Viruses of All Time*, http://crunkish.com/top-ten-worst-computer-viruses/, последњи пут приступили 12.04.2016.године.

Глобално информационо-комуникациона мрежа је допринела да основни начин преношења заразе постане размена фајлова путем електронске поште, програма за комуникацију и размену фајлова међу корисницима. Тај период обележила је појава такозваних макровируса, чије су „инструкције" написане речником скриптинг-програма (енгл. *Scripting program*), као што су „MS-Word" и „Outlook". Ти вируси су посебно усмерени на инфицирање различитих верзија Мајкрософтових (*Microsoft*) програма разменом докумената. Надаље, оперативни системи Мајкрософта највише су погођени вирусима зато што су и најраспрострањенији међу такозваним нестручним корисницима. У сваком случају, чињеница је да не постоје системи који су потпуно, или теоријски имуни на вирусе, будући да анатомија интернета дозвољава рачунарским вирусима да се много ефикасније шире него раније.

С порастом популарности интернета, малициозни софтвер све више настаје због жеље за профитом, а не за шалом и деструкцијом, као што је био случај с ДОС-вирусима, који су брисали податке с диска или мењали састав фолдера записивањем неправилних података у њих. Од 2003. године већина рапидно ширећих вируса и црва дизајнирана је за преузимање контроле над рачунарима корисника намењеним за црно тржиште. Вирус може да конзумира меморију тако што се уписује на крај exe извршних фајлова који се покрену на зараженом рачунару. Величина заражених фајлова повећава се за око 1 килобајт а вирусом бива заражен и сваки други рачунара ком покрене неки од заражених фајлова.[218] Такав вирус, под називом 5lo, откривен је октобра 1992. године. [219] Вирус може да функционише као P2P програм за шеровање који с других заражених рачунара скида фајлове разне садржине, попут музике, порнографије, па чак и целих игара и, по могућности, инсталира их. Заражени рачунар такође служи као извор фајлова другим зараженим рачунарима. Пример овог вируса је *Ares.exe*,

[218] Више о томе: Пошто је једном покренут, вирус се смешта у радну меморију користећи инструкцију INT 21, AX=3521h. Сваки фајл који ће се покренути биће заражен тако што ће вирус додати свој код и поруку променљиве садржине на његов крај. Након тога вирус мења време настанка фајла на време када је заражен, а и његово поље 0Ch у заглављу фајла на FFAAh. Дужина инфицираног дела фајла креће се од 1.000 до 1.100 бајтова, а најчешћа дужина је 1.032 бајта. Где год је неки заражени фајл покренут, вирус се пребаци у радну меморију. Вирус инфицира један фајл само једном, а у меморији може постојати само једна његова инстанца.Најћешћа порука коју вирус додаје на непосредан крај фајла је: 92.05.24.5lo.2.23MZ. Друге поруке садрже се у самом вирусу. Вирус инсталиран у меморији не може се наћи помоћу MEM/C зато што се инсталира тако да га покреће сам оперативни систем. Слободна меморија се смањи за око 2 килобајта.

[219] Најпознатије верзије 5lo су *Ares.exe*, *Brontok*, *Natas*, *W32.Mytob.V@mm*, *W97M.Verlor*, *Win32.Parite*, *ZMist* и *Zenux*.

верзија црва *Gaobot.ee*[220], који битише под именом *ARES*. Постоје сумње да овај вирус скида и инсталира спајвер, друге вирусе, тројанце и црве, мада те тврдње нису никада званично доказане.

Бројни су вируси који се шире тако што сами себе шаљу на имејл адресе које пронађу на зараженом рачунару. За слање користе сопствено окружење а као пошиљаоца означавају особу са чијег рачунара се шаљу. Рачунарски вирус који на поменути начин делује је Бронток (енг. *Brontokworm*)[221], направљен у Индонезији. Када га жртва први пут покрене, копира сам себе у фајл с подацима о корисничким апликацијама. Овај вирус даје инструкције да га оперативни систем стартује заједно са свим другим апликацијама путем кључа *HKLM\Software\Microsoft\Windows\ CurrentVersion\Run* у *Windows Registry* и онемогући корисника да то измени тако што постави забрану коришћења *Windows Registry* кориснику. Своје фајове учини недоступним тако што их модификује у системске фајлове и учини их невидљивим, а потом уклони опцију *FolderOptions*. У случају појаве програма који би могао да му нашкоди, активирања МС ДОС-а или преузимања фајлова с интернета, рачунар се рестартује, што је знак инфекције овим малициозним програмом.

Вируси могу да буду наменски створени да би заразили рачунаре тајних служби. Пад мреже америчке тајне службе на 3 дана проузроковао је вирус *Natas* (од енг. *satan*, читано уназад, што значи сатана, ђаво). Овај полиморфичан вирус први пут је регистрован у Мексико Ситију маја 1994. године, када је био ширен путем заражених флопи дискова. Убрзо је постао веома проширен у Мексику и југозападном делу САД.

Вирус може да користи и сопствени SMTP механизам, помоћу ког шаље масовне имејл поруке на адресе које прикупи из фајлова на зараженом рачунару. Имејлови које шаље имају променљиве параметре за наслов (енг. *subtitle*) и прикачени фајл (енг. *attachment*). Прикачени фајл који садржи вирус може да има екстензије .bat, .cmd, .doc, .exe, .htm, .pif, .scr,

[220] *Gaobot.EE* је црв који помоћу спостеног СМТП механизама шаље бројне спам мејлове. Црв на зараженом рачунару такође отвара случајно изабран TCP порт и обавештава могуће нападаче на претходно одабраном IRC каналу, где покушава да деактивира сигурносне системе и алат за надгледање оперативног система.

[221] Друга имена под којима се овај црв појављује су: W32/Rontokbro.gen@MM, W32.Rontokbro@mm, BackDoor.Generic.1138, W32/Korbo-B, Worm/Brontok.a, Win32.Brontok.A@mm, Worm.Mytob.GH, W32/Brontok.C.worm и Win32/Brontok.E.

.tmp, .txt, или .zip. Вирус *W32.Mytob.V@mm*[222], откривен 3. априла 2005. године, има способност да искористи уобичајене сигурносне пропусте у систему да отвори себи порт преко ког ће се ширити кроз мрежу.

Постоје вируси специјализовани за инфицирање докумената Мајкрософт ворда '97 и 2000. Макровирус *W97M.Verlor*, познат као *W97M.Overlord*, покреће се затварањем зараженог документа тако што на С диску у меморији (C:\windows\) снима два фајла: tempad.dll и tempnt.dll. Сваки следећи отворени документ и новоотворени документ (бланко) инфицирају се тим фајловима.

Листа заражених вируса смешта се у фајл C:\Himem.sys. [223] Вирусова стелт-функција активира се у случају да корисник покуша да приступи *Visual Basic* едитору (Tools ->Macros ->VisualBasicEditor), чиме би вирус могао да буде откривен. Та функција мења назив корисника на *TheOverlord*, а потом у фајлу win.ini додаје линију: run = <Директоријум индоуса>\overlord.b.vbs. Потом вирус сам себе брише из главног шаблона и свих активних докумената, што онемогућава његово проналажење путем покренутог алата. По свом покретању *overlord.b.vbs* поново инфицира главни шаблон и све фајлове чија су имена записана у C:\Himem.sys. Уколико корисник покуша да приступи листи макроа (Tools ->Macros ->Macro), вирус се брише из главног шаблона и свих активних докумената пре отварања прозора. То онемогућава да се нађе у листи присутних макроа, јер по затварању радног прозора с подешавањима вирус опет инфицира све активне документе и главни шаблон.

Постоје и специјализовани вируси који инфицирају фајлове с екстензијама .exe и .scr на рачурарима који раде под оперативним системом *Microsoft Windows*. Један од њих је паразитски вирус *Win32.Parite*[224],који има три верзије, A, B и C. Прве две верзије разликују

[222] Такође је познат као Win32.Mytob.AA Computer Assoc, Net-Worm.Win32.Mytob.c [Kasper, W32/Mytob.c@MM [McAfee], W32/Mytob-C [Sophos], WORM_MYTOB.V [Trend Micro].

[223] Вирус такође за собом оставља или користи фајлове overlord.b.vbs и overlord.b.dll.

[224] Овај вирус је такође познат као W32/Pate, W32/Pinfi и PE_PARITE. Верзија вируса означава се додавањем црте или тачке пре слова ознаке, на пример, Win32.Parite.C. Вирус чине два дела. Први је мало језгро написано у асемблеру које се брине о ширењу тела вируса, а други је тело вируса написано у борландовом C++, које је од заражавања рачунара смештено у директоријуму windows\temp.

се само у садржају вредности којом се инстанцирају у *Windows Registry*, док трећа верзија има побољшан систем скривања своје инстанце.[225]

Једном овако инсталиран вирус заражава све .exe и .scr фајлове који су били и који ће бити покренути зе време његовог дејства. То резултује врло брзим ширењем вируса. Изузети су само фајлови које систем закључа пре него што се вирус учита у меморију, што аутоматски спречава било какву инфекцију. Но, таквих фајлова има изузетно мало или их уопште нема, у зависности од инсталације. Последице деловања овог вируса с повећање заражених фајлова за 200 килобајта и делимично или потпуно губљење функционалности програма.

Први вирус који користи технику познату под називом интеграција кода је *ZMist* или *Zombie.Mistfall,* ког је направио руски творац вируса познат под именом *Z0mbie*. Овај вирус подржава потпуно нову технику: интеграцију кода. *Mistfall* механизам који вирус садржи способан је да декомпајлира преносиве извршиве фајлове до њихових најмањих елемената, изискујући 32 мегабајта меморије. По овоме, *Zmist* се убацује у код тако што помера блокове кода с места где ће се убацити, након чега регенерише код укључивањем информације о направљеним померањима, и поново гради извршни фајл.

Вирусе према окружењу и методама инфекције можемо поделити на:

• *boot* сектор вируси (тј. вируси стартног записа) – нападају *Master Boot* сектор;

• паразитски – заразе извршне датотеке додавањем свог садржаја у структуру програма, при чему оне остају делимично или потпуно функционалне;

• свестрани вируси – нападају *boot* секторе и извршне програме;

• вируси пратиоци – створи .com датотеку користећи име већ постојећег .exe програма и угради у њу свој код;

• линк вируси – у трену инфицирају нападнути рачунарски систем, што може изазвати велику штету на диску;

• макровируси – који могу сами себе да копирају, бришу и да мењају документе.

[225] Пошто је на неком рачунару вирус први пут покренут, инстанцира вредност PINF у кључу HKEY_CURRENT_USER\Software\Microsoft\Windows\ CurrentVersion\ Explorer (верзије A и B) у регистру виндоуса?, копира своје тело у директоријум windows\temp. Тиме осигурава да ће увек бити покренут заједно са системом и да ће остати у његовој сенци.

Према месту у меморији, вирусе можемо поделити на:

• оне који су у притајној меморији – остају у меморији рачунара након активирања кода вируса;

• оне који нису у притајној меморији.

4.2.4 Тројански коњ

Назив овог малициозног програма настао је по познатој причи о освајању града Троје злоупотребом поверења. Свој назив ови малициозни програми оправдавају тако што користе методу лажног представљања. Наиме, они се представљају као корисни или пожељни програми, који приликом покретања заједно с намераваном фунцкијом у позадини спроводе нежељене активности без корисниковог знања. Пример су антивируси или *antispyware* програми, који се на енглеском зову *rogue* или *fake antivirus*. Корисник, када посећује интернет странице њиховог произвођача, може да се зарази њима, и то често приликом постојања сигурносних рупа у интернет претраживачу. Програми попут *Trojan-FakeAV*-а детектују измишљен малициозни софтвер на корисниковом рачунару, а потом настоје да увере корисника да ће уклонити вирусе...". Ови програми, осим што узнемире корисника и изазову његове несмотрене ракције, могу и блокирати активацију правих антивирусних и антиспајвер програма, као и инсталирати остале врсте малициозног софтвера.[226] Захваљујући програму порт скенер (*port scanner*), особа која није заслужна за инфицирање рачунара може искористити то што је одређени рачунар заражен тројанским коњем да би на тај начин могла да приступи том рачунару.

Могућности које су на располагању хакерима пошто инсталирају ову врсту малвера су велике: крађа лозинки и других осетљивих података (*password stealers* или *infostealers*), омогућавање удаљеног приступа инфицираном рачунару неовлашћеној особи (*backdoors*), инсталирање другог малициозног софтвера (*downloaders*), коришћење система као дела ботнета (нпр. за аутоматско спамирање или за ДОС нападе), рушење система, анонимно интернет сурфовање, брисање или измењивање датотека итд.

Тешко је одредити прецизну класификацију ове врсте малициозног софтвера због њиховог свакодневног јављања и унапређивања њихових могућности. Међутим, с обзиром на критеријум њихових могућности, тројанске коње можемо поделити на:

[226] Најпознатији тројански коњи ове врсте су: SpySheriff, ErrorSafe, WinAntivirus и XP Antivirus.

– Бекдор (енг. *Backdoor*)[227], што је програм који инсталирају тројански коњи (без знања власника) и који служи да трећим особама омогућава несметан и од власника неовлаштен приступ рачунару. Бекдор користи слабости оперативног или заштитних система (заштитног зида или антивирусног програма). Кад се тројанац инсталира на корисниковом систему, хакер може удаљено да му приступи и изводи разне операције. Говорило се да произвођачи рачунара прединсталирају бекдор на саставе својих купаца ради лакше техничке подршке, но то никада није поуздано доказано.[228]

Downloader је тројански коњ који обично мирује на рачунару и приступа различитим интернет страницама да би с њих скинуо обично малициозне фајлове које су на крају и покренули.

PSW (*password*) тројанац је специјализован да претражује рачунар ради откривања лозинки, кључева (приватних и јавних), сертификата и података о кредитиним картицама. Све корисне информације, које су резултат претраге PSW тројанаца, битие прослеђене његовом власнику.

Тројански шпијун (*trojan spy*) је врста тројанског коња који после инфекције рачунара мирује у меморији не приказујући своје присуство и омогућава нападачу да прати рад корисника рачунара било тако што бележи притиснуте тастере (*keylogging*), снима екране, или на неки други сличан начин. Информације до којих дође приликом праћења рада корисника, власник и управљач тројанског коња најчешће користи за уцену.

Пример је тројански коњ *Kenzero,* који погађа кориснике који нелегално с интернета преузимају *Hentai* игре за одрасле преко јапанског *file/sharing* сајта *Winni*. Када корисник покрене игру, тројански коњ маскиран као инсталациони екран тражи од корисника да унесе одређене податке, а за то време праве *screenshotove* с информацијама о последњим отвараним страницама. *Screenshotov*-и историје браузер инфицираног корисника аутоматски се објављују, а затим кориснику стиже порука, поп-ап или имејл с понудом садржине: ако

[227] Бекдор је термин који се у енглеском језику користи за врата окренута дворишној страни куће. То су врата која су најслабије заштићена и одакле провалници најлакше улазе у кућу.

[228] *TROJANS AND BACKDOORS*, http://www.webpronews.com/trojans-and-backdoors-2005-08/ , последњи пут приступили 12.04.2016.године.

корисник уплати 1.500 јена, вредност од 1.200 динара, сајт с подацима о његовим интернет навикама биће избрисани.[229] Према последњим подацима, око пет и по хиљада људи признало је да су били жртва Кензера.[230]

Тројанац обавештајац (*trojan notifiers*) свом аутору шаље информације као што су IP адресе, адресе електронске поште и стање портова (често се користи као део злонамерног софтверског пакета који обавештава аутора о успешној инсталацији црва или задњих врата тројанаца). Познат је и случај деловања тројанског коња *Topig*, који је компромитовао и украо податке за пријаву за 250.000 банковних рачуна и једнак број кредитних и дебитних картица, имејл адреса и FTP рачуна.[231]

Тројански прокси сервер (engl. *proxy server*) је тројански коњ који покушава да претвори инфицирани рачунар у прокси сервер и на тај начин омогући удаљеном кориснику да приступи интернету анонимно путем удаљеног рачунара. На тај начин инфицирани рачунар постаје тзв. Зомби (слепо слуша наредбе) и може да се искористи за слање нежељених порука (спама) или учествовање у ДОС нападу.

Иновација у развоју тројанских коња је могућност искоришћавања безбедносне рупе у старијој верзији IE-а или *Google Chrome*-а да би се инфициран рачунар користио као анонимни прокси да се ефективно прикрије коришћење интернета. Хакер на тај начин може да сурфује интернетом и погледа интернет сајт док се колачићи, ИП логови и слично налазе на рачунару домаћина.

У историји посећених страница на рачунару жртве може да се, али и не мора да се налази и списак сајтова којима је хакер који користи рачунар као *proxy* посећивао. Прва генерација таквих тројанских коња често није прикривала трагове, док новије то раде

[229] Више о томе: *Kenzero Porn Virus Publishes Web History Of Victims On The Net--Unless They Pay,* http://www.huffingtonpost.com/2010/04/16/kenzero-porn-virus-publis_n_540133.html, последњи пут приступили 12.04.2016.године.

[230] Више о томе: *5.500 hentai pirates afflicted by blackmailing malware*, http://www.geek.com/news/5500-hentai-pirates-afflicted-by-blackmailing-malware-1191821/, последњи пут приступили 12.04.2016.године.

[231] Више о томе: *250.000 Credit Cards Stolen in Wine Industry Hack*, http://svbwine.blogspot.rs/2015/07/250000-credit-cards-stolen-in-wine.html, последњи пут приступили 12.04.2016.године.

ефективније. Неколико верзија *Slavebot*-а широко се распространило у САД и Европи и највише су дистрибуирани примери ове врсте тројанаца

Легални тројански коњи су тројански коњи у служби полиције који се баве прикупљањем информација са циљем откривања кривичног дела (engl. *Remote Forensic Software*). Ово је облик шпијунирања грађана који је у неким земљама легалан и врши се по судском налогу (нпр., САД, Аустралија). Различита су становишта у вези с питањем прихватања ове методе доказивања. Већина држава одбила је ову могућност сматрајући да је легални тројански коњ у сукобу с Уставом, јер крши основна људска права, док је у неким државама у фази припреме (Немачка, Аустрија, Швајцарска)[232]. Легални тројански коњи шире се инсталацијом или актуализацијом комерцијалних оперативних система и других софтверских компоненти рачунара и пропаганде, као и путем ISP-ова инфилтрирањем у постојеће механизме преноса података, који познају такву могућност у својим производима и услугама.Тројански коњи који су однели највише жртава су: *Back Orifice, Netbus* и *SubSeven*.

Последњих година, тројански коњи постају све већа опасност корисницима приликом сурфовања интернетом због популарности ботнетова међу хакерима и приступачности оглашивачких сервиса који допуштају ауторима да крше приватност њихових корисника. Према статистикама *BitDefender*-а из 2009, 83% детектираног малициозног софтвера чинили су тројански коњи.[233] За разлику од већ наведеног софтвера, постоји и малициозан софтвер намењен крађи података (*data-stealing malware*). Како назив каже, то је софтвер који је дизајниран тако да прикупи информације и проследи их трећој страни без пристанка или знања жртве, а с намером оштећивања жртве директним коришћењем података или њиховом *underground* дистрибуцијом.

4.2.5 Малвери за крађу података- Data-stealing malware

У крадљивце података спадају: *keyloggeri*, *spyware*, *adware*, *backdoorov*-и и *botov*-и. Технике које користе ови злоћудни програми рапидно се умножавају.

[232] Више о томе: *German Government Fesses Up to Spying on Citizens With Trojan, Says It's Legal,* http://www.themarysue.com/german-gov-trojan/, последњи пут приступили 12.04.2016.године.

[233] Више о томе: *Top 10 malicious programs sent by email, Q2 2015 Most common form of malware*,http://www.guinnessworldrecords.com/world-records/most-common-form-of-malware, последњи пут приступили 12.04.2016.године.

Ова врста малициозних софтвера може се инсталирати путем *drive-by-download*-а, а интернет страница која је домаћин малициозном софтверу је неретко привремена или лажна, при чему се користи више начина енкрипције, а подаци се краду приликом декрипције.Захваљујући овим малициозним програмима, њихови творци и корисници могу стећи право богатство. Успех хакера Алберта Гонзалеза (рођ. 1981. године) огледа се у крађи путем малициозних програма и продаји више од 170 милиона бројева кредитних картица у 2006. и 2007. години. Следствено томе, то је била највећа рачунарска превара у историји. Осим појединаца оштећене су и многе фирме попут: *BJ's Wholesale Club*, TJX, DSW *Shoes*, *OfficeMax, Barnes & Noble, Boston Market, Sports Authority* и Forever 21.

Spyware је широка категорија малициозног софтвара с наменом да пресреће или преузима делимично контролу рада на компјутеру без знања или дозволе корисника. Сам назив сугерише да је реч о програмима који надгледају рад корисника. Међутим, *Spyware* означава широку палету програма који искоришћавају корисников компјутер за стицање користи за неку трећу особу или комерцијалну добит. Појам *spyware* први пут се спомиње 1995. године на *Usenet*-у у поруци која је исмевала *Microsoft* пословни модел. Реч *spyware* означавала је софтвер намењен шпијунажи или прислушкивању. Почетком 2000. године оснивач *Zone Labs*-а Gregor Freund користио је појам у прес издању за *ZoneAlarm*-ov заштитни механизам. Касније те исте године откривено је да је *Reader Rabbit*, едукативни дечји софтвер који је развила фирма *Mattel*, тајно слао податке споменутој фирми. Од тада је *spyware* поступно почео заузимати свој садашњи облик.

Углавном се тајно инсталирају на личне рачунаре да би пратили рад корисника без њиховог знања. Међутим, често се ови програми и добровољно инсталирају на јавним, дељеним или компјутерима неке фирме да би власник пратио активности корисника, тј. запослених. Није редак случај да нека особа користи *spyware* да надзире интернет активности свог партнера. Малициозни софтвер *Loverspy* посебно је дизајниран да тајно прати активности корисника тако што ће његов партнер моћи даљински да контролише рачунар жртве, укључујући ту и приступ, промену и брисање фајлова, као и укључивање камере.Други начин инфицирања је коришћење слабе заштите система, тј. недостатка антивирусне (бројне антивирусне фирме, као што су *Symantec, PC Tools, McAfee* и *Sophos* су своје антивирус програме обогатиле *antispyware* додацима) и антишпијунске заштите, тзв. *antispyware* програма (нпр., *Ad-Aware, WindowsDefender, SpywareBlaster, Spybot Search &*

Destroy, *Spyware Doctor* (*PC Tools*), *Ad-Adware SE* (*Lavasoft*) и *Spybot Search & Destroy* Патрика Кола (Patrick Kolla).

Активни корисници услуга интернета често су заражени с више облика *spyware*-а. Као последицу постојања *spyware*-а корисник зараженог компјутера може приметити чудно понашање система или значајан пад системских перформанси (брзине), што је само по себи значајан проблем. Шпијунски софтвер може да утиче на повећану активност процесора и већи промет интернета. Такође, јављају се проблеми са стабилношћу, програми се нагло руше, систем се редовно смрзава, а повремено није могуће успоставити интернет везу, или је она веома спора.

Све то може да створи утисак корисника да су узроци тих проблема лоше перформансе рачунара, проблеми с хардвером, *Windowsim*-а, или зараза неким другим малициозним софтвером. Неки корисници тешко инфицираних систем контактирају техничку подршку или купе нови компјутер зато што им је постојећи систем „постао је преспор". У већини случајева врло заражени системи изискују чисту инсталацију *Windows*-а (јер се реинсталацијом не бришу сви подаци с диска), а да би се повратиле функционалност и брзина.

У ову групу малициозних софтвера спада и *Keylogger* или *keystroke logging program*, малициозни софтвер који прати притиснуте тастере на рачунару, а користи се за крађу корисничких лозинки, бројева кредитних картица и осталих осетљивих информација које потом шаље нападачу – неауторизованом трећем лицу.

У тренутку инсталације малициозног софтвера на рачунар веома је битно да остане непримећен и недетектован, те потом уклоњен. Наведена непримећеност малициозних програма остварива је захваљујући техници руткит. Руткит као скуп алата прикрива присуство нападача тако што омогућује сакривање малициозног прграма у *Task Manager*-u (engl. *hidden process* – скривени процес) или може да спречи читање његових фајлова.

4.3. КОМБИНОВАНИ МОДЕЛ

Рапидно усавршавање технологије и информационе структуре условили су да социјални инжењеринг и малициозни програм самостално нису адекватне методе за

извршење сајбер превара. Да би се сајбер превара успешно извршила, потребно је њихово међусобно допуњавање и усклађивање.

Многе сајбер преваре техничког типа користе социјални инжењеринг да би се стекло поверење жртве, тј. да би жртва насела на лажну причу. Самостално социјални инжињеринг, пак, као метода за извршење преваре у сајбер простору може се олакшати коришћењем малициозних програма. На тај начин превара ће брже и без већих трошкова бити извршена.
Да би се малициозни програм користио, увертира мора имати елементе социјалног инжењеринга. Да би жртва преузела малициозни програм, потребно је намамити је, тј. навести на преузимање. Због тога сајбер криминалци одлучно користе мешавину раније виђених и успешних тактика социјалног инжењеринга за ширење малвера. Постоји више тактика, а малициозни програми могу да буду различити у зависности од користи која се жели имати (крађа података, шпијунажа, прекид рада система и др.). Комбиновање та два метода показало се као кључ успеха преварних радњи у сајбер простору. Примери су познте сајбер преваре у којим је немогуће рашчланити ова два метода: *Spam*, *Phishing*, *Pharming*, *Spearphishing*, *Vishing* и *Hoax*.

Комбинован модел може се извршити преузимањем малициозног софтвера, што се дешава коришћењем социјалног инжењеринга да се кликне на линк у мејлу или инстант поруци у програму за размену порука. Циљ тих превара је преузимање фајла који се може појавити у облику zip формата којим се прикрива шта у ствари корисник преузима или отварањем JAP-фајла, који користи технику *drive-by download* и представља пречицу за преузимање малвера с *Dropbox* налога нападача или компромитованог *Dropbox* налога.

4.3.1 Комбинован модел послат путем имејла

Ови напади најчешће су усмерени слањем електронске поште у којој се жртва наводи да приступи унапред припремљеном хиперлинку (URL – *UniformResourceLocator* адреса) који води до лажне веб-адресе у којој жртва оставља поверљиве информације (нпр., податке о банковним рачунима, платним картицама и др.) попуњавањем различитих образаца. Дакле, у овој превари социјални инжењеринг се најпре користи да би заинтригирао жртву да отвори електронску поруку непознатог пошиљаоца. Пажњу и заинтересованост жртве треба да покрене поље *subject*, у које пошиљалац уноси предмет поруке. Техника социјалног инжињеринга користи се ради уверавања жртве у аутентичност и легитимност интернет странице тако што ће изгледом, информацијама, фалсификовањем адресе веб-странице.

Затим следи примена малициозних програма који се огледају у зараженој интернет адреси на коју жртва приступа, поступку прикупљања унесених података и инфицирању рачунара жртве, као и преузимању контроле над њим. Дакле, овде можемо уочити да се поред техничких сегмената преваре, који обухватају примену малициозних програма, најпре користе методе манипулације које представљају прву фазу преваре која ће омогућити деловање злонамерном софтверу.

Црв *MyDomm.A* изазвао је епидемију управо зато што је користио методе друштвеног инжењеринга и поруке с „техничким" призвуком: ”*The message contains Unicode characters and has been sent as a binary attachment”*. Овај злоћудни програм користио је период кад је највећи проток поште да би се умножавао тако што би слао поруке на адресе састављене од корисничких имена и имена домена нађених на рачунару.

MyDoom генерише поруке с насловом као што је: ”*Mail TransactionFailed*”, са садржином која упућује на то да поступак није извршен: ”*Mail transaction failed*”. У атачменту мејла је датотека с називима *read me, doc, text, file*. Ако се она покрене, црв отвара *Notepad* са случајно изгенерисаним знаковима. Потом, у системски директоријум смешта се извршна датотека (*taskmon.exe*) и датотека *shimgapi.dll*, чији је циљ ослушкивање долазећих веза на TCP портовима (и на тај начин неовлашћени корисник може да убаци додатне извршне фајлове у систем и да их покрене, или да инфицирани систем употреби као *TCP proksi server*). [234] Знаци зараженост овим вирусом су чудно понашање рачунара (нпр., отварање *Notepad*-а с гомилом бесмислених карактера и модификација базе *Registry* у инфицираном рачунару). Међутим, праву штету овај вирус чини искоришћавајући даљински приступ рачунару и злоупотребом информација које на тај начин може да добије.

Преко мејла (тј. *Outlook*-а) преноси се и Мелиса, макровирус који инфицира *MS Word* документа. Жртва добија поруку следећег наслова: ”Important Message From:”, са следећим текстом: ”Here is the document you asked for...”, а у атачменту су датотека с линковима ка порнографским садржајима и макровирус. Вирус се извршава отварањем *Word* документ ако су дозвољени макрои (VBA код), чиме ће се *template MS Word*-а у сваки документ уписивати текст: ”Twenty-two points, plus triple-world-score...” Кад се инсталлира вирус, он обара ниво

[234] Више о томе: *MyDoom worm spreading fast, Sophos warns users to be wary of viral email and hacker attack*, https://www.sophos.com/ en-us/press-office/press-releases/2004/01/va_mydoom.aspx, последњи пут приступили 12.04.2016.године.

безбедности и остали макрои могу слободно да се извршавају. Чим се забране макрои, документ ће се нормално отварати.[235]

4.3.2 Комбиновани модел који се шаље путем инстант порука

За ширење малициозних програма користе се инстант поруке путем *Skype*-а, *MSN*-а или *Yahoo*-а.Један од садржаја инстант поруке је акроним „lol" и зип фајл за који жртва треба да помисли да је слика коју треба преузети. То се показало као добар мамац за кориснике да отворе фајл. Из истог разлога користе се и текстови "*omg, is this you*" или "*I can't believe someone posted this*" итд. Порукама ове садржине, које корисник добија од пријатеља, почиње ланац инфекције. Назив фајла је уобичајен за слике: IMG_xxxx.zip. С обзиром на то да поруку шаље пријатељ, мање опрезни корисници можда ће преузети зип фајл који уместо слике садржи JAR-фајл истог назива IMG_xxxx.jar. Када се JAP-фајл покрене, преузима се малвер с *Dropbox* налога. Прва два поменута фајла, зип и JAP фајлови, нису сами по себи малициозни, али трећи фајл је тројанац који се убацује у текуће процесе на систему жртве. Налог жртве на друшвеној мрежи је тада компромитован и биће искоришћен за даље ширење малвера међу пријатељима жртве.

Такође, из радозналости, а путем комбинованог модела хиљаде корисника *Facebook* -а заразили су своје рачунаре тројанцем *Fake Flash* вођени жељом да виде голишаве видео-снимке својих пријатеља на мрежи. Државе у којима је откривен највећи број инфекција овим тројанцем су Пољска, Велика Британија, Италија и Немачка. Да би избегли да буду откривени, криминалци користе стари трик: текст у објавама се мења, па су тако до сада забележени покушаји намамљивања корисника да кликну на линк са "See [Име корисника] private video", "[име корисника] приватни видео" и "XXX private video". Када знатижељни корисник кликне на линк који обећава да ће видети неког од пријатеља на Фејсбуку у разголићеном издању, преусмерава се на лажни *YouTube*, с ког треба да преузме фајл *FlashPlayer.exe* који крије тројанца. Малвер инсталира екстензију *browser*-а која даље шири ову исту превару у име жртве и краде његове/њене фотографије с *Facebook*-а. Пријатељи жртве видеће исту објаву која је привукла жртву да кликне на линк, што је уобичајено за овакву врсту превара на *Facebook*-у. Овога пута у улози мамца је сама жртва чије

[235] Више о томе: *Melissa Macro Virus*, https://www.cert.org/historical/advisories/CA-1999-04.cfm?, последњи пут приступили 12.04.2016.године.

фотографије с *Facebook*-а користи малвер да би привукао њене пријатеље. Да би се жртва натерала да преузме малициозни фајл, на лажном сајту *YouTube* приказује се следеће обавештење: "*Adobe Flash Player has crashed, please update to the latest versions*."

Сајбер криминалци се труде да све изгледа уверљивије тако да лажирају број прегледа наводног видео снимка: жртва можда ништа неће посумњати ако види да је наводно више од два милиона људи кликнуло на *YouTube* линк. Још један трик који користе криминалци да би убедили жртву да је видео-снимак прави је обавештење о ограничењу за малолетнике.[236] Сајбер криминалци прате трендове савремених технологија, па моделе превара прилагођавају њима. Објекат комбинованог метода извршења сајбер преваре, осим рачунара, сада су и мобилни телфони новије генерације с андроид системом, који имају приступ интернету. Комбинација највеће друштвене мреже *Facebook*, најпопуларнијег оперативног система за мобилне уређаје андроид и апликације за размену порука – *WhatsApp* је добитна за криминалце који покушавају да привуку пажњу корисника да би остварили своје циљеве.[237]

Корисници *Facebook*–а, који приступају сајту друштвене мреже с андроид уређаја, суочени су с мноштвом „предложених објава", тј. реклама за популарну апликацију *WhatsApp*. Социјалним инжењерингом покушавају се привући корисници тако што се нуди могућност шпијунирања разговора контаката на *WhatsApp*-у или трикови како сакрити статус на *WhatsApp*-у или блокирати некога.Ако жртва наседне на превару и кликне на неку од предложених објава, преусмерава се на лажну верзију *Google*-ове продавнице апликација *Google Play*, одакле ће, верујући да се заиста налази на *Google Play* маркету, преузети апликацију која је бесплатна или која ће коштати онолико колико коштају услуге премијум СМС-сервиса на који се тројанац претплаћује без знања жртве. У зараженом мобилном телефону тројанац проверава све долазне поруке на уређају и, ако је пошиљалац премијум СМС сервис, порука се пресреће и брише тако да корисник никада не сазна за њу.

[236] Више о томе: *Fake Flash update installs feared banking Trojan*, http://www.nbcnews.com/technology/fake-flash-update-installs-feared-banking-trojan-1B8202115, последњи пут приступили 12.04.2016.године.

[237] Више о томе: *Facebook integrišeWhatsApp u svoju Android aplikaciju?*, http://www.informacija.rs/Mobilni-telefoni/Facebook-integrise-WhatsApp-u-svoju-Android-aplikaciju.html, последњи пут приступили 12.04.2016.године.

5 ПРОФИЛ САЈБЕР ПРЕВАРАНАТА И ПОСТУПАК ОТКРИВАЊА И ДОКАЗИВАЊА ПРЕВАРЕ КАО МОДЕЛА ОСТВАРИВАЊА САЈБЕР КРИМИНАЛА

5.1. МОТИВИ САЈБЕР ПРЕВАРАНАТА

Генерализовано, то су углавном малолетници жељни славе и знања који користе програме за обављање тих радњи да би непосредо пре самог извршења тих штетних радњи они крстарили мрежом, скенирали је и доколичарили у потрази за одговарајућом метом. Након одабира мете, употребљавајући прави алат, врше своје кажњиве радње, што изгледа једноставно када се овако опише, али је у стварности пуно знатно већи опсег радњи око припреме, планирања или извршења.

У овој категорији постоји још једна група хакера којима је главни циљ да разбију сигурносни систем.[238] Због тога они проводе сате у проучавању система обезбеђења, односно заштићених компјутерских система да би пронашли начин за рушење те заштите. Сматра се да је број ових хакера аматера релативно велики. Сам став хакера аматера илуструје њихову „наивност", у којој они, детињасто, желе да демонстрирају своју памет и виспреност упадом у одређени систем и слабости обезбеђења тог система, а истовремено да остану некажњени јер то нису радили с намером да проузрокују штету.

Не мали број међу њима су вандали који упадом у систем желе да нанесу штету, успоре систем, обришу податке, онемогуће кориснике, а и да изврше саботажу одређеног система.

Хакери-аматери имају један објекат напада или више таквих објеката, који могу да буду:

1. да пронађу довољно изазован систем и поиграју се с њим;
2. да добију приступ систему и претраже га да би задовољили знатижељу и доказивали своја знања и способности;
3. да пронађу неку нову, занимљиву игрицу у систему да би се играли;

[238] Samociuk, M., Hacking, edicija – *The Protection of Computer Software-its technology and applications*, Cambridge, Cambridge University Press, The British Computer Society, 1989, стр. 153.

4. да униште или модификују податке, убаце вирусе и вирусолике програме или да оставе неку, најчешће шаљиву поруку.[239]

Једна од најприхватљивијих је класификација хакера на следећи начин: „Неки хакери уништавају људима датотеке или целокупан садржај дискова – они су провалници или вандали. Неки хакери почетници се не труде да науче технологију, већ користе хакерске алате да би провалили у рачунарске системе – они су скрипташи. Искуснији хакери развијају хакерске програме и објављују их на вебу и у дискусионим групама. А ту су и особе које технологија не занима, већ рачунар користе само као помоћно средство за крађу новца, добра и услуга."[240]

Независно од мотива који их покрећу, реално представљају велику опасност нарочито када се упуштају у ризичне информатичке авантуре у подручјима као што су национална безбедност, индустрија наоружања, сателитска технологија и др. Начини испуњења циља су различити и разноврсни, те их је тешко открити, поготово што их има много и што један хакер аматер више пута покушава упад у систем док му покушај не успе. Занимљиво је да се они ретко враћају истом систему, тако да је и то отежавајућа околост за откривање. Једини путоказ је њихова хвалисавост, на основу које се дуготрајним и мукотрпним истрагама може понекад доћи до починиоца.

5.2. ПСИХОЛОШКИ ПРОФИЛ САЈБЕР ПРЕВАРАНАТА

Тешко је постићи прецизну слику психолошког профила сајбер преваранта с обзиром на психичка и социјална обележја превараната, као и специфичности ове врсте криминала. Одговоре који се односе на дескрипцију психолошког профила сајбер преваранта можемо наћи у криминалној феноменологији, науци која се бави проучавањем појавних облика извршених кривичних дела и социјално-индивидуалних својства извршилаца. Иако постоје различите предрасуде када су хакери у питању, на основу различитих анализа ове специфичне групације учинилаца рачунарских кривичних дела јасно је да су свим хакерима

[239] Више о томе: Дракулић, М., *Основи компјутерског права*, Друштво операционих истраживача Југославије, Београд, 1996, стр. 452.

[240] Више о томе: Mitnik, D. K., Sajmon, L. V., *Уметност обмане: утицај људског фактора на безбедност*, Микро књига, Београд, 2003, стр 3.

заједничке следеће особине: висок коефицијент интелигенције, велика радозналост и лакоћа интелектуалне апстракције. Имају повишену способност апсорпције знања и обраћају пажњу на мноштво обичним људима необичних детаља. Нису једнострани, већ се труде да буду укључени у било коју тему која изазива интелектуални напор. Хакери уживају у учењу о информационим система (компјутерским, комуникационим) и како да повећају његове могућности, насупрот већини корисника, који уче само минимум онога што је неопходно. Хакери су они који с ентузијазмом програмирају и у томе више уживају него да о њему теоретишу. Током 1994. и 1995. године код људи који се баве хакингом откривен је ADD синдром (*Attention Deficit Disorder*), који је окарактерисан као немогућност одржавања пажње комбинована с хиперфокусирањем на ствари које их занимају.

У највећем броју случаја као сајбер преваранти јављају се студенти и ђаци. Посебно треба имати у виду да су студенти развили први вирус. Неки аутори заступају став да учиниоци рачунарских кривичних дела немају развијену моралну зрелост. Код млађих починилаца сајбер криминала бављење противправним активностима узрокује њихова зависност од интернета. Већ су 1995. године формулисани изрази *Addiction Disorder* (IAD) и *Patologycal Internet Usage* (PIU), чији су индикатори потреба за повећањем времена проведеног на интернету ради постизања осећаја задовољства и немогућност контроле времена које се проводи на интернету, као и апстиненцијална криза, која наступа након неколико дана без интернета или при покушају да се смањи или прекине коришћење интернета. Услед ове појаве, пак, јавља се повлачења у себе када се није на интернету, асоцијално понашање, које одликује запостављање социјалних, друштвених, рекреационих и других обавеза у корист интернета. Ту је употреба интернета замена за решавање материјалних, породичних и професионалних проблема. На тај начин редукује се осећај кривице, страха, беспомоћности и ниже вредности. Ту појаву прати и лаж као средство обмањивања о времену коришћења интернета. Лажу се блиске особе о времену које се проводи у коришћењу интернета.

Теорија није усвојила општеприхваћену дефиницију зависности од интернета. То се може објаснити тиме што зависност од интернета по начину свог испољавања делимично одговара болестима зависности, а делимично поремећајима који подразумевају губитак контроле импулса. Интернет зависност не може се операционализовати дужином времена које појединац проводи у овој активности. Уколико је везаност за интернет деструктивна и изазива поремећаје породичног, социјалног, професионалног функционисања може се констатовати постојање зависности од интернета. Особе зависне од интернета уочавају

потешкоће у свакодневном животу које им се јављају као последица немогућности контролисања употребе интернета.Бројни корисници интернета показује знаке овог поремећаја, који се испољава играњем онлајн игара, онлајн шопингом, коришћењем мејла, четова или различитих мејлинг листи. Чак су и судови у првим пресудама познатим хакерима признавали зависност као олакшавајућу околност и у оквиру пресуде налагали су одређене терапије за одвикавање од зависности. Тим ставовима иде у прилог и чињеница да је финансијска корист коју су први хакери имали од својих активности занемарљива у односу на оно што би својом даровитошћу могли легално да зараде.

Хакери имају своју специфичну културу, по којој су препознатљиви. Иако према њима не треба имати предрасуде, јасно је да свака култура, па и хакерска, има у своје особене карактеристике у вези с питањем начина комуникације, међусобних односа припадника, понашања, навика итд. Хакерска култура почиње да се развија почетком 60-их година прошлог века. После 1969. године стопила се с технолошком културом у коју су спадали зачетници интернета. Временом су се у њу стапале све културе повезане с развојем технологије и рачунара, па је од 1990. године хакерска култура скоро изједначена с оним што се зове „покрет отвореног кода" (*Open Source Movement*).[241] Централни стубови хакерске културе на којима се она развија су: интернет, *World Wide Web*, *GNU project*, *Linux* оперативни систем и све хакерске креације. Од 1990-их година па до данас хакерска култура добија још неке препознатљиве симболе: *Tux, the Linux penquin*, *the BSD Daemon, Perl Camel*, као и хакерски амблем.

Хакери су развили и свој специфичан начин комуникације, што представља још једну њихову особеност. С обзиром на то да су много бољи у писаном изражавању него у живој интерперсоналој комуникацији, временом је усвојен *leet speak* који представља шифровану форму писања замењивањем слова бројевима, симболима и другим знаковима који личе на њих. Основна улога овог начина комуникације јесте да искључи странца из комуникације, односно да се јасно успостави разлика између језика ове групације лица и језика већине. Овај говор не треба мешати са тзв. AOL језиком који се среће на интернету, а чија је функција да скрати писање неких речи, док је код литспика основни циљ да учини традиоционални језик неразумљивим за неупућене особе.

[241] Више о томе: *Overview of the Open-Source Movement* Copyright © 2000 by R. E. Wyllys, https://www.ischool.utexas.edu/~l38613dw/readings/opensourceoverview.html, последњи пут приступили 12.04.2016.године.

Хакери мисле да су многа њихова незаконита дела оправдана и етички коректна. Трослојну теорија објашњава развој морала. Први ниво бави се избегавањем казни и добијањем награда, други обухвата друштвена правила, а трећи моралне принципе. Сваки од та три нивоа садржи две фазе. Компјутерски криминалци еволуирали су само путем најниже три фазе овог модела: две фазе из првог нивоа и прва фаза из другог нивоа.[242]

Хакери су особе које су способне да изводе социјални инжењеринга без способности емотивне идентификације с осталим људима. На тај начин постижу откривање информација „веровањем на реч", а не упадом у рачунар. Овај метод се заснива на претпоставци да је човек најслабија карика у ланцу безбедности. Године 1999. открива се AS (Asperger`s Syndrom) код ових лица. Тај поремећај зове се и високофункционални аутизам. Испољава се у виду немогућности да се разуме говор лица и тела других особа, као и немогућности саосећања с њима. Постоје, пак, висок коефицијент интелигенције, велике аналитичке способности, као изузетна способност решавања проблема на техничком пољу.

5.3. КЛАСИФИКАЦИЈА САЈБЕР ПРЕВАРАНТА

Хакинг се може класификовати:

1) по намери: добронамерни или малициозни;
3) по извршиоцима: учињен од стране појединца или групе;
4) по месту извршења: екстерни или интерни;
5) по начину реализације: организован или стихијски.

По стручности извршиоца хакинга, што ће имати импликације на начин извршења, хакинг може да буде:

1. аматерски;
2. професионалан.

Ову класификацију поједини аутори означавају као најпотпунију и превасходну.

[242] Више о томе: A SUMMARY OF LAWRENCE KOHLBERG'S, STAGES OF MORAL DEVELOPMENT Copyright 2000 by Robert N. Barger, Ph.D. University of Notre Dame Notre Dame, IN 46556 http://www.csudh.edu/dearhabermas/kohlberg01bk.htm, последњи пут приступили 12.04.2016.године.

5.3.1. Аматери

Вршење хакинга не изискује много труда и трошкова. Сасвим је довољно поседовање рачунара, софтвера и повезивање на информациону мрежу. Није ни потребно посебно техничко знање. Када је у питању социјални инжењеринг, претпоставка је да је реч о учиниоцу с мањим техничким знањем, јер није потребно да извршилац поседује и примењује техничка знања из информатике и рачунарства, већ успех напада зависи од уверљивости извршиоца. У случају напада малвером, напади су олакшани постојањем многобројних блогова где се могу добити упутства за упаде у системе и купити софтвер за сајбер криминал.

Аматери најчешће имају легално занимање, а из различитих разлога се повремено упуштају у криминалну активност. У ту групу спадају:

1) слаби и поводљиви појединци, чији су криминални акти најчешће узроковани тренутном повољном приликом. Често нису ни свесни могућих последица својих радњи. Веома лако их изманипулишу особе које их обећањима, претњама, уценама, наводе на злоупотребе рачунарских система;
2) људи с пороком и особе с приватним проблемима, изазваним неким социопатолошким понашањем, који излаз виде у криминалном понашању;
3) фрустрирани појединци, тј. незадовољне, разочаране и огорчене особе које својим унутрашњим осећајем (сматрају да су преварене, неоправдано запостављене) оправдавају своја чињења.

Професионалци су особе којима је једно од главних, а често и једино занимање бављење криминалом. Владају изузетним технолошким знањима, које константно усавршавају и дограђују. Поред високог нивоа стручности, изузетно су мотивисани и у свом раду показују велику упорност и истрајност, услед чега се веома тешко откривају, а још теже се њихова дела доказују у судском поступку.

Осовна одлика аматерског хакинга је што је то, по правилу, дело младих људи. Хакери аматери обично имају од 17 до 25 година, мада је уочена појава снижавања ове

старосне границе на 13 или чак мање година.[243] И они не наносе, односно не желе да наносе стварне штете (или то не чине намерно) својим упадом у систем.

Мање даровити крекери су *script kiddies*, који користе готова решења за своје криминалне активности. Ова групација је изузетно опасна и расте сваким даном готово експоненцијалном брзином. Углавном не поседују никакво знање програмирања. Мотивацију налазе у школи, односно у кругу своје генерације у којем се крећу и на тај начин желе да привуку пажњу других, стекну признање у друштву због могућности и знања који их уздижи изнад осталих. Под појмом *script kiddies* јавља се једна групација сивих хакера који, у ствари, не познају добро информацијске технологије. *Script kiddies* је погрдан назив за неискусне, пакосне кракере који користе такве програме које су произвели други хакери за нападе на компјутерске саставе и хаковане веб-странице. То не значи да су они хакери, него један вид извршиоца којима су хакери дали алат и пратили су њихов рад да би видели колико су моћно оружје направили.

5.3.2 Хакери

Као извршиоци кривичних дела сајбер криминала, поред типичних криминалаца, који су заинтересовани једино да достигну циљ у виду материјалне користи и у ту сврху користе било који инструмент, софистициран или деструктиван, јављају се хакери као посебна категорија извршилаца. *Diferentia specifica* између ове две категорије извршилаца сајбер криминала лежи у обелодањивању њихових активности. Хакерима је циљ да перманентно развијају нове, софистициране технике напада, гоњени жељом за доказивањем и скретањем пажње на постигнути учинак, док је тежња класичних криминалаца усмерена на прикривање учињених дела.

Реч хакер често се користи да означи извршиоце од клинца који добро игра неку компјутерску игрицу до злих криминалаца какви се последњих година појављују у америчким акционим филмовима, а који се од осталих криминалаца разликује само по томе што, уместо пиштоља, држи лаптоп.Термин хакер у оригинално означава свакога ко је

[243] Више о томе: Forester, T., Morrison, P., *Computer Ethics, Cautionary Tales and Ethical Dilemmas in Computing*, London, Basil Blackwell, 1994, стр. 46.

заинтересован да стекне знања о компјутерским системима и њиховом коришћењу, те многи компјутерски ентузијасти себе сматрају хакерима у том непежоративном смислу.[244]

Прапочетак хакинга и садашњих рачунарских вируса повезује се с раним 60-им година и M.I.T., када је хакингом убачен „*cookie monster*". У време појаве првих хакера, 60-их година, овај термин превасходно се користио у позитивном смислу за групу компјутерских заљубљеника. Сходно томе, под хакерима су подразумевани компјутерски ентузијасти који су формирали клубове, међусобно су размењивали вести, стварали посебне часописе, групно присуствовали и пратили сајмове рачунара, сличне манифестације и презентације и имали су сопствену конвенцију о основним правилима понашања.[245]

Почетком 70-их година хакери су и даље били окупирани разумевањем и савладавањем компјутерских система, суочени с непрегледним могућностима персоналних рачунара.[246]Почетаком 80-их година штампа, извештавајући о хапшењу „хакерске банде", познате као банда 414 (414 *Gang*), састављене од паметних клинаца, старих између 15 и 22 године, који су упадали у компјутерске системе *Los Alamos National Laboratories, Security Pacific Bank, Pepsi-Cola, Canadian cement company, Telenet national communication network, Sloan Kettering centar for cancer*, почела је да користи термин „хакер" у негативној конотацији.[247] Од тада појам хакера еволуира у негативном смислу и употребљава се за означавање „бескрупулозних младих људи" који користе компјутерске могућности за упаде у системе, крађу информација, компјутерских и телекомуникационих ресурса и ремећење рада без дозволе њихових власника или корисника.[248]

Поједине дефиниције хакере изједначавају с програмерима чиме дају значаја њиховом знању из области информатике. Сходно томе, хакер представља „сваког програмера који

[244] Више о томе: Denning, D., *The United States v. craig Neidorf*, „Communications of ACM", vol. 34, no. 3/91, стр. 25.

[245] Више о томе: Roberts, R., Kane, P., *Computers Computer Security*, Greensboro, Computer Books, 1989, стр.16–18.

[246] Више о томе: Kane, P., V.*I.R.U.S. Protection*, Vital Information Resources Under Siege, Includes dr Panda Utilites, New York, Bantam Books, 1989, стр. 75–83.

[247] Више о томе: Lobel, J., *Foiling the System Breakers, Computer Security and Access Control*, New York, McGraw-Hill Book Company, 1986, стр. 1.

[248] Више о томе: Denning, D., *The United States v Craig Neidorf*, „Communications of ACM", vol. 34, no. 3/91, стр. 24–32.

експлоатише, проверава или доводи компјутерске и комуникационе системе до крањих граница, без обзира на последице. Што може довести и до уништења или саботаже вредних података, као и великих штета."[249]

Појам хакер повезује се с упадом у туђе системе: „Хакинг је неауторизовани, насилни приступ односно покушај приступа систему (компјутерском, комуникационом), а хакер је особа која има знање, способности и жеље да у потпуности неовлашћено користи туђе компјутерске и комуникационе системе."[250]

У домаћој теорији се на следећи начин дефинише ова врста изршилаца сајбер криминала: „Хакер је, заправо, особа која толико добро познаје рачунаре и саставе у њима да је у стању проширити њихове могућнсости, за разлику од већине корисника који знају само минималне функције рачунара који су им неопходни за рад."[251]

Хакери не чине хомогену групу нападача на информатичке ресурсе. Они се могу поделити у више група према психолошком профилу, социолошком профилу, мотивима за бављење хакингом и др. Особе које нарушавају безбедност су крекери (*crackers*). Ако наведене активности обављају ради откривања и упозоравања на одређене безбедносне пропусте, називају се „хакери са белим шеширима" (*white hat*), или с намером да нашкоде том систему, када се називају „хакери са црним шеширима" (*black hat*). Крекери немају дефинисане етичке принципе, не деле знање, не доприносе развоју у области рачунарства. Они се служе крађом, вандализмом и нарушавањем поверљивости. За разлику од хакера, крекери не морају да буду рачунарски професионалци, него користе расположиве програме за одређену злонамерну активност не знајући њихову структуру. Док крекери уништавају и саботирају, хакери граде и увећавају знање из области рачунарства и информатике анализом функционисања рачунарских система и укупном информатичком развоју. Примери хакера у наведеном смислу су: Stiv Vozniak (саоснивач фирме *Apple*), Tim Berners-Li (аутор WWW интернет сервиса), Linus Torvalds (отац *Linux* оперативног система), Ričard Talman (оснивач GNU пројекта слободног софтвера). Ти хакери су у својим студентским данима имали

[249] Више о томе: Група аутора, *Organizing for Computer Crime, Investigation and Prosecuting*, Nacional Institute of Justice USA, 1990 стр. 7. и 8.

[250] Више о томе: Denning, D., *A Dialog on Hacking and Security*, edicija – *Computers Under Attack, Intruders, Worms and Viruses*, New York, ACM Press, 1990, стр. 421–439.

[251] Више о томе:Бабић, В., *Компјутерски криминал*, Рабић, Сарајево, 2009, стр. 124.

хакерска искуства, а касније као успешни пословни људи остали поборници слободног приступа информацијама.

Хакери оправдавају своје активности чињеницом да је свако учење и истраживање корисно, да је слободан проток информација од значаја за друштво, а њихово скривање представља злочин. Такође заступају мишљење да је откривање рањивости система које могу да буду искоришћени за злонамерне нападе корисно, а да су неке организације због свог неетичког понашања заслужиле да буду нападнуте.

5.3.3 Организоване групе

Као извршиоци сајбер криминала могу се јавити:

1) индивидуални криминалци мотивисани остваривањем материјалне користи, који немају разрађене дугорочне планове, нити самосталну стратегију деловања. Врло ретко се удружују с другим особама;
2) организоване групе компјутерсских хакера, које су састављене од појединаца који делују под заједничким интересима.

Организоване хакерске групе карактеришу се чврстом организацијом и хијерархијском устројеношћу. Резултати које остварују у директном су односу с бројношћу и стручношћу чланова и квалитетом организације. Ове групе, поред класичних начела деловања организованих криминалних група, владају изузетним информатичким знањима која користе у извршавању тешких облика кривичних дела из области сајбер криминалитета, што их сврстава у професионалне извршиоце највишег ранга. Усамљени хакери у мрачним собама, који провaљују у рачунаре у разним деловима света због славе, постали су прошлост. Модерни хакери не раде за славу, већ за новац, и то у склопу добро организованих скупина.

При удруживању хакера из разноразних разлога, а пре свега због извршења радњи које су окарактерисане као казнена дела сајбер криминала, долазимо до форме злочиначке организације, која је удружена, па сеже и до самих структура власти. У ову групу спадају сви хакери који се баве било којом врстом сајбер криминала а укључени су у рад злочиначке организације.

Све наведене скупине могу се окарактерисати називом организоване хакерске скупине. Оне нису ништа другачије окарактерисане него као скупине организованог

криминала. То су категорије које представљају скупове појединаца који имају заједничке интересе, а они су најчешће скуп појединачнх интереса и у њиховој реализацији заједнички делују. Организоване хакерске групе варирају од лабавих удружења са заједничким интересима и врло често одвојеним, појединачним циљевима, до чврсто усклађених организација с добро дефинисаним циљевима.

Сајбер простор постао је ново поље акције организованог криминала, карактеристичан по организационој чврстини, хијерархијским односима, строгој дисциплини, послушности и особеној лојалности уз изграђену дугорочну стратегију и детаљно разрађену тактику.Организоване криминалне групе брзо се прилагођавају новим технологијама, напуштају физичко застрашивање у корист сајбер оружја, попут *botnet*-а и малвера.

Компромитована рачунарска мрежа (енгл. *botnet*), сачињена од 20 до 30 хиљада заражених рачунара којима управљају „информатички плаћеници", користи се за нападање и уцењивање привредних корпорација и других комерцијалних организација. Евидентирани су и случајеви давања *botnet*-а у закуп, при чему цена изнајмљивања достиже износ и до 28.000 долара месечно, а тарифа по сату и до 100 долара. Претпоставка је да се на дневном нивоу, број компромитованих рачунарских мрежа увећава за 25.

Запажа се растући однос између сајбер криминала и организованог криминала. Интернет користе криминалне групе не само као помоћ већ и као место извршења традиционалних кривичних дела – превара, крађа, изнуда. Према подацима Европола, само у Европској унији има око 3.600 таквих група. Током последњих година дошло је до „професионализације" организованог сајбер криминала, и то не само у смислу да компјутерски напади постају све сложенији и изискују учешће професионалаца у њиховој припреми. Осим тога, интернет све више користе организоване криминалне групе за прање новца. Интернет је огромна прилика за преваре с рачунима. Онлине аукције омогућавају да се преносу средстава у вези с наводним правним трансферима, развој електронског плаћања и онлајн банкарство пружају многе начине да се сакрију кретања прихода од криминала и да се обаве илегалне трансакције.

У пословни модел организације компјутерског криминала спадају спам, шпијунажа и саботажа, док се за организовање послова и подршку организације старају маркетинг менаџери, програмери и неизоставно логистичари. Код подршке ту су маркетинг менаџери

који врше консултације на тржишту и прибављају послове, а логистичари су ту да би прибавили ,,алатке и машинерију" за рад. Организоване хакерске скупине имају углавном локални карактер, али до одређеног нивоа, с дефинисаним циљевима и разрађеном тактиком. Самим тим врше бирање и истраживање циљева. Виша инстанца организоване хакерске скупине је криминала организација. Постоје мишљења да хакери још увек не поседују највиши ступањ организованости, мада није искључено да такво нешто и постоји унутар других криминалних оргаизованих скупина, као огранак или ћелија.[252]

Према истраживању фирме Финјан, која се бави мрежном сигурношћу а истражила је свет хакера и дошла до спознаје да се модерни хакери удружују у криминалне организације сличне мафији: ,,Хакери су организовани у скупине које хијерархијом подсећају на италијанску мафију. На врху организације је шеф који доноси стратешке одлуке, али се никада не бави криминалним делима, а не мора да буде ни информатички образован. Његов заменик организује криминалне делатности и понекад набавља специјалне програме за извршавање одређених казнених радњи. Испод њих су управитељи послова који помоћу мрежа сарадника непосредно извршавају наведене казнене радње. Украдене податке продају такође специјалним припадницима организације који не знају ништа о начину којим су прибављени, као ни то ко је непосредни извршитељ. Добра организација посла је повећала ефикасност, па се данас банковни подаци и подаци с кредитних картица могу купити врло јефтино, али подаци за логовање у фирме и приступ имејлу и приступ FTP рачунарима коштају знатно више."[253]

Хакери и хакерски организовани криминал делују на свим фронтовима и могу се унајмити за све врсте сајбер криминалитета, а нарочито за облике који су нови и још увек нису довољно истражени, те спроведени кроз казнено законодавство и тиме окарактерисани као казнено дело, што спада у домене нових или чак неокласичних казнених дела која нису ништа друго него већ позната казнене дела која су у неким државама окарактерисана кроз законодавство као таква док у нашем још нису.

Инсајдер је припадник уског круга људи који познаје прилике унтар круга, односно добро је упућен у послове којима се бави организација било да је она криминална, било да је

[252] Више о томе:Бабић, В., *Компјутерски криминал*, Рабић, Сарајево, 2009, стр. 132.

[253] Више о томе:*Researchers Trace Structure of Cybercrime Gangs*, http://www.pcworld.com/article/148416/article.html, последњи пут приступили 12.04.2016.године.

друга организација и та је особа пожељна за сведока приликом процесуирања или других радњи у доказивању. Свакако, инсајдер је особа која добро познаје информациону технологију неке организације и спремна је да подели ту информисаност с другима за одређене уступке, новчана средства или сведочења.

Најпознатија организација која се бави таквим малверзацијама је *Shedow Crew*, која је, у ствари, међународна криминална организација која се бави трговином хакерски прибављеним материјалима, а у шта спадају украдени лични подаци власника текућих рачуна, или бројеви украдених кредитних картица или лажне идентификације других дигиталних исправа или матични бројеви који могу довести до података у вези с финансијским средствима одређених особа по унапред познатом имену. Наведена организација изашла је на светлост с веб-странице www.counterfeitlibrary.com да би након тога настао и www.carderplanet.com, која је првенствено руска веза страница за пуно горе намене. На наведеној страници се налази и форум који је најопаснији, јер поред тих малверзација с кредитним картицама поседује и собе за чет и форум с другим лицима ради остваривања других кажњивих радњи, као што су: порнографија, педофилија, спам, фишинг, крек кодови, вируси, тројанци и слично. Поред наведених кредитних веб-страница, постоје и www.iaaca.com и www.cardeportal.com, које се баве софтверском и хардверском подршком за регуларну израду кредитних картица и њиховом дистрибуцијом, те сваком делатношћу повезаном с израдом кредитних картица. Вредност прибављених података процењује се према могућностима њиховог коришћења за куповину путем интернета, израду и дистрибуцију кривотворених кредитних картица које се могу употребити за подизање готовине или неке још разрађеније криминалне делатности. Што се тиче организованих хакерских група из области е-банкарства, најпознатија је група Карбанак. Ова интернационална група хакера из Русије, Украјине и других делова Европе, као и Кине, користи разне хакерске технике за циљане нападе.[254]

5.4 ОТКРИВАЊЕ ПРЕВАРА КАО МОДЕЛА ОСТВАРИВАЊА САЈБЕР КРИМИНАЛА

Анонимност интернета, бежични приступ и коришћење прокси сервера значајно ометају откривање криминалаца: у извршењу кривичног дела може да се користи „ланац" сервера тако што се приступа интернету путем јавних приступних тачака, као што су интернет кафеи,

[254] Више о томе: http://www.informacija.rs/Vesti/Kako-je-sajber-banda-Karbanak-ukrala-od-banaka-milijardu-dolara.html, последњи пут приступили 12.04.2016.године.

или Ви-Фи мреже. Дакле, постоји довољно начина да се опструира истрага. Откривање сајбер деликта отежава и *Rootkit*, који представља скуп програма које користе хакери да би избегли откривање док покушавају да остваре недозвољени приступ компјутеру. Ова невидљива форма за прикривање активности малвера по инсталацији бива невидљива како за корисника, тако и за избегавање да их открије антивирусни софтвер.

Први корак отпочиње након пријема аларма комбинацијом различитих индикатора добијених од вишеструких сензора постављених на одређеним мрежним компонентама, или тако што администратор система или одговарајући тимови прегледају логова. Различити мрежни уређаји (системи за детекцију напада) знатно помажу у том процесу јер бележе различите врсте активности које могу да буду важан извор доказа у случају сајбер криминала. У зависности од подешавања наведених мрежних уређаја, подаци које они евидентирају обично обухватају време догађаја, наводну изворну IP адресу, као и остале податке који могу довести до починиоца.Значајну помоћ у откривању инцидената у сајбер простору могу пружити различите организације, као што су *Computer Emergency Response Team* (CERT) и *Internet Storm Centar*, који упозоравају на претње на интернету.

The Cooperative Association for Internet Data Analysis (CAIDA) је организација која обезбеђује алат и објављује резултате у вези с надгледањем интернета. У Европској унији је покренут пројекат *Lobster* за надгледање „кичме" (*backbone*) интернет инфраструктуре.[255] Помоћу различитих сензора и уређаја прате се активности, тако да једна особа може да надгледа више система истовремено. Надгледање наведених уређаја остварује се у оперативним центрима.Пошто одређени мрежни уређај детектује напад, упозорење се шаље на конзолу за надзор система, где је стално присутно стручно лице, односно тим за одногов у случају инцидента. Пре адекватног одговора реализује се форензичка анализа инцидента у реалном времену, тако да прикупљени подаци могу послужити као доказни материјал за процесуирање починилаца.

У Републици Србији Служба за борбу против високотехнолошког криминала у оквиру Министарства унутрашњих послова предузима активности усмерене на откривање кривичног дела и починиоца које претходе формално започетом кривичном поступку. Преткривични поступак завршава се када је откривање кривичног дела и починиоца остварено у мери која омогућава посебном тужиоцу да донесе одлуку о томе да ли ће

[255] Више о томе: Bhasin, S., *Web Security Basics*, Premier Press, Ohio, 2003, p. 9.

одбацити кривичну пријаву или ће поднети захтев за покретање кривичног поступка. На основу члана 235, став 2 Законика о кривичном поступку, тужилац може захтевати од органа унутрашњих послова да прикупе потребна обавештења и да предузму друге мере ради откривања кривичног дела и починиоца.[256] Служба за борбу против високотехнолошког криминала, дакле, јесте орган откривања сајбер криминала који може да буде ангажован у преткривичном поступку, односно у претходном кривичном поступку, када је потребно извршити увиђај.

Многе државе у фази откривања кривичних дела из области сајбер криминала користе програм *FinSpy*. *FinSpy* је сличан малициозним програмима, пре свега тројанском коњу, који у рачунар доспева путем зараженог мејла. По инсталацији овај софтвер без знања корисника снима екран, разговоре путем *Skype*-а, бележи активности на тастатури, краде фотографије и документа с рачунара и смарт телефона. Овај шпијунски програм је у власништву обавештајних служби јер виду да произвођач тврди да се софтвер продаје искључиво владиним агенцијама за потребе кривичних истрага и у ту сврху праћења педофила, терориста, припадника организованих криминалних група, отмичара и трговца људима. У законодавствима држава корисница *FinSpy* нису јасно дефинисана правила употребе, па није искључено да се у државама које се налазе на списку клијената компаније овај програм користи и у друге сврхе.По тврдњама *Njujork Tajms*-а, Србија спада у 25 државе у свету чије власти користе софтвер *FinSpy* (*FinFisher*) за шпијунирање својих грађана. [257]

У фази откривања надлежни органи могу помоћ да затраже од друштвених мрежа, који ће им доставити основне информације о корисницима, као што су име и датум регистрације налога, приступ логовима IP адресе или садржају налога. У четвртом извештају Facebook-а о захтевима власти широм света за информацијама о корисничким налозима и блокирању садржаја истакнуто је: „У другој половини 2014. године америчке власти послале су 14.274 захтева за приступ подацима 21.731 налога. Facebook је у 79% случајева одговорио позитивно на те захтеве пружајући неке од тражених информација. Међутим, прави број захтева америчких власти могао би бити и већи, јер извештај који је објавио Facebook није укључио одређене врсте захтева који су у вези с националном безбедности. Из Немачке су

[256] *Законик о кривичном поступку Републике Србије* „(Сл. гласник РС”, бр. 85/05, 88/05 – исправка, 107/05 – исправка, 72/09, 111/09, 121/12, 104/13), члан 235.

[257] Више о томе:*Da li nas država špijunira*, http://www.informacija.rs/Vesti/Da-li-nas-drzava-spijunira.html, последњи пут приступили 12.04.2016.године.

стигла 2.132 захтева, док су у првих шест месеци прошле године немачке власти послале Facebook-у 2.537 захтева. Из Србије је стигло 15 захтева за информацијама о 25 налога корисника, а у 60% случајева на те захтеве је одговорено позитивно."[258]

У извештају друштвене мреже Твитер о власницима налога у 2014. години се први пут међу подносиоцима захтева појављују власти Србије, Кипра, Доминиканске Републике и Пољске, које су се тиме придружиле десетини других земаља које су и раније тражиле информације о власницима Twitter налога. Из Србије су Twitter-у упућена три захтева за информаце о корисницима, од којих је Twitter само на један одговорио позитивно, док су друга два захтева одбијена. Највећи број захтева овој друштвеној мрежи стигао је из SAD (2.436), и они чине 56% укупног броја захтева које је компанија добила. Јапан је на другом месту са 425 захтева, а Турска на трећем са 412 захтева.[259]

Сајбер преваре, ако нису крајње очигледне, прилично тешко се откривају и доказују. Сматра се да постоји и велика „тамна бројка" када су сајбер преваре у питању пошто оштећена лица та кривична дела не пријављују што из страха да су саучесници у противправним радњама, што из убеђења да су сами криви због своје лаковерности и наивности, или их је због околине срамота да пријаве да су оштећени.

5.5. ДОКАЗИВАЊЕ ПРЕВАРА КАО МОДЕЛА ОСТВАРИВАЊА САЈБЕР КРИМИНАЛА

Доказ представља „утврђену, констатовану релевантну везу међу процесима који су директно или индирекно утицали на настанак кривичног дела, траговима, предметима и људима. Посматрано са гносеолошке стране, докази представљају све промене у средини припремања, извршења, прикривања и уживања плодова кривичног дела, које су у

[258] Више о томе: https://govtrequests.facebook.com/country/Serbia/2014-H2/, последњи пут приступили 12.04.2016.године.

[259] Више о томе: *I Srbija među zemljama koje su tražile informacije o korisnicima* Twitter *naloga*, http://www.informacija.rs/Ostalo/I-Srbija-medju-zemljama-koje-su-trazile-informacije-o-korisnicima-Twitter-naloga.html, последњи пут приступили 12.04.2016.године.

релевантној вези са делом. Доказ је само она чињеница која је повезана са кривичним делом."[260]

Докази у кривичном поступку се дефинишу као „извори сазнања уз помоћ којих се установљавају чињенице у кривичном поступку". У науци кривично-процесног права о доказима постоје веома разноврсна схватања, која се углавном односе на одређивање њиховог материјалног појма. Тако се, поред наведеног, наилази на ставове да су докази чињенице о истинитости или неистинитости спорне чињенице, да су то фактички подаци који се налазе у законом одређеним изворима, да су извори сазнања о чињеницама које подлежу утврђивању, као и да представљају фактичке податке који у законом предвиђеним процесним формама утврђују постојање кривичног дела и кривицу лица позваног на кривичну одговорност."[261]

С обзиром на форму доказа, општа подела обухвата: непосредне (усмено сведочење), материјалне (реалне), документоване (записи, упутства, штампани материјали). Већина доказа у случају компјутерског криминала и сајбер криминала су документовани докази и демонстративни докази (у форми елемента, модела).[262]

Дигитални доказ је податак или информација у дигиталном облику којим се установљавају чињенице у кривичном поступку. Не обухвата само кривична дела где се појављују рачунари или рачунарске мреже већ и друге облике криминала где се докази могу наћи у дигиталном облику.[263] У буквалном смислу, дигитални доказ представља низ нула и јединица које електронски уређаји преводе у разумљив облик.

С обзиром на постојаност, дигитални докази могу се поделити на:

[260] Више о томе:Водинелић, В., *Научни проблеми на релацији доказни извор – доказ – доказивање у кривичном процесном праву*, „Анали правног факултета", бр. 3–4, Правни факултет, Београд, 1994, стр. 293.

[261] Више о томе:Алексић, Ж., Миловановић, З., *Лексикон криминалистике*, Глосаријум, Београд, 1995, стр. 63.

[262] Више о томе:Tipton, H., Krause, M., *Information Security management Handbook* (fifth edition), CRC Press, New York, 2004, part: Welch, T., *Computer Crime Investigation and Computer Forensics*, p. 2877.

[263] Више о томе:*Forensic Examination of Digital Evidence/A Guide for Law Enforcement*, National Institute of Justice, Washinghton, 2004, p. 39.

– привремене – носач података се напаја из спољашњег извора напајања, те прекидањем тог напајања нестају и подаци (РАМ, тј. Радна меморија с насумичним приступом, чији садржај може да се мења);
– нестале – носач података се напаја из унутршњег извора напајања, нпр. батеријом, и прекидањем напајања нестају и подаци (нпр., рам на лаптоп рачунару који има напајање на батерију);
– полусталне – носач податка је сталан, али се може променити (нпр., хард-диск, цд, двд и сл.);
– сталне – носач податка је сталан и не може се променити (нпр., РОМ, тј. меморија чији је садржај унет прликом производње, која је фиксна и не може се мењати током рада рачунара, а не губи се искључивањем из напајања).[264]

Према изворности, дигитални докази могу да буду оригинални и копирани (прецизна дигитална репродукција свих елемената који су садржани у оригиналу).[265]

Дигитални докази морају да буду:
– прихватљиви, тј. добијени на правно ваљан начин;
– аутентични, односно без сумње повезани с инцидентом;
– потпуни, тј. комплетни, чиме се може створити целовита слика о починиоцу и незаконитим активностима;
– поуздани, односно не смеју бацити сумњу на аутентичност и веродостојност и
– уверљиви, тј. разумљиви за учеснике у кривичном поступку.[266]

Према ”*The Scientfic Working Group on Dgital Evidence*”, сматра се да неки објекат постаје доказ када га суд призна и прикупљен је на легалан и законит начин.Пре прихватања дигиталних доказа потребно је да суд провери да ли су ти докази релевантни, аутентични, а проверава се ида ли представљају оригиналне доказе или копије.

[264] Више о томе:Mohay, G., Anderson, A., Collie, B. and others, *Computer and Intrusion Forensics*, Artech House, London 2003, p. 25.

[265] Више о томе:Shinder, D., *Scene of the Cybercrime*, Computer Forensics Handbook, Syngress Publishing, Inc., Rockland (USA), 2002, p. 550.

[266] Више о томе:Vacca, J., *Computer Forensics – Computer Crime Scene Investigations*, Charles River Media, Hingham, Massachusetts, USA, 2002, p. 2.

Дигитални докази могу да буду од велике важности у криминалним истрагама. Дигиталне евиденције могу помоћи да се утврди када се догађај десио, где су жртва и осумњичени били, с ким су комуницирали, чак могу да покажу и намеру да се злочин изврши. На пример, у веб-претраживачима могу се наћи претраге као што су „упити", „крађе" и слично, што може показати намеру за извршењем злочина. Некада су информације сачуване у рачунару једини докази у истрази, некада је електронска пошта једина веза између злочинца и жртве.

У вези с дигиталним доказима јавља се проблем јер се подаци настали на рачунару или другим дигиталним уређајима лако могу изменити, обрисати или оштетити. Са самим престанком рада и коришћења одређеног хард-диска дигитални докази нису уништени. Брисање самих дигиталних доказа не значи да су се они трајно уништили, јер данас на интернету можемо да пронађемо програме који су бесплатни и који нам податке са самог хард-диска могу вратити, могу форматирати диск и макар делимично вратити податке уколико је диск физички оштећен.Дигиталне доказе можемо потпуно уништити само рециклажом хард-диска, што је еколошки јако корисно да не би одређеним материјама загадили животну средину, а омогућава и уштеду енергије. У том случају дигитални докази су трајно уништени и не могу се више користити, тако да се прихватљивим дигиталним доказима сматрају они који имају правну основу и могу да задовоље одређене критеријуме.

6 НАДЛЕЖНОСТ ДРЖАВНИХ ОРГАНА У БОРБИ ПРОТИВ САЈБЕР КРИМИНАЛА

6.1. НАДЛЕЖНОСТ ДРЖАВНИХ ОРГАНА У БОРБИ ПРОТИВ САЈБЕР КРИМИНАЛА У РЕПУБЛИЦИ СРБИЈИ

6.1.1. Служба за борбу против сајбер криминала у оквиру МУП-а

Полицијски кадрови морају да буду високообучени, технолошки опремљени најсавременијом средствима јер се не може борити против најновијих техологија рачунарима из прошлог миленијума. Процес оснивања посебних органа по Закону о оснивању и надлежности државних органа за борбу против високотехнолошког криминала трајао је две и по године. Последња карика у том ланцу јесте Посебна служба у оквиру МУП РС, која је почела да ради у априлу 2008. године.

Закон о оснивању и надлежности државних органа за борбу против високотехнолошког криминала у члану 9. Регулише рад Службе за борбу против високотехнолошког криминала: „Ради обављања послова органа унутрашњих послова у вези са кривичним делима из члана 3. овог закона, образује се у оквиру министарства надлежног за унутрашње послове служба за борбу против високотехнолошког криминала (у даљем тексту: Служба).”[267]

Служба за борбу против високотехнолошког криминала поступа по захтевима посебног тужиоца, а у складу са законом. Овај орган је дакле орган откривања сајбер криминала, који може да буде ангажован у преткривичном поступку, односно у претходном кривичном поступку када је потребно извршити увиђај.Министар надлежан за унутрашње послове, по прибављеном мишљењу посебног тужиоца, поставља и разрешава старешину Службе и ближе уређује њен рад у складу са законом.

Наиме, током 2008. године поднете су кривичне пријаве против тридесет пет лица, одузети су 53 рачунара и 49.000 оптичких дискова. Карактеристика рада у том периоду огледа се у чињеници да се 90% предмета односи на извршење кривичног дела из члана 199 КЗ. Такође, јавља се и повећан број извршења кривичних дела рачунарска превара и злоупотреба платних картица.[268]

У оквиру Одељења за борбу против високотехнолошког криминала Службе за борбу против организованог криминала Министарства унутрашњих послова Републике Србије, од 03. 08. 2001. године, када је у ИНТЕРПОЛ-у Београд регистрован први случај високотехнолошког криминала на основу обављене кореспонденције с иностраним органима од 01. 03. 2010. године, формирано је укупно 256 досијеа, у којима се налазе појединани или групни случајеви високотехнолошког криминала.[269]

[267] Закон о организацији и надлежности државних органа у борби против високотехнолошког криминала („Сл. гласник РС", бр. 61/2005 и 104/2009), члан 9.

[268] Више о томе:Удружење јавних тужилаца и заменика јавних тужилаца, Сузбијање високотехнолошког криминала, АТС, Београд, 2010, стр. 231.

[269] Више о томе:Уљанов, С., Урошевић, В., Ивановић, З., *Високотехнолошки криминал из угла међународне сарадње криминалистичке полиције*, зборник радова с међународног научно-стручног скупа „Међународна и национална сарадња и координација у супротстављању криминалитету”, вол. 3, бр. 1, стр. 530–541, Интернационална асоцијација криминалиста, Бања Лука, 2010, стр. 537.

6.1.2. Посебно тужилаштво у случајевима сајбер криминала

За поступање у предметима кривичних дела на основу Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала надлежно је Више јавно тужилаштво у Београду за територију Републике Србије.У Вишем јавном тужилаштву у Београду образовано је посебно одељење за борбу против високотехнолошког криминала, тј. посебно тужилаштво, којим руководи посебни тужилац за високотехнолошки криминал. Посебног тужиоца за високотехнолошки криминал поставља републички јавни тужилац из реда заменика јавних тужилаца који испуњавају услове за избор за заменика вишег јавног тужиоца, уз писмену сагласност лица које се поставља. При избору предност имају заменици јавних тужилаца који поседују посебна знања из области информатичких технологија.[270]

Сходно наведеном, 5. августа 2011. године Републички јавни тужилац Загорка Доловац поставила је заменика вишег јавног тужиоца Бранка Стаменковића за руководиоца Посебног одељења за високотехнолошки криминал, тј. посебног тужиоца за високотехнолошки криминал. У Посебном тужилаштву, поред руководилаца, ангажована су још два заменика вишег јавног тужиоца специјализована за ову област, као и два тужилачка саветника уз пратеће административно особље.

Од оснивања почетком 2006. године закључно с 1. октобром 2011. године Посебно тужилаштво за високотехнолошки криминал поступало је или поступа у више од 1.700 предмета у оквиру своје надлежности.[271]

У овом тренутку техничке могућности Посебног тужилаштва за борбу против сајбер криминала нису на задовољавајућем нивоу. Ради се и даље у оквиру постојећег простора Окружног јавног тужилаштва на 6. спрату Палате правде, у улици Савској 17а у Београду, уз коришћење заједничких техничких ресурса који својим особинама не одговарају потребама Посебног тужилаштва.

---

[270] *Закон о организацији и надлежности државних органа у борби против високотехнолошког криминала* („Сл. гласник РС", бр. 61/2005 и 104/2009), члан 4.

[271] Више о томе:Посебно тужилаштво за високотехнолошки криминал, http://www.beograd.vtk.jt.rs/, последњи пут приступили 12.04.2016.године.

У раду Посебног тужилаштва велика пажња је посвећена стручном усавршавању и присуству на стручним семинарима и другим видовима обуке који су значајни за успешну борбу против сајбер криминала. Велики број семинара и скупова на ову тему узрокован је и све већим интересом јавности, као и подизањем свести о значају сузбијања ове врсте криминалитета и формирања концепта сајбер безбедности активним учешћем свих друштвених субјеката и успостављањем чврше сарадње с органима откривања и гоњења, и то како на домаћем, тако и на међународном плану.[272] У наведеном смислу, током 2008. године постављена је и интернет презентација тужилаштва на адреси http://www.beograd.vtk.jt.rs/, а у циљу да омогући јавности да се боље упозна с радом тужилаштва и оствареним резултатима.

6.1.3. Надлежност и организација судова у случајевима сајбер криминала

Закон о организацији и надлежности државних органа у борби против високотехнолошког криминала у 3. делу прописује „Надлежност и организацију судова у предметима сајбер криминала". У члану 10. наведено је: „За поступање у предметима кривичних дела из члана 3. овог закона надлежан је Виши суд у Београду, за територију Републике Србије."[273]

Судска пракса Већа за борбу против високотехнолошког криминала Окружног суда у Београду пре свега је одређена законом постављеним оквиром, односно одредбама којима је регулисана стварна надлежност овог суда за суђење кривичних дела високотехнолошког криминала, а које обухватају:

1) кривична дела против безбедности рачунарских података одређена Кривичним закоником;

2) кривична дела против интелектуалне својине, имовине, привреде и правног саобраћаја, у којима се као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже и рачунарски подаци, као и њихови производи у материјалном или електронском облику ако број примерака ауторских дела прелази 2.000 или настала материјална штета прелази износ од 1.000.000 динара;

[272] Више о томе:Удружење јавних тужилаца и заменика јавних тужилаца, Сузбијање високотехнолошког криминала, АТС, Београд, 2010, стр. 236.

[273] *Закон о организацији и надлежности државних органа у борби против високотехнолошког криминала* („Сл. гласник РС", бр. 61/2005 и 104/2009), члан 3.

3) кривична дела против слобода и права човека и грађанина, полне слободе, јавног реда и мира и уставног уређења и безбедности Републике Србије, која се због начина извршења или употребљених средстава могу сматрати кривичним делима високотехнолошког криминала, у складу са чланом 2. став 1 Закона о организацији и надлежности државних органа у борби против високотехнолошког криминала. [274]

У другостепеном поступку надлежан је Апелациони суд у Београду. Судије у Одељењу распоређује председник Вишег суда у Београду из реда судија тог суда, а уз њихову сагласност. Приоритет је дат судијама које имају искуства у области информационих технологија. Председник Вишег суда у Београду може да распореди у Одељење и судије других судова, а уз њихову сагласност. Распоређивање траје најдуже две године и може се продужити одлуком председника Вишег суда у Београду, а уз писану сагласност лица која су ту распоређена.

У досадашњој судској пракси посебног Већа за борбу против високотехнолошког криминала запажено је да се највећи број кривичних предмета односи на кривична дела против интелектуалне својине у којима је објекат заштите ауторско дело, и то на кривично дело неовлашћено искоришћавање ауторског дела или предмета сродног права из члана 199. Кривичног законика Републике Србије. У погледу осталих кривичних дела из области високотехнолошког криминала која су предмет судског поступка, назаступљенији облици су превара из члана 208. КЗ, у којој се као средство извршеног дела појављује рачунар, рачунарска превара из члана 301. КЗ, рачунарска саботажа из члана 299. КЗ, и неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података из члана 302. КЗ. [275]

[274] *Закон о организацији и надлежности државних органа у борби против високотехнолошког криминала* („Сл.гласник РС", бр. 61/2005 и 104/2009), члан 3.

[275] Више о томе:Удружење јавних тужилаца и заменика јавних тужилаца, Сузбијање високотехнолошког криминала, АТС, Београд, 2010, стр. 237.

6.2. АКТИВНОСТИ МЕЂУНАРОДНИХ ОРГАНА И ОРГАНИЗАЦИЈА НА ПОЉУ СУЗБИЈАЊА САЈБЕР КРИМИНАЛА

Имајући у виду чињеницу да је сајбер криминал врло комплексан савремени облик криминала, брзину којом се развија и сложености и последице које су сваким даном све садржајније и обимније, током развоја и квалитативног усавршавања одговора на различите феноменолошке поставке сајбер криминала, значајне активности су предузимане и свакодневно се предузимају на међународном и регионалном нивоу као адекватан одговор у националним оквирима. Сваки извештај, свака препорука и смерница представљају својеврсне упоришне тачке за даља теоријска разматрања, доношење и измене позитивноправних прописа и квалитетније практичне делатности органа надлежних за истрагу, гоњење и процесно уобличавање ових противзаконитих делатности.

6.2.1 Уједињене нације

Генерална скупштина Уједињених нација је Резолуцијом 65/230 покренула питање о проблему сајбер криминала да би се сазвале међудржавне експертске групе да спроведу свеобухватну студију о проблему сајбер криминала као одговор на то питање. Студијску групу организовао је UNODC у Бечу са циљем истраживања могућности за јачање постојећих националних и међународних правних или других одговора на сајбер киминал и предлозима за стварање нових.

Експертска група одржала је своју прву седницу у Бечу јануара 2011. године. Упитник је у фебруару 2012. године упућен свим државама чланицама Уједињених нација, приватном сектору, међународним организацијама и академским заједницама. Организоване су и регионалне радионице.Друга седница одржана је у Бечу 25–28. фебруара 2013. године, када је дискутовано о нацрту и препорукама из студије, а затим је одлучено о даљим корацима.

6.2.2 Генерална скупштина

Резолуција о борби против злоупотребе информационих технологија, коју је усвојила Генерална скупштина 4. децембра 2000. године резолуцијом бр. 55/63, предвиђа: "Државе треба да осигурају да њихови закони и пракса елиминишу уточишта за оне који злоупотребљавају информационе технологије.

Правни системи би требало да штите поверљивост, интегритет и доступност података и рачунарских система од неовлашћеног оштећења и осигурати да се свака злоупотреба кажњава."Резолуција 56/121, усвојена 19. децембра 2001. године, обухвата препоруке о спречавању злоупотребе информационих технологија и борби против ње.Генерална скупштина је 2010. године усвојила Резолуцију 65/230 засновану на члану 42. Салвадорске декларације. Нацрт резолуције који је направила Комисија за превенцију криминала и кривично правосуђе у члану 8. предвидео је члан 42. Салвадорске декларације (2010). Резолуција је предложила успостављање на следећи начин: ,,Међудржавне експертске групе су задужене за спровођење свеобухватне студије о проблему сајбер криминала и одговора на њега од стране држава чланица, међународне заједнице и приватног сектора, укључујући и размену информација о националном законодавству, најбоље примере из праксе, техничку помоћ и међународну сарадњу, са циљем налажења начина за јачање постојећих и предлагања нових националних и међународних правних или других одговора на сајбер криминал.” Резолуцију је усвојила Комисија, а касније и Генерална скупштина Уједињених нација у својој Резолуцији 65/230.

6.2.3 Канцеларија Уједињених нација за дрогу и криминал

Конгрес о спречавању криминала и кривично правосуђе Уједињених нација разматрао је техничка питања и кривично процесуирање компјутерских злоупотреба за последња четири конгреса. Уједињене нације усвојиле су 1990. године резолуцију о законодавству компјутерског криминала на 8. конгресу УН о превенцији криминала и поступању према починиоцима у Хавани, Куба. 12. конгрес у Салвадору, у Бразилу, одржан је 2010. године, а у фокусу конгреса била су питања сајбер криминала у вези с неколико догађаја. Извештаји Конгреса и нацрти доступни су у Канцеларији Уједињених нација за дрогу и криминал.

6.2.4. Савет Европе

Савет Европе био је једна од првих међународних организација које су покренуле иницијативу за стварање правних претпоставки за сузбијање компјутерског криминала удруженим напорима више земаља. У сфери кривичног права одржано је више од двадесет конвенција и усвојено је више од осамдесет препорука. Године 1989. Комитет министара, састављен од министара иностраних послова држава чланица, усвојио је препоруку о

заштити података. Том препоруком позивају се државе чланице да размотре увођење неких прописа у вези с компјутерским криминалом.

Тек 1995. године Савет Европе донео је Препоруку 95 којом представља процедуре за имплементацију претходне препоруке. Препорука 95 представља први моменат дефинисања процедура претраге и заплене, надгледања, електронских доказа, енкрипције и интернационалне кооперације. У фебруару 1997. године формиран је Комитет експерата о криминалу у сајбер простору (PC-CY). Задатак тог комитета је био испитивање компјутерског криминала и проблематике у вези њим у кривично-процесном праву. Крајњи циљ рада тог комитета био је дефинисање преступа, надлежности, претраге и заплене, заштите података и одговорности интернет провајдера. Комитет је сачинио предлог за Конвенције о сајбер криминалу.

Конвенција Савета Европе о сајбер-криминалу усвојена је и постала је отворена за потписе на конференцији у Будимпешти, Мађарска, 2001. године. Конвенција је ступила на снагу 1. јула 2004. године. До септембра 2015. године 7 земаља потписница није ратификовало Конвенцију. Укупно 47 држава чланица је ратификовало Конвенцију Савета Европе о сајбер криминалу. Конвенција Савета Европе о сајбер-криминалу из 2001. године је историјски корак у борби против високотехнолошког криминала. Државе чланице требало би да је ратификују, а друге државе да размотре могућност приступања Конвенцији или оцене оправданост спровођења принципа Конвенције. С Конвенцијом Савета Европе о сајбер криминалу и препорукама Г8, ОАС, и АПЕЦ једино се може остварити циљ стварања глобалног правног оквира против сајбер-криминала. Ратификацијом или приступањем Конвенцији Савета Европе о сајбер криминалу, или имплементацијом принципа државе прихватају да њихово домаће законодавство кажњава описана дела у материјалном кривичном делу и успоставља процедурална средства потребна за истрагу и гоњење таквих дела. На тај начин постићи ће се хармонизација националних права у области сајбер криминала.

6.2.5. Међународна унија за телекомуникације

Улога Међународна унија за телекомуникације је да нађе консензус за међународну сарадњу у области сајбер безбедности да би постигла заједничко разумевање сајбер претњи држава у свим фазама привредног развоја, који укључује развој и стављање на располагање решења чији је циљ решавање глобалних изазова сајбер безбедности и сајбер криминала.

Најактивнија УН институција у постизању хармонизације на глобалном нивоу у области сајбер безбедности је Међународна унија за телекомуникације (ИТУ), са седиштем у Женеви.

Генерална скупштина УН је 2001. године признала потребу за мултифазним Светским самитом о информационом друштву (WSIS) и затражила је од Међународне уније за телекомуникације да преузме водећу улогу у координацији и учешћу више заинтересованих страна у тим догађајима.

Прва фаза Светског самита о информационом друштву догодила се у Женеви у децембру 2003. године, а друга фаза одржана је у Тунису 2005. године. После Светског самита о информационом друштву и Конференције опуномоћеника 2006. године, Међународна унија за телекомуникације преузела је важну улогу у координацији изградње поверења и сигурности у коришћењу података и комуникационе технологије (ИКТ). Циљеви Светског самита о информационом друштву, усвојени 2005. године у оквиру Агенде из Туниса, дефинисани су на следећи начин:„Ми потврђујемо да су предузете мере у циљу веће стабилности Интернета и сигурности, приликом борбе против сајбер криминала и сузбијања спама, штитећи и поштујући одредбе о приватности и слободи изражавања у складу са релевантним одредбама Универзалне декларације о људским правима и Женевске декларације (став 42)." „Позивамо власти да сарађују са другим заинтересованим странама и развијају неопходно законодавство везано за истрагу и кривично гоњење сајбер криминала, угледајући се на постојеће оквире, на пример UNGA резолуције 55/63 и 56/121 о борби против злоупотребе информационих технологија и регионалне иницијативе, која укључује, али не ограничава Конвенцију Савета Европе о сајбер криминалу " (став 40).

ITU је покренуо Глобалну агенду о сајбер безбедности (GCA) у мају 2007. године као глобални оквир за дијалог и међународну сарадњу ради предлагања стратегије за проналажење решења и побољшање безбедности у информационом друштву. GCA представља оквир за предлагање стратегије за стицање поверења и побољшање сигурности у информационом друштву, а под окриљем сајбер безбедности.У циљу помоћи ITU’s генералне безбедности у развоју стратешких предлога држава чланица, глобална високо позиционирана експертска група (HLEG), коју чини 100 стручњака, основана је у октобру 2007. године.Та експертска група је у августу 2008. године усвојила председников извештај с препорукама, укључујући ту и правне прописе о сајбер криминалу. Глобални стратегијски извештај достављен је у новембру 2008. године и садржи стратегије у пет области рада:

законске мере, техничке и процедуралне мере, организациону структуру, изградњу капацитета и међународну сарадњу.

Међународна унија за телекомуникације (ITU) је у 2011. години објавила књигу професора Марка Герцкеа (*Marco Gercke*) *Разумевање сајбер криминала: појаве, изазови и правни одговори*. Та књига сматра се најистакнутијом презентацијом сајбер криминала у свету данас.HIPCAR пројекат „Јачање конкурентности на Карибима кроз усклађивање ИКТ политика, законодавство и регулаторне процедуре" покренуле су у децембру 2008. године Међународна уније за телекомуникације (ИТУ) и Европска унија. Пројекат представља сарадњу и са Секретаријатом Карибске заједнице (CARICOM) и Карибске уније за телекомуникације (ЦТУ) као део глобалног ITU-EC-ACP пројекта. Овај пројекат завршен је у септембру 2013. године.На тај начин подржаће се HIPCAR државе кориснице, CARIFORUM, који чине 15 независних држава у региону Кариба, а затражио је ову помоћ, укључујући и препоруке и смернице које се односе на модел закона о сајбер криминалу.

Основане су регионалне радионице, посебно радионице за сајбер криминал (е-криминал). Предвиђена су следећа кажњива дела: незаконит приступ, недозвољено пресретање података, недозвољено коришћење података, шпијунажа, недозвољено ометање система, употреба недозвољених уређаја, компјутерски фалсификат, компјутерска превара, дечија порнографија, крађа идентитета, спам, објављивање детаља истраге и узнемиравање коришћењем средства електронске комуникације.

Земље кориснице овог HIPCAR пројекта су: Антигва и Барбуда, Бахами, Барбадос, Белизе, Доминиканска Република, Гренада, Гвајана, Хаити, Јамајка, Сент Китс и Невис, Света Луција, Свети Винсент и Гренадини, Суринам и Тринидад и Тобаго. Све наведене државе су потписнице ACP-EC Конвенције.

6.2.6. Удружење земаља Југоисточне Азије

Удружење земаља југоисточне Азије (ASEAN) основано је на министарском састанаку о транснационалном криминалу (AMMTC). На састанку у Бангкоку 8. јануара 2004. године закључено је да је неопходна ефикаснаправна сарадња у борби против транснационалног криминала и сајбер криминала.

План за спровођење заједничке декларације АСЕАН и Кине о стратешком партнерству за мир и просперитет потписан је 8. октобра 2003. године на Балију, у Индонезији. Удружење земаља југоисточне Азије (ASEAN) и Кина наставиће следеће заједничке акције и мере: формулисати сарадњу и процедуру за хитно реаговање у циљу одржавања и унапређења сајбер безбедности, као и превенцију и борбу против сајбер криминала. У саопштењу из Регионалног форума АСЕАН (АРФ) из јула 2006. године истакнуто је да: „Верујући да ефикасна борба против сајбер напада и терористичке злоупотребе сајбер простора захтева повећано, брзо и добро функционисање правних и других облика сарадње."

ARF државе чланице и организација настоје да донесу, ако то до сада нису учиниле, и имплементирају норме о сајбер криминалу и сајбер безбедности у складу са својим националним условима и позивајући се на релевантне међународне инструменте и препоруке/упутства за спречавање, откривање, смањење и ублажавање напада, укључујући ту и десет препорука из Резолуције Генералне скупштине УН 55/63 о борби против злоупотребе информационих технологија. ARF државе чланице и организација признају значај националног оквира за сарадњу у борби против криминала, укључујући ту и тероризам, злоупотребу сајбер простора и подстицање одређења оквира који може укључивати.

Министри земаља чланица Удружења земаља Југоисточне Азије и Кине с одговорношћу за сарадњу у борби против транснационалног криминала састали су се у Брунеју у новембру 2007. године. Сложили су да је Меморандум о разумевању (МоУ) Удружења земаља Југоисточне Азије и Кине потребно ревидирати у складу с новим изазовима.Заједничко саопштење, које укључује и Кину, Јапан и Републику Кореју, усвојено је на следећи начин: „Оджали смо размену мишљења о јачању АСЕАН + 3 сарадње у борби против транснационалног криминала који се фокусира на развој изазова сајбер криминала и његових јаких веза до другог транснационалног криминала на пример тероризма и трговине-људима."Заједничко саопштење начелника Полицијске конференције у Брунеју у мају 2008. године подразумева залагање за усвајање резолуције о сајбер криминалу. Шефови полиције Удружење земаља југоисточне Азије састали су се у Ханоју, у Вијетнаму у мају 2009. године. Конференција је усвојила резолуције, укључујући и оне везане за сајбер криминал: „8.7.1. Треба наставити да се подстичу државе чланице да преиспитују потребу за основним одредбама закона о сајбер криминалу и обезбедити доношење таквих закона, ако је потребно."

Министарски скуп за телекомуникације и информационе технологије одржан је у Виентианеу, у Лаосу у октобру 2009. године. Седми министарски састанак Удружења земаља југоисточне Азије о транснационалном криминалу у Siem Reap, Камбоџа, 17. новембра 2009. године прогласио је потребу за консолидовањем и даље јачање регионалне сарадње у борби против транснационалног криминала. Такође је једногласно поздрављено потписивање ревидиране АСЕАН Киног Меморандума о разумевању (MoU) и сарадњи у области нетрадиционалних безбедносних проблема.

Осми министарски састанак о транснационалном криминалу Удружења земаља југоисточне Азије одржан је у Балију, у Индонезији, 10. и 11. октобра 2011. године у циљу консолидовања и јачања даље регионалне сарадње у борби против транснационалног криминала. Министри су истакли да се сајбер криминал шири рапидно, па се јавља потреба за појачаним напорима и сарадњу у сузбијању овог вида криминала.

31. конференција начелника полиције у оквиру Удружења земаља југоисточне Азије (ASEANAPOL) одржан је у Vientiane, Лаос, од 30. маја до 3. јуна 2011. године. Сарадња с ИНТЕРПОЛ-ом у региону као глобалног комплекса (IGC) у Сингапуру, омогућио би ASEANAPOL-у да реагује на изазове које задаје сајбер криминал.

Састанак високих званичника Удружења земаља југоисточне Азије о транснационалном криминалу (SOMTC) је усвојио закључак да будући рад треба да обухвати обавезне планове рада у борби против транснационалног криминала који се састоји од пројеката и активности на кључним областима као што су борба против тероризма, трговине људима и сајбер криминала.

6.2.7. Организација за економску сарадњу и развој

ОЕЦД је прва међународна организација која је иницирала смернице за сајбер криминал. Организација се фокусирала више на сајбер безбедност и промовисала је глобални координисан приступ политици изградње поверења. ОЕЦД Радна група за информисање и приватности (WPISP) развила је међународне смернице.

Организација за економску сарадњу и развој (ОЕЦД) усвојила је 2002. године нове препоруке за безбедност информационих система и мрежа. Овај приступ критике заштитне информационе инфраструктуре је смерница и као таква не обавезује државе чланице.OECD Глобални форум о информационим системима и мрежној безбедности одржан је 2003. године у Ослу, Норвешка. Радионица о сајбер криминалу организована је у сарадњи с овим форумом. OECD Радна група за спам основана је 2004. године и доставила је извјештај у 2006. години.Заједничка APEC-OECD радионица о сигурности информација одржана је у Сеулу 2005. године. Једна од тема радионице била је повезана с промовисањем глобалне невладине борбе. У априлу 2007. године спроведена је APEC-OECD малвар радионица у Манили. OECD је објавио 2008. године извештај пројекта под називом „Студијски рад у вези с онлајн крађом идентитета", којим препоручује развој адекватних противмера за спровођење закона за превенцију, откривање и искорењивање ове појаве. Извештај је обухватио анализу различитих правних приступа крађи идентитета које су усвојиле државе чланице ОЕЦД-а, као и испитивање последица стварања посебног кривичног дела крађе идентитета.

OECD-а је објавила књигу *Компјутерски вируси и други малициозни софтвери: Претња за Интернет економију*. Како су малвер напади у порасту, књига препоручује широк спектар побољшања, између осталог: побољшање законског оквира и јачање спровођења закона. Извјештај о интернет крађи идентитета под називом „OECD-а политички водич за онлајн крађу идентитета" доприноси дефинисању, спознаји облика и метода крађа идентитета, као и препоруке за индустрију и владе о начинима борбе против њих.

OECD и Светска банка сарађивале су у организовању радионица за кохерентност политика у примени ИКТ за развој (ICT4D). Главни закључак радионица да су кључни изазови безбедности јављају због недостатка примене постојећих пракси и непостојања прекограничне сарадње.

6.2.8. Организација Северноатлантског споразума

Комитет за заштиту (CPC) покренуо је рад на заштити критичне инфраструктуре и сачинио је Концепт заштите критичне инфраструктуре 2003. године. Комитет за заштиту организовао је едукациони семинар о заштити кључне инфраструктуре. Комитет о планирању индустрије (IPC) такође је допринео превентивним мерама за заштиту критичне инфраструктуре.

Организација Северноатлантског споразума (*North Atlantic Treaty Organization*- НАТО) је такође била активна у области цивилног кризног планирања. Ургентни Комитет за планирање (SCEPC) помаже државама чланицама у заштити цивилног становништва од терористичких напада против критичне инфраструктуре и одговорна је за координацију цивилне заштита критичне инфраструктуре у SCEPC[276]. Комитет за заштиту цивилне комуникације је одговорна за електронску јавност и нејавне инфраструктурне комуникације, при чему су објављени радови у области цивилних комуникација да би се умањиле последице у вези са сајбер напада.

НАТО је основао Центар за одбрану од тероризма 2008. године[277]. Радионица о сајбер тероризму организована је у Молдавији 12–16. октобра 2009. године. Главни циљ била је обука учесника у идентификовању и процени сајбер претњи, доношење ефикасне одлуке и израда стратегије у борби против сајбер тероризма.

НАТО часопис из 2009 године („The NATO Review magazine". Summer 2009. edition) представља расправу о терористима и организованом криминалу, између којих не постоји јасна подела.

Савезничка команда за трансформацију је у 2010. години поставила оквир за групне интеракције (Framework for Collaborative Interaction -FFCI), који омогућава државама НАТО и приватном сектору да успоставе сарадњу у борби против сајбер напада, који су једна од три највеће претње с којима се суочавају.

Цивилни и војни стручњаци из Русије и НАТО земаља састали су се у Анкари, у Турској, 20. и 21. јуна 2011. године да би разменили искуства и стратегије за различите аспекте заштите критичне инфраструктуре, при чему је наглашен значај заштите од сајбер напада.

Генерални секретар Anders Fogh Rasmussen залагао се у 2012. години за ближу сарадњу с Аустралијом у борби против сајбер криминала, а осврнуо се на пиратерију и друге нове безбедносне претње, као и потписивање споразума о политичком партнерству с аустралијском владом.

[276] The Senior Civil Emergency Planning Committee (SCEPC).

[277] Centre of Excellence Defense Against Terrorism.

Приручник о Међународном закону за сајбер ратовања настоји да испита како постојеће норме међународног права налазе примену за овај нови облик ратовања.Овај приручник не одражава НАТО доктрину, али је израз мишљења групе експерата.

6.2.9 Европска унија

У Европској унији Комисија Европске заједнице је представила 19. априла 2002. године предлог за оквирну одлуку Савета о нападима на информационе системе. Предлог је усвојио Савет 2005. године и обухвата:

члан 2. – Неовлашћен приступ информационим системима
1. Свака држава чланица предузеће неопходне мере да би осигурала да намерни неовлашћени приступ целом информационом систему или његовом делу буде кажњив као кривично дело, барем у случајевима који нису минорни.
2. Свака држава чланица може да одлучи да се понашање из става 1 инкриминише само када је кривично дело учињено кршењем мера безбедности;

члан 3. – Незаконито ометање система
Свака држава чланица предузеће неопходне мере да би осигурала да намерно ометање или озбиљан прекид функционисања информационог система уношењем, емитовањем, оштећењем, брисањем, погоршањем, мењањем, сузбијање или пружање неприступних компјутерских података буду кажњиви као кривична дело када су почињени без овлашћења, барем за случајеве који нису безазлени.

Члан 4. – Неовлашћено ометање података
Свака држава чланица предузеће неопходне мере да би осигурала да се намерно брисање, оштећење, квар, измена, куцање или тумачење неприступачних компјутерских података у информационом систему сматрају као кривична дела када су учињена без овлашћења, барем за случајеве који нису безазлени.

У мају 2007. године Европска комисија разматрала је иницијативу у вези с европским законодавства о крађи идентитета, и то под називом: „Општи принципи о борби против сајбер криминала"(Towards a general policy on the fight against cyber crime).

Комисија је организовала експертски састанак о сајбер криминалу у новембру 2007. године. Састанак представља следећи корак Европске уније у спровођењу опште политике коју је навела Комисија. Саопштење гласи овако:

„Повећање сајбер криминала широм Европе, које обухвата нападе великих размера у Естонији, крађу идентитета у Шпанији, илегални садржај и онлајн злостављања деце у Аустрији, Немачкој, Италији и Великој Британији, указује на потребу за успешно усаглашеном акцијом. Случајеви као што су 'Случај Коала' и глобална потрага за 'Vico' педофилима зависи од регионалне и међународне сарадње. Закључци састанка представљају важан корак ЕУ ка успостављању сарадње којом се гради успех."

Одлука о изменама и допунама одлуке 2002/475 ЈХА о борби против тероризма је припремљена у 2008. години. Она ће обухватити три нова кривична дела у законодавству ЕУ: јавно провоцирање за вршење терористичких дела, врбовање за тероризам, као и обуку за тероризам.

Савет министара Европске уније усвојио је у новембру 2008. године стратегију савета да се појача борба против сајбер криминала. Нова стратегија препоручује:„Јачање партнерства између полиције и приватног сектора допринеће бољој размени знања о методама истраге и трендовима у области сајбер криминала. Такође, охрабрују се обе стране да брзо реагују на информације, прибегавају удаљеним претрагама, сајбер патролама за онлајн праћење криминалаца и заједничким истрагама преко граница.

Комисија Европске уније је 2009. године донела информатор о заштити критичне информационе инфраструктуре (ЦИИП) под називом „Заштита Европе од великих сајбер-напада ".

EU–U. S. самит одржан је 20. новембра 2010. године у Лисабону, Португалија. У заједничком саопштењу лидера Европске уније и Сједињених Америчких Држава, укључује оснивање EU–U.S радне групе за сајбер криминал.

Комисија Европске уније је 30. септембра 2010. године представила Предлог директиве о нападима на информационе системе. Комисија такође планира одржавање обуке из области истраге у вези са сајбер криминалом.

Такође, Комисија помаже Европолу и државама чланицама да спроведу Европску платформу упозорења на прекршаје у вези с интернетом који ће омогућити удруживање извештаја о сајбер криминалу почињеном у различитим државама чланицама. Савет Европске уније усвојио је 2010. године закључак Акционог плана за спровођење заједничке стратегије у борби против сајбер криминала.

Сајбер вежба Атлантик одржана је у Бриселу 3. новембра 2011. године као тест одговор на сајбер инциденате, укључујући ту и напад на супервизорску контролу и прикупљање података (SCADA) система у ЕУ.

Предлог Директиве Европског парламента и Савета о нападима на информационе системе (Directive of the European Parliament and of the Council on Attacks against Information Systems) , 2005/222JXA, представљена је 30. маја 2010. године с изменама с презентације ЕУ комисије из 2010. године.

Нацрт закључка Савета Европске уније о успостављању европског центра за сајбер криминал (European Cybercrime Centre -EC3) представљен је 4. јуна 2012. године.

Директива Европског парламента и Савета 2013/40/ЕУ 12. августа 2013. године (Directive 2013/40/EU of the European Parliament and of the The Council of 12. August 2013), о нападима на информационе системе и замене Оквирна одлука Савета 2005/222 / JXA, усвојена је и ступила на снагу двадесетог дана након њеног објављивања у „Службеном листу" Европске уније. Прва Европол-ИНТЕРПОЛ-сајбер конференција одржана је 24. и 25. септембра 2013. године. Европска комисија одлучила је да оснује EC3 у оквиру Европола у Хагу, који је званично отворен 1. јануара 2013. Центар је намењен да буде кључна тачка у борби против сајбер криминала Европске уније да би државе чланице биле подржане у изградњи оперативних и аналитичких капацитета за истрагу и сарадњу с међународним партнерима.

6.2.10. Комонвелт

У настојању да се хармонизује сајбер право у државама Комонвелта, модел закона је усвојен на Конференцији министара у 2002. године. Модел закона, под називом Закон о

компјутерском криминалу, дели исти оквир као Конвенција Савета Европе о сајбер криминалу. Модел закона служи као пример заједничких принципа које свака држава може користити да се усвоји оквирни закон који је компатибилан с другим државама Комонвелта.

Састанак високих званичника из Комонвелта одржан је у октобру 2007. године и односи се на законе за борбу против тероризма и прања новца.

Трећи државни тренинг програм, који је одржан 15–20. јуна 2009. године у Малти, намењен је стварању правног оквира за информационе и комуникационе технологије. Циљ ове обука је и да обезбеди разумевање најбитнијих питања и савременог међународног дијалога о питањима као што су радио-дифузија и интерконекција, управљање интернетом, сајбер криминалом и надлежности.Високотехнолошка конференција за полицију и тужиоце у 15 карипских земаља одржана је 28–29. августа 2009. године у Бермудима.Министри Комонвелта састали су се 11–14. јула 2011. године у Сиднеју, Аустралија. Министри из 44 државе присуствовали су састанаку намењеном акутелним питањима с којима се тренутно суочавају државе чланице, укључујући ту и сајбер криминал. Министри су донели следеће закључке:

„а. Признати као озбиљну претњу сајбер криминал за националну безбедност и спровођење закона у свим земљама Комонвелта;

б. Секретаријат Комонвелта је сачинио мултидисциплинарну радну групу експерата како би сагледала практичне импликације сајбер криминала у заједници и идентификовала најефикасније средство међународне сарадње и спровођења, узимајући у обзир, између осталог, Конвенцију Савета Европе о сајбер криминалу, без дуплирања рад других међународних тела; и

ц. радне групе сарађују са другим међународним и регионалним телима са циљем да се идентификују најбоље праксе, едукативни материјал и програми обуке за истражитеље, тужиоце и судске службенике.”

Комонвелта Радну групу експерата основао је Секретаријат Комонвелта. Група се састала пет пута од јануара 2012. до маја 2013. године, а извештај је завршен у јулу 2013. године.

На састанаку министара Комонвелта у Gaborone, Боцвана, одржаном 5–8.маја 2014. године, усвојен је извештај Радне групе експерата Комонвелта о сајбер криминалу. Извештај

Радне групе првобитно је завршен у јулу 2013. године и разматрали су га високи званичници и министар Комонвелта у септембру 2013. године.

6.2.11. Азијско-пацифичка економска сарадња

Министри и лидери Азија Пацифик економске сарадње (Asia Pacific Economic Cooperation -APEC) на састанку у 2002. години саопштили су: „Тежња је да се донесе свеобухватан сет закона који се односе на сајбер и компјутерски криминал, а у складу су с одредбама међународних правних инструмената, укључујући ту и Резолуцију Генералне скупштине Уједињених нација 55/63 (2000) и Конвенције о сајбер криминалу (2001) до октобра 2003. године."

Радна група за е-безбедност основана је 2003. године. У заједничкој изјави на министарском састанку у Сантијагу, Чиле, у новембру 17–18. 2004. године, договорено је да се ојача економска способност да се бори против високотехнолошког криминала доношењем домаћег законодавства у складу с одредбама међународних правних инструмената, укључујући ту и Конвенцију о високотехнолошком криминалу (2001) и релевантним резолуцијама Генералне скупштине Уједињених нација.

На састанку APEC Радне групе за телекомуникације и информације, одржаном 5–9. септембра 2005. године у Сеулу, у Кореји, дато је саопштење: „Економије тренутно спроводе сајбер законе и залажу се за њихово доношење у складу с Резолуцијом Генералне скупштине УН 55/63 (2000) и Конвенцијом о сајбер криминалу (2001). ТЕЛ иницијатива сајбер законодавства и спровођење Пројекта изградње капацитета подржаће институције да спроведу нове законе."

На министарском састанку у новембру 2005. године министри су обновили посвећеност наводећи да: „Треба подстаћи све економије да проуче Конвенцију о високотехнолошком криминалу (2001) и настоје да донесе свеобухватан сет закона који се односе на сајбер и компјутерски криминал који су у складу са међународним правним инструментима, укључујући ту и Резолуцију Генералне скупштине Уједињених нација 55/63 (2000) и Конвенцију о сајбер криминалу (2001)."

Заједничка APEC-OECD радионица о безбедности информисања одржана је у Сеулу 2005. године, где су између осталог разговарали о промовисању глобалног одговора на

инциденате. У априлу 2007. године спроведена је APEC-ASEAN радионица у Манили.Председнички извештај Управе Радне групе за телекомуникације и информације презентован је на седмом APEC министарском састанку у Бангкоку 23. априла 2008. године, укључујући ту и безбедносна питања и пројекте сајбер криминала.

APECTEL је организовао програм обуке за борбу против високотехнолошког криминала и промовисао је сајбер безбедност на 3. дану конференције у Малезији у децембру 2008. године. Радна група за телекомуникације и информације (ТЕЛВГ) представила је нацрт плана рада 2009. године на састанку у Сингапуру 18. фебруара 2009. Године. ТЕЛВГ ће радити у правцу многих циљева у 2009. години, од којих је један да се подигне свест о потреби за сарадњом унутар АПЕЦ-а.Сарадња са ОЕЦД наставиће да развија иницијативе у области просперитета сајбер безбедности фокусирајући се на малваре.

6.2.12 Лига арапских држава

Лига арапских држава основана је 1945. године и има 22 државе чланице.Неколико земаља усвојило је законе о сајбер криминалу, као што су Пакистан, Саудијска Арабија и Уједињени Арапски Емирати (УЕА). УЕА је прва земља у региону која је усвојила законе, са Законом о сајбер криминалу бр. 2, у фебруару 2006. године.

Савет за сарадњу у Заливу (GCC) укључује Бахреин, Кувајт, Оман, Катар, Саудијску Арабију и Уједињене Арапске Емирате, и на конференцији у јуну 2007. године препоручио је да GCC земље направе споразум о сајбер криминалу.ITU Регионална радионица за сајбер безбедност и заштиту критичне инфраструктуре (CIIP) и Радионица за сајбер форензику одржане су у Дохи у фебруару 2008. године. Наглашен је значај разматрања националних закона о сајбер криминалу који се односе на претње у сајбер простору и развијање одговарајућих инструмената за борбу против сајбер напада.

Уједињени Арапски Емирати (УАЕ) залажу се за ажурирање закона о сајбер криминалу да би се покриле рупе у закону. Године 2010. одржан је први регионални IPR и Конференција о сајбер криминалу у Јордану. Дискутовано је о већој сарадњи Арапске лиге и изради нових закона. Препоручено је неколико иницијатива за владе и приватне индустрије, укључујући ту и успостављање специјализованих судова за сајбер криминал и доношење нових закона за заштиту корисника и приватних индустрија.

6.2.13. Организација америчких држава

Министри правде Америке у оквиру Организације америчких држава (ОАС) залагали су се у Перуу 1999. године за оснивање групе владиних стручњака о сајбер криминалу. Препоруке су разматране на састанку у Вашингтону 23–24. јуна 2003. године.

Пети састанак министара правде Америке одржан је 28–30. априла 2004. године, када су одобрени закључци и препоруке Генералне скупштине ОАД, укључујући и следеће:„Државе чланице оцењују оправданост спровођења принципа Конвенције Савета Европе о сајбер криминалу (2001), и разматрају могућност приступања конвенцији." Генерална скупштина Организације америчких држава затражила је на састанку 7. јуна 2005. године да стални савет сазове састанак групе владиних експерата о сајбер криминалу. Организација америчких држава, у сарадњи са Саветом Европе и Шпанијом, организовала је конференцију под називом „Сајбер криминал – глобални изазов, глобални одговор" у Мадриду 12–13. децембра 2005. године. На конференцији је, између осталог, закључено:

1. „Признаје се значај јединог међународног уговора у овој области: Конвенције о сајбер криминалу која је отворена за све државе, као и значај јачања међународног правног оквира;
2. треба снажно подстаћи државе да размотре могућност да постану чланице ове конвенције како би имала ефикасне и компатибилне законе и средства за борбу против сајбер криминала, на националном нивоу, а у име међународне сарадње;
3. препознаје се потреба да се спроводи сарадња, пружање техничке помоћи и организовање сличних догађаја у другим регионима света."

Стални савет Организације америчких држава одлучио је 15. децембра 2005. године, да група владиних стручњака о сајбер криминалу треба да заседа 27–28. фебруара 2006. године ради обављања мандата у складу са закључцима и препорукама с петог састанака министара правде, одржаног 28–30. априла 2004. године.

Група владиних експерата о сајбер криминалу састала се у Вашингтону 27–28. фебруара 2006. године, где је истакнуто да је неопхоно остварити приступ, израду и измене закона у складу с принципима, материјалним и процесним правом, а у складу с Конвенцијом Савета Европе о сајбер криминалу (2001).

На шестом састанку министара правде у јуну 2006. године истакнуто је:„[...] Неопходно је ојачати сарадњу са Саветом Европе, тако да државе чланице ОАС могу да размотре примену начела Конвенције Савета Европе о сајбер криминалу и да јој приступе, као и да усвоје законске и друге мере које су потребне за имплементацију. Сходно томе, треба уложити напоре у јачање механизама за размену информација и сарадњу с другим међународним организацијама и агенцијама у области сајбер криминала, као што су Уједињене нације, Европска унија, Форум Азија Пацифик за економску сарадњу, Организација за економску сарадњу и развој (ОЕЦД), Г-8, Комонвелт и Интерпол." Закључци и препоруке прихваћени су на пленарној седници у јуну 2007. године и усвојена је резолуција (AG/RES. 2266 (XXXVII-o/07).

Портал о интерамеричкој сарадњи у области сајбер криминала саставио је постојеће законодавство сајбер криминала држава чланица ОАС.[278]Пети састанак групе владиних стручњака из области сајбер криминала одржан је у новембру 2007. године у Вашингтону, када је постигнут договор о препорукама за јачање и консолидацију сарадње у превенцији и борби против сајберкриминала, с посебним освртом на одредбу 3 и 8: „Државе, које то још нису учиниле, што је пре могуће треба да испитају своје правне системе и усвоје посебан закон и процедуралне мере неопходне за криминализовање различитих модалитета сајбер криминала, обезбеде ефикасну, ефективну и правовремену истрагу и кривично гоњење, као и да омогуће државама да сарађују у истрази и кривичном гоњењу сајбер криминала."(3),„Државе треба да размотре примену принципа Конвенције о сајбер криминалу Савета Еуропе приступајући јој, и усвајањем законских и других мера потребних за њено спровођење."(8) Такође је препоручено да се државе придруже мрежи „24/7 контакт центара групе.

Интерамерички портал о сарадњи у области сајбер криминала саставио је постојеће законодавство о сајбер криминалу држава чланица ОАС[279].Радионица о праву сајбер криминала, у сарадњи са Саветом Европе, одржана је у септембру 2008. године у Боготи, Колумбија. Регионална радионица о сајбер криминалу одржана је у августу 2009. године у Панами.[280] Шести састанак Радне групе за сајбер криминал одржан је 21–22. јануара 2010.

[278] Више о томе:http://www.oas.org/juridico/english/cyber_legis.htm, последњи пут приступили 12.03.2016.године.

[279] op.cit.

[280] http://www.oas.org/juridico/newsletter/lc_en.htm, последњи пут приступили 12.03.2016.године.

године у Вашингтону. Стручњаци су сачинили неколико препорука да се предузму даљи кораци у циљу дефинисања закона о високотехнолошком криминалу и начинима гоњења. Седми састанак Радне групе за сајбер криминал одржан је 6. и 7. фебруара 2012. године у Вашингтону. Техничка радионица која прати шести састанак Радне групе о сајбер криминалу организована је 9–13. маја 2011. године у Мајамију, САД. Радионица о компјутерском криминалу одржана је 11–13. марта 2013. године у Перуу. Сврха је била обука за спровођење закона тужилаца и службеника из Поливија, Чилеа, Колумбије, Еквадора, Панаме и Перуа.

6.2.14 Афричка унија

Афричка унија (АУ), основана 1999. године, предвиђа: „ефикасан форум који би омогућио да све државе чланице усвоје координисане позиције о питањима од заједничког интереса за континенте..."

Маурицијус, Јужна Африка и Замбија усвојиле су законе о сајбер криминалу. Јужноафричка заједница за развој (T*he Southern African Development Community* – SADC) која обухвата Замбију, Зимбабве, Јужну Африку, Малави и Мозамбик, године 2005. покренула је напоре за усклађивање закона о сајбер криминалу.

Источноафрички регион обухвата Танзанију, Кенију и Уганду. Напредак закона о сајбер криминалу је спор на овим просторима, осим у Уганди. Земље источне Африке покушавају да координишу напоре да би закони били слични за сајбер криминал у региону јужне Африке.

AfriNIC је основала своју Радну групу владе (AfGWG). AfGWG, први округли сто за спровођење закона, одржан је 25–26. јануара 2010. године у Маурицијусу.Пет источноафричких држава: Уганда, Кенија, Танзанија, Руанда и Бурунди планирају да оснују компјутерске тимове за реаговање (*Computer Emergency Response Teams* – CERT) у циљу сузбијања сајбер криминала уз помоћ ITU.

Источноафричка заједница (ЕАЦО) планира да усвоји заједничке законе против сајбер криминала уз помоћ агенције Уједињених нација за трговину, UNCTAD. Радна група Источноафричке заједнице за сајбер криминал успостављена је 2010. године.

Први самит западне Африке о сајбер криминалу одржан је 30. новембра – 2. децембра 2011. године у Абуји, Нигерија. Разматрано је неколико домаћих и међународних стратегија сајбер криминала, укључујући ту и јачање међународне сарадње и развијање регионалних планова за борбу против високотехнолошког криминала.Други годишњи јужноафрички самит о сајбер криминалу одржан је 29–30. новембра 2011. године у Кејптауну. Влада Камеруна је 2011. године у Парламенту предложила нов закон о сајбер криминалу. Предлог закона дефинисаће главне облике сајбер криминала, укључујући ту и педофилију, порнографију, повреде људског достојанства, ширења лажних гласина и упаде у банкарски систем.

6.2.15. Група осам најразвијенијих земаља (Г-8)

Највећи допринос борби против компјутерског криминала дала је група осам најразвијенијих земаља (Г-8) формирањем такозване Лионске групе. Већ 1996. године у Лиону ова група је представила четрдесет препорука за борбу против организованог криминала. Након самита у Лиону формиране су специфичне подгрупе, које ће се касније бавити специфичним проблемима повезаним с организованим криминалом (високотехнолошки криминал, трговина људима, дељење доказа у кривичним процесима, имиграцијске преваре и тероризам).

Циљ подгрупе за високотехнолошки криминал био је да повећа могућности земаља чланица да спрече, истраже и процесирају злочине у вези с компјутерима, мрежама и другим новим технологијама. Већ 1997. године усвојено је десет принципа за борбу против компјутерског криминала, као и десет ставки акционог плана. Циљ је био да се осигура да кривична дела компјутерског криминала не налазе уточиште било где у свету. Кључни моменти у раду те групе су: креирање глобалног (тренутно 40 чланова) директоријума за критичне информације (директоријум је доступан само владиним институцијама земаља чланица), разни документи о најбољој пракси (упутства за сигурност компјутерских мрежа, интернационални захтеви за подршку, глобално праћење комуникација и др.) и одржавање конференција за обуку националних служби безбедности, а у вези с компјутерским криминалом.

На састанку Г-8 министара правосуђе и унутрашњих послова у Вашингтону, 10–11. маја 2004. године, издато је следеће саопштење: „Наставити са ојачавањем домаћих закона.

Уз Конвенцију Савета Европе о сајбер криминалу, која је ступила на снагу 1. јула 2004. године, требало би да предузму кораке да охрабре усвајање правних стандарда који се налазе на широкој основи."

У саопштењу са састанка Г-8 у 2005. години као циљ је истакнуто:

„Да се обезбеди да агенције за спровођење закона могу брзо да одговоре на озбиљне сајбер претње и инциденте." На састанку у Москви 2006. године Г-8 министри за правосуђе и унутрашње послове разговарали су о питањима високотехнолошког криминала и сајбер простора. Самит Г-8 у 2006. години одржан је у Санкт Петербургу, када је и донета Декларација самита о борби против тероризма.На састанку Г-8 министара правде и унутрашњих послова у Минхену 23–25. маја 2007. године делегати су се сложили „да раде на кажњавању у оквиру националних правних оквира, појединих злоупотреба интернета за терористичке сврхе".Г–8 група имала је састанак у Хокаиду 7–9. јула 2008. године, када је представљен извештај Г-8 Самита лидера и експерата о међународном тероризму и транснационалном организованом криминалу.Г-8 група одржала је састанак у Мускоки и у Канади 2010. године, када су придодате одредбе о тероризму и организованом криминалу.Године 2011. група Г-8 одржала је састанак у Довилу, у Француској. Довилска декларација обухватила је и део који се односи на интернет.

6.2.16 Шангајска организација за сарадњу

Шангајску организацију за сарадњу **(** *The Shanghai Cooperation Organization* -SCO) основале су Кина, Русија, Казахстан и Узбекистан 15. јуна 2001. године Декларацијом о Шангајској организацији.

Савет шефова држава чланица састао се у Душанбеу у августу 2008. године. Позивајући се на забринутост због претњи које се односе на могућност коришћења савремених информационих и телекомуникационих технологија за потребе неспојиве са задацима обезбеђивања међународне стабилности и безбедности, Савет је дао следећу изјаву: [...] Са циљем стварања правног оквира за сарадњу у овој области сматра се да је неопходно да се изради међувладин споразум у СЦО оквиру у области међународне безбедности информација."

Јекатеринбуршка декларација од 16. јуна 2009. године укључила је следећу изјаву:

„СЦО чланице наглашавају значај питања обезбеђивања међународне информационе безбедности као један од кључних елемената заједничког система међународне безбедности."

Одржан је редовни састанак Савета шефова влада држава чланица СЦО у Пекингу 14. октобра 2009. године. Шефови влада потврдили су да у тренутним условима научна и технолошка сарадња доприносе јачању способности држава чланица СЦО у суочавању с глобалним изазовима и претњама.Декларација са 10. састанка Савета шефова држава чланица одржан је 10–11. јуна 2010. године у Ташкенту.

Десетогодишњица СЦО прослављена је на састанку Савета шефова држава чланица, који је одржан у Астани 14–15. јуна 2011. године.На састанку Савета шефова држава чланица 2012. године дата је следећа изјава:„SCO ће се борити против тероризма, сепаратизма и екстремизма, као и међународног сајбер криминала."

6.3. МЕЂУНАРОДНА САРАДЊА У ОБЛАСТИ САЈБЕР КРИМИНАЛА

Изазови које намеће сајбер криминал налажу допуњавање традиционалних канала сарадње. Конвенција о сајбер криминалу је у члану 35. предвидела постојање мреже 24/7: „Свака чланица треба да одреди место за контакте, које ће бити доступно 24 сата свих 7 данау недељи, а да би омогућила моменталну помоћ у истражне сврхе или за процедуре у вези с кривичним делима која се односе на компјутерске системе и компјутерске податке или ради прикупљања доказа за кривична дела у електронском облику."

Успостављање мреже 24/7 заснива се на искуству стеченом из рада мреже коју је створила организација Г-8, а коју је координисало Министарство правде САД 1998. године ради олакшавања добијања податка доступних у другој држави у хитним случајевима.[281] САД, Француска и Италија биле су међу првим државама које су успоставиле контакт-центре.

Конвенција о сајбер криминалу није прописала у оквиру ког државног органа или институције ће функционисати контакт-центри мреже 24/7. Државе чланице које су основале

[281] Више о томе:http://www.oas.org/juridico/english/cyb20_network_en.pdf, последњи пут приступили 12.03.2016.године.

контакт-центре определиле су се за полицију, тужилаштво, комбинацију тих органа или специјализоване органе. Контакт-центри се у већини држава налазе у оквиру Министарства унутрашњих послова, криминалистичке полиције или националне полиције. Овакви модели контакт-центара успостављени су у следећим држава: Албанији, Јерменији, Аустралији, Аустрији, Белгији, Босни и Херцеговини, Бразилу, Бугарској, Канади, Чилеу, Кипру, Чешкој, Данској, Доминиканској Републици, Естонији, Финској, Француској, Немачкој, Хонг Конгу, Мађарској, Исланду, Индији, Индонезији, Израелу, Италији, Јамајки, Јапану, Лихтенштајну, Литванији, Луксембургу, Малезији, Малти, Маурицијусу, Мексику, Мароку, Намибији, Холандији, Новом Зеланду, Пакистану, Перуу, Филипинима, Португалији, Румунији, Руској Федерацији, Србији, Сингапуру, Словачкој, Словенији, Шпанији, Шведској, Тајвану/Кинеском Тајпеју, Тајланду, Тунису и Великој Британији.[282]Естонија, Финска, Исланд и Холандија искористиле су националне канцеларије Интерпола као контакт-центар мреже 24/7. На тај начин избегнута је употреба контакт-тачке за различите намене, олакшана је координација и специјализација у међународној сарадњи. Република Србија као потписница Конвенције о сајбер криминалу успоставила је контакт-центар доступан 24 сата сваког дана у недељи у оквиру Националног централног бироа Интерпола.

Контакт-центри основани у тужилаштву налазе се у оквиру Одељења за правосуђе, што омогућава успешније спровођење правосудне сарадње или извршавање захтева за узајамну правну помоћ. Ови типови контакт-центара заступљени су у: Републици Конго, Кореји, Румунији, Јужноафричкој Републици, Македонији и САД.[283]

Државе попут Нигерије и Норвешке успоставиле су хибридне облике контакт-центара. Норвешки контакт-центар мреже 24/7 налази се у оквиру криминалистичке полиције и поседује тужилачка овлашћења, па је надлежан за узајамну правну помоћ током припремног поступка. Иако овај модел изгледа као најефикасније решење јер комбинује предности претходна два модела, његово постојање не може да буде компатибилно с кривично-правним системом многих држава.

Модел постојања два контакт-центра у једној држави може ефикасно функционисати у неким државама и олакшати сарадњу између полиције и тужилаштва. Пример овог модела

[282] Више о томе:www.coe.int/cybercrime, последњи пут приступили 12.03.2016.године.

[283]Више о томе:www.coe.int/cybercrime, последњи пут приступили 12.03.2016.године.

можемо наћи у Румунији, где се један контакт-центар налази у оквиру тужилаштва при Врховном касационом суду као Канцеларија државног тужиоца која је формално успостављена законом, а други у оквиру криминалистичке полиције. Предности овог модела контакт-центра су што полиција може да искористи своје канале и инструменте, а тужилац може да нареди чување и да буде задужен за узајамну правну помоћ. Лоше стране овог модела контакт-центра су дуплирање захтева, сукоб надлежности, пролиферација контакт-центара и збуњивање странака.

Постоје и становишта да контакт-центри мреже 24/7 не треба да буду при полицијским или тужилачким органима, већ да се налазе унутар обавештајне службе или Центра за сајбер криминал (CERT). Проблем настаје јер контакт центар једне државе тешко може да се укључи у пуну сарадњу с другачијом врстом контакт-центра друге државе.У Бразилу и Намбији контакт-центар постоји као сајбер форензички сервис. Предности овог модела контакт-центра је тимски рад, тј. сарадња лица ангажованих у вођењу истраге, форензичке аквизиције, анализе доказног поступка и презентације дигиталних доказа на суду. Овај контакт-центар је специјализован субјекат који ће ефикасно омогућити помоћ другим државама када је су у питању поврат и анализа обрисаних, скривених и привремених датотека, а које у свакодневном раду нису видљиве. Међутим, овај контакт-центар је уклоњен из полицијских операција и на тај начин онемогућен да покрене хитну акцију. Конвенција о сајбер криминалу одобрава постојање овог облика контакт-центра уз испуњење услова сарадње с органима надлежним за међународну узајамну помоћ или екстрадицију: ,,Уколико место за контакте које је одредила једна чланица није део овлашћених органа задужених за међународну узајамну помоћ или екстрадицију, то место за контакте мора да гарантује да с тим органима може експедитивно да сарађује.”

Не постоји једнообразност у структури и начину рада контакт-центара мреже 24/7. Конвенција о сајбер криминалу у члану 35, став 3 прописује да: ,,Свака чланица треба да обезбеди увежбано и обучено особље да би мрежа могла да функционише.”

Број запослених службеника у контакт-центру не само да показује велике варијације, већ и две различите врсте концепата структуре контакт-центра: контакт центар мреже 24/7 у Бугарској, Републици Конго, Хрватској, Италији, Румунији, Шпанији или Македонији обухвата од једног до три стручњака. Одговорне особе у контакт-центру је могуће препознати, чиме се олакшава лични контакат, умрежавање и стварање међусобног поверења. Радно време контакт-центра износи углавном 8 сати, након чега одговорна лица

имају обавезу да одговарају на позиве или мејлове. Како је сарадња мање институционализована, могу се јавити проблеми, нарочито у хитним случајевима, због заузетости одговорног лица или ако на други начин постане недоступно. У другим државама контакт центар функционише као канцеларија специјализована за сајбер криминал и обухвата много више службеника. Контакт центри у Мађарској (11 службеника), Холандији (30 службеника), Норвешкој (40 службеника), САД (40 службеника) и Француској (55 службеника) обезбедили су рад стручних службених лица у било које време, као и висок ниво специјализације и обуке.[284]

Може се закључити да су државе које су прихватиле концепт анонимне институције и неперсонализовања стручњака много мање укључене у рад мреже 24/7. Зато се чини да је најефикасније и најодрживије решење да се, поред контакт-података канцеларије, обезбеде и контакт-подаци одговорних службених лица ради успостављања директног контакта. Било који од та два концепта да се одабере, државе чланице треба да обезбеде доступност одговорних лица 24 часа 7 дана у недељи да би били у могућности да по потреби укажу помоћ. Такође, стална доступност одговорних лица допринеће да се преброде временске разлике између држава (нпр., ако се открије сајбер напад у подне у Токију, конзервирање података биће неопходно у компјутерском систему САД у 22 часа).

Употреба паметних телефона или таблет рачунара с UMTS или HSDPA мрежом, које омогућавају брзину протока информација и до више мегабита у секунди, у раду мреже 24/7 налазе широку примену. Такође, функционисање мреже 24/7 незамисливо је без сигурног онлајн приступа свим врстама телекомуникационих мрежа, као и коришћења редундантног рачунарског система са хетерогеним платформама (*Windows*/*Linux*) с високом пропусном моћи мреже. Овај систем, који поседује алтернативе за све сегменте система, омогућује сигурно и експедитивно остваривање комуникације с местом контакта друге државе. Конвенција о сајбер криминалу у члану 35. прописује: „Место за контакте сваке чланице мора располагати могућностима довољним да може експедитивно преносити комуницирање са местом контакта друге чланице.” Може се закључити да контакт-центри мреже 24/7 не изискују посебне инвестиције, осим поседовања интернет конекције, факса, фиксног телефона, мобилног телефона, штампача, скенера или сличних уређаја.[285]Коришћење

[284] www.coe.int/cybercrime, последњи пут приступили 12.03.2016.године.

[285]Више о томе: http://www.oas.org/juridico/english/cyb_pry_G8_network.pdf, последњи пут приступили 12.03.2016.године.

експедитивних начина комуникације, у које спадају факс и електронска пошта, оправдано је у хитним случајевима ради испуњења захтева за међусобну помоћ. Примена овог начина комуцирања прихватљива је када постоји одговарајући безбедносни ниво и одговарајућа аутентичност, укључујући ту и коришћење шифровања. На захтев замољене чланице мораће да следи и званична потврда таквог комуницирања, која ће такође бити достављена експедитивним начином комуницирања.

Када је замољеном контакт-центру дозвољено да међусобну сарадњу услови постојањем обостране кажњивости, сматраће се да је тај услов испуњен без обзира на то да ли закони замољене државе стављају тај преступ у исту категорију преступа или га означавају истим терминима као у држави која захтева сарадњу уколико чињење, које је основа преступа у вези с којим се сарадња захтева, представља кривично дело и по њеним законима.Замољени контакт-центар хитно ће обавестити контакт-центар државе која је упутила захтев о исходу извршења захтева за помоћ, као и о сваком разлогу који онемогућава извршење захтева или ће вероватно у значајној мери одложити извршење.

Контакт-центар који упућује захтев може тражити да замољени контакт-центар чува тајност како самог захтева, тако и садржаја захтева до степена неопходног да би се захтев могао извршити. Уколико замољени контакт-центар не може да испуни критеријум тајности, треба одмах о томе да обавести контакт-центар који упућује захтев, који ће затим одлучити да ли ће захтев упркос томе проследити на извршење. Искуства показују да су неки контакт-центри прилично прилагодљиви и не захтевају посебну форму захтева, па су у стању да делују на телефонски позив добијен од контакт-центра друге државе. Многе државе централне, источне и југоисточне Европе захтевају формално потписан и оверен документ. У ту групу држава спадају: Босна и Херцеговина, Бугарска, Хрватска, Црна Гора и Македонија.[286]

Уместо увођења јединствене форме, коју ће уважавати све државе чланице, да би контакт-центри знали унапред како да се обрате, решење је сачињавање „листе" у којој ће се навести услови у погледу форме захтева за сваку државу.

---

[286] Више о томе:http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/points%20of%20contact/aboutpoc_EN.asp, последњи пут приступили 12.03.2016.године.

Сврха контакт центра је да експресно делују ради пружања хитне помоћи другим контакт-центрима у оквиру мреже 24/7 када постоје разлози да се верује да су релевантни подаци посебно подложни губитку или измени.Помоћ контакт-центра мреже 24/7 обухвата:
1) давање техничких савета;
2) конзервирање података и
3) прикупљање доказа, давање информација правног карактера и лоцирање осумњичених.[287]

Способност контакт-тачке да пружи техничке савете и да комуницира с контакт-тачком друге државе по хитном поступку у директној су надлежности већине контакт-центара. Сајбер напади техничког типа, тј. малициозни програми и хакинг технике сваког дана све више се усавршавају, па је потребно примењивати специјалне истражне технике, као што су електронско праћење, пресретање електронских комуникација или други облици надзора. За примену ових техника неопходно је ангажовати квалификованог експерта за информационе технологије, специјалисту за конкретан оперативни систем, програм, платформу, мрежу итд. Уколико контакт-центар, нарочито с малим бројем службеника, не поседује те стручњаке, може да затражи пружање техничких савета од другог контакт-центра.Најважније функције контакт-центра мреже 24/7 су експедитивно конзервирање компјутерских података и експедитивно откривање конзервираних података који се односе на пренос, а у складу с националним процесним правом замољене државе. Реч је о подацима у оперативној меморији, на хард-диску, флеш-картицама, али и подаци који се налазе у трансмисији, нпр., радио-таласи.

Држава која нема могућност да „експедитивно конзервира ускладиштене компјутерске податке" и „експедитивно конзервира и заштити и делимично открије података о преносу" у складу са члановима 16. и 17. Конвенције о сајбер криминалу, биће суочена с великим тешкоћама при учествовању у мрежи 24/7.

Компјутерски подаци су осетљиви, лако се могу уништити, сакрити или на други начин учинити недоступним или неупотребљивим, па чување ових података треба да се одвија на хитан начин и без непотребних формалности. На пример, немачком контакт-центру је потребно 1–3 сата да одговори на захтеве који се односе на чување ускладиштених компјутерских података или откривање сачуваних података, а за приступ сачуваним

[287] Конвенција о сајбер криминалу, Будимпешта 23. новембар 2001.

подацима 1–3 дана, у зависности од количине тражених података. Генерално, време одзива мора да буде прихватљиво у погледу хитне привремене мере и зависи од нивоа сарадње контакт-центра с интернет-провајдером.

У члану 29, став 2 Конвенције о сајбер криминалу таксативно су наведени подаци које захтев за конзервирање ускладиштених компјутерских података мора садржати:
1) орган који захтева конзервирање података;
2) преступ који је предмет кривичне истраге или поступка и сажет резиме чињеница у вези с тим;
3) опис ускладиштених компјутерских података које треба конзервирати и њихове повезаности с преступом;
4) сви расположиви подаци у циљу идентификације лица које поседује, односно чува ускладиштене компјутерске податке, као и податке о локацији компјутерског система;
5) разлог због којег је неопходно да се подаци конзервишу;
6) изјава намере чланице да поднесе захтев за узајамну помоћ у циљу претраживања или сличну форму приступа компјутерским подацима, њиховог одузимања, обезбеђивања или откривања.

Контакт-центри у Италији, Холандији и Немачкој, поред испуњења садржине захтева наведених у члану 29. Конвенције о сајбер криминалу, захтевају и налог надлежног органа (тужиоца или судије) за експедитивно конзервирање ускладиштених компјутерских података и експедитивно конзервирање и заштиту, као и делимично откривање података о преносу. [288]

Контакт-центри у Бугарској, Данској, Француској, Норвешкој, Шпанији или САД врше конзервирање ускладиштених компјутерских података и експедитивно конзервирање и заштиту и делимично откривање података о преносу без претходног судског налога.[289]

Конзервирање ускладиштених компјутерских података и експедитивно конзервирање и заштита и делимично откривање података о преносу не смеју се условљавати постојањем обостране кажњивости. Када замољени контакт-центар сматра да би се конзервирањем

[288] Више о томе:www.coe.int/cybercrime, последњи пут приступили 12.03.2016.године.

[289]Више о томе:http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20study4-Version7%20provisional%20_12%20March%2008_.pdf, последњи пут приступили 12.03.2016.године.

онемогућила будућа доступност података или сматра да би се тиме угрозила тајност или други аспекти истраге коју води држава која захтев упућује, он мора о томе одмах да обавести контакт-центар који захтев упућује, а који ће затим да одлучи да ли ће и поред тога тражити испуњење свог захтева.Захтев за конзервирање компјутерских података може да буде одбијен само у следећим случајевима:

1. када се захтев односи на преступ који замољена држава сматра политичким преступом или сматра да је у вези с политичким преступом, или
2. када замољена држава сматра да извршење захтева може угрозити њен суверенитет, безбедност, јавни ред или друге битне интересе.[290]

Контакт-центри мреже 24/7 надлежни су и за експедитивно откривање конзервираних података који се односе на пренос. Експедитивно откривање конзервираних података који се односе на пренос има великог значаја за сајбер кривична дела учињена било којим видом нетехничког сајбер напада, као што је социјални инжењеринг, тј. акт манипулације којим се људи наводе да одају поверљиве информације.Уколико се приликом извршавања захтева за конзервирање података који се односе на пренос одређеног комуницирања открије да је давалац услуга из друге државе умешан у пренос тог комуницирања, замољени контакт-центар одмах ће контакт-центру државе која је захтев упутила открити довољно података о том преносу и путању којом је комуницирање обављено да би се тај давалац услуга могао идентификовати.

Значајну улогу контакт-центар има у прикупљању доказа, тј. утврђивању времена када су компјутерски подаци били унети, модификовани, дистрибуирани, коришћени, ускладиштени, склоњени, као и времена када су фајлови били креирани, постављени, пуњени, модификовани или када им се приступило.

Пружање информација правног карактера је у духу Конвенције о сајбер криминалу која одређује да контакт-центри треба „међусобно да сарађују у најширем могућем обиму". Контакт-центри треба да пруже информације правног карактера другим контакт-центрима, као што су, на пример, савети о законским условима потребаним за пружање неформалне или формалне сарадње.

[290] Конвенција о сајбер криминалу, Будимпешта 23. новембар 2001. (члан 27, ст. 4).

Даље, сарадња контакт-центара у оквиру мреже 24/7 често је неопходна у случају идентификације осумњичених, што представља повезивање IP адресе (енгл. *Internet Protocol address*) или имејл адресе с особом или локацијом. Подаци о кориснику интернета (идентитет, адреса, број телефона, врста комуникацијских услуга које је користио, техничке услуге и временски период коришћења услуга) могу се добити од интернет-провајдера. С тим у вези, рад мреже 24/7 је немогуће замислити без активне сарадње контакт-центара мреже 24/7 с интернет-провајдерима. Информација о локацији осумњиченог је поверљиве природе, заштићена националним прописима и контакт-центри ће моћи да обезбеде такву информацију неформално само у ретким приликама. Често је за спровођење ове мере потребан званичан захтев од иностраног контакт-центра или другог надлежног органа (захтев од тужиоца или судије), а у складу са чланом 31. Конвенције о сајбер криминалу.

Поред одговарања на упућен захтев, контакт-центар може самоиницијативно да другом контакт-центру проследи информације до којих је дошао у оквиру сопствених истрага. Откривање тих информација контакт центру друге државе помоћи ће у покретању или вођењу истраге или других процедура које се тичу кажњивих дела сајбер криминала, или би могло водити томе да контакт-центар те државе упути захтев за међусобну сарадњу. Пре него што достави такве информације, у границама свог националног права, контакт-центар који их доставља може захтевати да оне буду чуване у тајности или да се могу користити само под одређеним условима.

Контакт-центар у САД спада у најактивније учеснике мреже 24/7 и послао је више од 80% од укупног броја послатих захтева, а примио је више од 50% од укупног броја примљених захтева. То није изненађујуће с обзиром на велику погођеност САД сајбер криминалом. Ова држава искористила је ефикасан механизам за сарадњу с другим државама и остале погодности мреже 24/7. Најупечатљивији напредак у борби против сајбер криминала је међународна сарадња САД и Кине, јер су управо те државе извориште сајбер криминала.[291] Осим тога, САД су пуно уложиле у усавршавање свог контакт центра на тај начин што су ангажовале око 40 стручњака из области сајбер криминала.

[291] Више о томе:http://www.engadget.com/2015/04/13/dhs-china-cyber-security/, последњи пут приступили 12.03.2016.године.

У Европи најактивнији контакт-центри у смислу броја примљених и послатих захтева за међународну сарадњу у области сајбер криминала налазе се у Бугарској и Холандији.[292] Број послатих и примљених захтева од стране већине контакт-центара прилично је скроман и броји мање од десет захтева годишње, чак и међу државама врло угроженим сајбер криминалом, као што су Француска, Италија, Румунија или Шпанија.

Државе које су ратификовале Конвенцију о сајбер криминалу, али не могу да се похвале бројем послатих и примљених захтева јесу Албанија, Јерменија, Босна и Херцеговина, Словенија и Република Македонија. [293]

Многи сматрају да је Србија технолошки заостала држава. Међутим, Србија броји 2,85 милиона корисника интернета и по сајбер криминалу, а нарочито по преварама путем интернета налази се у светском врху. У Републици Србији је међународна правна помоћ регулисана Законом о пружању међународне правне помоћи у кривичним стварима. Овај закон регулише међународну правну помоћ која обухвата: изручење окривљеног или осуђеног, преузимање и уступање кривичног гоњења, извршење кривичне пресуде и остале облике међународне правне помоћи.

Закон о пружању међународне правне помоћи у кривичним стварима пропустио је да регулише специфичне аспекте пружања међународне правне помоћи у кривичним стварима из области сајбер криминала, у којој је брзина поступања од пресудног значаја за успешно вођење кривичног поступка. [294]Дуго трајање поступка међународне правне помоћи, често по две године и више, обесмишљавало је не само коришћење овог правног института већ и самог кривичног поступка.

Република Србија потписала је 16. априла 2005. године у Хелсинкију како Конвецију о сајбер криминалу, тако и Додатни протокол уз ту Конвенцију. Основни значај ове конвенције је формирање посебних државних органа који су специјализовани за борбу против сајбер криминала, укључујући ту и мрежу 24/7. Место за контакте које је доступно 24 сата сваког дана у недељи тренутно је у оквиру Националног централног бироа Интерпола Београд. Национални централни биро Интерпола Београд представља координациони центар

[292] Више о томе:www.coe.int/cybercrime, последњи пут приступили 12.03.2016.године.

[293] Више о томе:www.coe.int/cybercrime, последњи пут приступили 12.03.2016.године.

[294] „Службени гласник РС”, бр. 20/2009.

између организационих јединица МУП-а (посебно Одељења за борбу против високотехнолошког криминала) и ИНТЕРПОЛ-а и страних полиција. Размена информација с осталим националним централним бироима одвија се путем поддиректората Генералног секретаријата у Лиону.[295]

И поред изузетног напретка, још увек су присутни бројни проблеми на пољу глобалних напора у сузбијању сајбер криминала и ефикасне међународне сарадње између контакт-центара мреже 24/7.Први проблем који се јавља јесте ограниченост мреже 24/7. Само државе које су ратификовале Конвенцију о сајбер криминалу моћи ће да искористе ту конвенцију као правни основ узајамне правне помоћи. Дакле, мрежа 24/7 обухвата само пуне потписнице Конвенције о сајбер криминалу.Други проблем јавља се у вези с временом одазива на хитне привремене мере у складу са члановима 29. и 30. Конвенције о сајбер криминалу.

Контакт-центри мреже 24/7 у обавези су да одговоре експресно и у разумном року. Различите државе захтевају различите форме потребног захтева за сарадњу, које варирају од телефонског позива до формалног захтева који су издале судке власти државе која тражи помоћ. Кашњења и тешкоће у раду су честе појаве у погледу хитног деловања за које се тражи формалан захтев од надлежних органа државе која тражи помоћ.

Мрежа 24/7 контакт-тачака користи се у изузетним, посебно хитним случајевима. Постоји сагласност чланица да су то случајеви експедитивног конзервирања компјутерских података и експедитивног откривања конзервираних података који се односе на пренос. Давање техничких савета, давање информација правног карактера, прикупљање доказа и сличне радње сматрају се мање хитним, па се за њих користе други видови међународне сарадње. Многе државе у својим националним законодавствима немају одредбе које се односе на експедитивно конзервирање компјутерских података и експедитивно откривање конзервираних података који се односе на пренос. Државе које немају те одредбе у свом законодавству имају велике тешкоће у остваривању сарадње у оквиру мреже 24/7. Често трајање поступка експедитивног конзервирања компјутерских података и експедитивног откривања конзервираних података који се односе на пренос зависе од нивоа сарадње које контакт-центар мреже 24/7 има с пружаоцима интернет услуга. Проблематичан је и однос

[295] Више о томе: http://www.mup.gov.rs/cms_lat/direkcija.nsf/odeljenje_za_poslove_interpola.h, последњи пут приступили 12.03.2016.године.

мреже 24/7 и надлежних државних органа за међународну сарадњу. Запажа се ограничено ангажовање и да надлежни органи за међународну сарадњу у хитним случајевима сајбер криминала траже помоћ од контакт-центара мреже 24/7.

Мрежа 24/7 успостављена је не као замена традиционалним видовима сарадње или њихова конкуренција, већ као орган који ће допуњавати формалне и неформалне видове сарадње у хитним случајевима. Помоћ контакт-центара мреже 24/7 традиционалним видовима сарадње више је него добродошла с обзиром на то да процес узајамне правне помоћи траје јако дуго. Неретко је потребно чак и више од шест месеци да би се добио формалан одговор на захтев за међународну сарадњу у области сајбер криминала.

Одуговлачење поступка узајамне правне помоћи јавља се због: различитог дефинисања извршења и обима радњи кривичних дела сајбер криминала у законодавствима различитих држава, недовољне обучености полицијских службеника, тужилаца и судија који поступају у предметима сајбер криминала, неусклађености процесних правила у националним законодавствима у погледу истраге кривичних дела сајбер криминала и неусклађености или одсуства механизама међународне правне помоћи.

Помоћ контакт-центара мреже 24/7 свакако ће олакшати рад надлежних органа за међународну сарадњу. Неопходно је да контакт-центри мреже 24/7 постану активнији учесници у међународној сарадњи тако што би добијали копије захтева за међународну сарадњу и, где је то могуће, уз директан контакт обезбедили давање техничких савета, конзервирање компјутерских података, прикупљање доказа, давање информација правног карактера или лоцирање осумњичених лица.

Ова идеја је оправдана јер надлежни органи за међународну сарадњу многих држава добијају бројне захтеве, па није увек могуће захтеву који се односи на сајбер криминал дати већи приоритет него осталим захтевима. Ако би се контакт-центрима мреже 24/7 проследиле копије захтева или замолница за међународну сарадњу, благовремено би се добили подаци које је сачувао провајдер или информације о индентитету особе повезане с IP адресом или би се сачували рачунарски подаци у другој држави, акоји ће користити у даљем раду истражних или судских органа.

Следећи проблем је сличност мреже 24/7 с мрежом националних тимова за рачунарске инциденте (*Computer Emergency Response Teams* – CERTS), па се јавља потреба

за консолидацијом или поједностављењем надлежности тих органа. Као што можемо уочити, ради се о органима различитих регионалних организација Европске уније и Савета Европе, којима је заједнички циљ борба против сајбер криминала. Европска унија је крајем 2010. године усвојила тзв. Европску унутрашњу стратегију безбедности, у којој је један од кључних циљева оснивање центара за сајбер криминал, тзв. CERTS, односно тимова за деловање у хитним случајевима.

Сврха тог центра је да унапреди процену и праћење постојећих превентивних и истражних мера, да подржи даљи развој обуке, као и да успостави сарадњу с Европском агенцијом за безбедност мрежа и информације (ENISA – *European Network and Information Security Agency*), те да сарађује с мрежом националних тимова за рачунарске инциденте (*Computer Emergency Response Teams* – CERTS). Центар за сајбер криминал замишљен је као централна тачка у борби Европске уније против сајбер криминала, па је обавеза сваке државе чланице Европске уније да оснује бар један такав центар.[296]Надлежности Центра за сајбер криминал су: израда стратегија, спровођење истраживања и пружање оперативне подршке. Сврха овог органа је да праћењем и брзом реакцијом на сајбер претње упозорава и штити грађане, владе и корпорације од ризика на глобалној мрежи.

Међутим, овај орган нема надлежност да води истраге у државама чланицама, осим уколико то нека држава чланица жели, тј. на њен изричит захтев моћи ће да спроводи истрагу. За разлику од Центра за сајбер криминал, контакт-центар мреже 24/7 није надлежан за израду стратегија, за спровођење истраживања или праћење ризика које угрожавају кориснике интернета. Центар за сајбер криминал, пак, нема овлашћења која има контакт-центар мреже 24/7, да моментално делује у хитним захтевима за помоћ који се односе на конзервирање компјутерских података, прикупљање доказа и лоцирање осумњичених лица.

[296] Више о томе:http://www.cert.org/, последњи пут приступили 12.03.2016.године.

ЗАКЉУЧНА РАЗМАТРАЊА

Глобалне рачунарске мреже створиле су могућности за нове облике криминала. Појављује се посебан, софистициран, продоран, технички поткован, бескрупулозан, опседнут, понекад осветољубив појединац коме је тешко супротставити се, а још га је теже зауставити. Све чешће не жели да буде сам, већ му је потребно друштво, као што му је неопходна и „публика". Лакоћа „вршљања" сајбер простором даје му осећај моћи и неухватљивости. Ти осећаји нису без основе, јер га је стварно изузетно тешко открити у моменту чињења дела, шта углавном представља и „прави" тренутак за његово идентификовање. Интернет, пак, који је толико рањив и несигуран због огромног броја корисника, отворености и нерегулисаности, идеално је скровиште криминалаца различитог типа.

Преваре као начин извршења сајбер криминала једна су од највећих претњи у сајбер простору. Не изискују посебно знање из области информационих технологија, већ само елоквентност и коришћење хеуристичког размишљања жртве.

Због великог броја жртва ранији облици превара, попут нигеријских превара и класичних спам превара, све више ишчезавају, а њих супституишу нови видови, који уз малвере на софистициран начин преузимају контролу над зараженим рачунаром, што ће допринети да лични подаци жртве буду уновчени на црном тржишту.

Последице тих противправних радњи могу да буду материјалне, нематеријалне у смислу нарушеног угледа или искоришћавања личних података на неприкладан начин, као и трагичне по жртве које се одлучују да окончају свој живот због наизглед безизлазне ситуације.

Деловање државних институција у циљу сузбијања сајбер криминала мора да буде како ***ex-post*** (након сумње да је превара настала или након откривања сајбер превара), тако и ***ex-ante*** (одвраћање од превара, тј. превентивно деловање). У пракси се више јавља потреба за спречавањем ризика од превара, уз констатацију да је превару боље спречити него решавати њене последице.

Једини начин да се одбранимо, тј. да не наседнемо на преваре које вребају на сваком нашем кораку приликом боравка на интернету јесте коришћење здравог разума. Без рационалног понашања и свести о опасностима које сајбер простор носи, сваки безбедносни програм биће узалудан.

Успешно сузбијање сајбер криминала и успостављање безбедности свих корисника информационих технологија подразумевају ревидирање постојећих и доношење нових прописа којима се регулишу област телекомуникација, заштита људских права и интелектуалне својине.

Може се закључити да примена неодговарајуће методологије у изради закона несумњиво представља један од основних разлога због којих је досадашња правна регулатива у овој области била мањкава. Разлоге за такво стање свакако ваља тражити и у чињеници да је реч о криминалу који својом виталношћу и мноштвом појавних облика ставља законодавца у инфериоран положај, тј. он у неравноправној трци стално сустиже инвентивност криминалаца, те изнова формулише правне норме, често анахроне већ у тренутку њиховог доношења. У том контексту, ни српско законодавство није изузетак.

Што се тиче употпуњавања правне регулативе у оквиру које би се одвијала борба против високотехнолошког криминала, потребно је напоменути да се Закон о оптичким дисковима, који у овом тренутку свакако недостаје, не налази чак ни у фази нацрта.

Постојећи закон о организацији и надлежности државних органа у сузбијању високотехнолошког криминала неопходно је изменити на тај начин што ће се проширити стварна надлежност ових органа на сва кривична дела која по начину, средствима и објекту извршења представљају дела из области високотехнолошког криминала, и то не само усредсређена на рачунар већ и на сва средства информационе технологије (нпр., модерне телефоне с приступом интернету).

Уколико би немогућност решавања наведених проблема могла да се оправда и актуелном економском ситуацијом, нерешавање тих проблема у претходном периоду свакако је резултат других фактора. Један од значајних је и одсуство визије развоја друштва, па тако и правне науке тренутно етаблиране у појединцима неспремним на нове изазове. Њихово неразумевање логике развоја информационих технологија и њених производа тако разумљивих тинејџерима носи неразумевање и аспеката IT-а који могу да угрозе друштво и

његов правни поредак. Такво неразумевање, као и потреба да се ,,докажемо" у процесу придруживања ЕУ имају за последицу политички мотивисано доношење закона, чије спровођење и обезбеђивање инструмената за њихово спровођење, као на нашем примеру, може потрајати три године, па и више.

Чињеница да се сајбер криминал не одвија на трговима и улицама отежава његово перципирање, али га због тога не чини и мање опасним. Напротив, реч је о криминалу *sui generis,* који својом виталношћу и способношћу мутације врло брзо постаје озбиљан проблем државе, јер задире не само у њену економску моћ већ и у саму безбедност, о чему нам говоре искуства других држава које су у информатичку еру крочиле знатно пре нас.

Да бисмо имали спреман одговор и на такав сценарио, неопходно је унапредити техничке и друге услове рада посебних организационих јединица државних органа које се боре против сајбер криминала.

Када је у питању унапређење техничких могућности државних органа који се боре против сајбер криминала, свакако је најзначајније унапређење техничких могућности полиције, посебно њиховог специјализованог одељења. Динамика развоја IT изискује континуирану непрекидну обуку свих учесника у борби против сајбер криминала, а одговарајућа техничка опремљеност само је предуслов примене тако стечених знања и вештина.

Фиксирање, прикупљање, чување и обрада дигиталних доказа налажу високу техничку опремљеност Посебног одељења МУП-а, при чему потреба за хитним и неодложним вештачењима налаже потребу поседовања најсавременијих хардверских и софтверских алата којим је могуће ,,ући у траг" извршиоцима тих кривичних дела, који се неретко регрутују из реда веома промућурних људи, с мултидисциплинарним знањима из IT-а, често стеченим на самом вебу.

Постојање контакт-тачке у оквиру ,,мреже 24/7", предвиђене Конвенцијом о високотехнолошком криминалу, незамисливо је без сигурног онлајн приступа свим врстама телекомуникационих мрежа. Овај контакт-центар у Републици Србији, који, по извештајима, спада у најнеактивније, треба унапредити како људским, тако и техничким ресурсима који подразумевају постојање редундантног рачунарског система, имплементираног на хетерогеним платформама, с високом пропусном моћи мреже, која би целокупним

перформансама обезбедила сигурност и брзину у обављању редовних послова Посебног тужилаштва.

С обзиром на толико помињан карактер сајбер криминала, који не познаје националне боје и обележја, намеће се логичан закључак да су техничка средства неопходна за његово откривање и сузбијање јединствена, па стога и универзална за све државе и правне системе. Да ли ће и у ком обиму таква техничка средства бити употребљена, у великој мери зависи од економске моћи државе, те је у том смислу излишно давати поређења и упоредне анализе у односу на техничку опремљеност.

Несумњива је, ипак, чињеница да је реч о знатним финансијским издацима, које многе државе из својих скромних буџета нису у стању да издвоје, у чему с правом очекују помоћ економски развијених, које би у сузбијању такве глобалне појаве као што је високотехнолошки криминал морале да препознају и сопствени интерес.

ПРИЛОЗИ

ПРИЛОГ БРОЈ 1- Списак држава потписница Конвенције о високотехнолошком криминалу

СПИСАК ДРЖАВА ПОТПИСНИЦА КОНВЕНЦИЈЕ О ВИСОКОТЕХНОЛОШКОМ КРИМИНАЛУ			
ДРЖАВЕ ЧЛАНИЦЕ САВЕТА ЕВРОПЕ			
	потписивање	**ратификација**	**ступање на снагу**
Азербеџан	30/06/2008	15/03/2010	01/07/2010
Албанија	23/11/2001	20/06/2002	01/07/2004
Андора	23/04/2013		
Аустрија	23/11/2001	13/06/2012	01/10/2012
Белгија	23/11/2001	20/08/2012	01/12/2012
Босна и Херцеговина	09/02/2005	19/05/2006	01/09/2006
Бугарска	23/11/2001	07/04/2005	01/08/2005
Велика Британија	23/11/2001	25/05/2011	01/09/2011
Грузија	01/04/2008	06/06/2012	01/10/2012
Грчка	23/11/2001		
Данска	22/04/2003	21/06/2005	01/10/2005
Естонија	23/11/2001	12/05/2003	01/07/2004
Ирска	28/02/2002		
Исланд	30/11/2001	29/01/2007	01/05/2007
Италија	23/11/2001	05/06/2008	01/10/2008
Јерменија	23/11/2001	12/10/2006	01/02/2007
Кипар	23/11/2001	19/01/2005	01/05/2005
Летонија	05/05/2004	14/02/2007	01/06/2007

Литванија	23/06/2003	18/03/2004	01/07/2004
Лихтенштајн	17/11/2008		
Луксембург	28/01/2003	16/10/2014	01/02/2015
Македонија	23/11/2001	15/09/2004	01/01/2005
Малта	17/01/2002	12/04/2012	01/08/2012
Мађарска	23/11/2001	04/12/2003	01/07/2004
Молдавија	23/11/2001	12/05/2009	01/09/2009
Монако	02/05/2013		
Немачка	23/11/2001	09/03/2009	01/07/2009
Норвешка	23/11/2001	30/06/2006	01/10/2006
Пољска	23/11/2001	20/02/2015	01/06/2015
Португалија	23/11/2001	24/03/2010	01/07/2010
Румунија	23/11/2001	12/05/2004	01/09/2004
Словачка	07/04/2005	14/04/2009	01/08/2009
Словенија	24/07/2002	08/09/2004	01/01/2005
Србија	04/02/2005	08/01/2008	01/05/2008
Турска	10/11/2010	29/09/2014	01/01/2015
Украјина	23/11/2001	10/03/2006	01/07/2006
Финска	23/11/2001	24/05/2007	01/09/2007
Француска	23/11/2001	10/01/2006	01/05/2006
Холандија	23/11/2001	16/11/2006	01/03/2007
Хрватска	23/11/2001	17/10/2002	01/07/2004
Црна Гора	07/04/2005	03/03/2010	01/07/2010
Чешка	09/02/2005	22/08/2013	01/12/2013
Швајцарска	23/11/2001	21/09/2011	01/01/2012
Шведска	23/11/2001		
Шпанија	23/11/2001	03/06/2010	01/10/2010

ДРЖАВЕ КОЈЕ НИСУ ЧЛАНИЦЕ САВЕТА ЕВРОПЕ			
	потписивање	**ратификација**	**ступање на снагу**
Аустралија		30/11/2012	01/03/2013
Доминиканска република		07/02/2013	01/06/2013
Јапан	23/11/2001	03/07/2012	01/11/2012
Јужна Африка	23/11/2001		
Канада	23/11/2001	08/07/2015	01/11/2015
Мауриција		15/11/2013	01/03/2014
Панама		05/03/2014	01/07/2014
САД	23/11/2001	29/09/2006	01/01/2007
Шри Ланка		29/05/2015	01/09/2015

Извор: *Chart of signatures and ratifications of Treaty 185*, Convention on Cybercrime, дана 28.10.2015. године [297]

[297] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures

ПРИЛОГ БРОЈ 2- Правни прописи из области сајбер криминала

ПРАВНИ ПРОПИСИ ИЗ ОБЛАСТИ САЈБЕР КРИМИНАЛА		
ДРЖАВА	***НАЗИВ АКТА***	***Ступање на снагу***
Аргентина	*Ley 26.388/2008 - Delitos Informaticos*	*2008*
Аустралија	*Cybercrime Act*	*2001*
Белгија	*Loi sur la criminalité informatique*	*2000*
Бермуда	*Computer Misuse Act*	*1996*
Велика Британија	*Computer Misuse Act*	*1990*
Велика Британија	*Regulation of Investigatory Power Act*	*2000*
Венецуела	*Ley Especial Contra los Delitos Informaticos*	*2001*
Европска Унија	*Council Framework Decision 2005/222/JHA on Attacks Against Information Systems*	*2005*
Европска Унија	*Europan Parliament recommendation to the Council on strengthening security and fundamental freedoms on the Internet*	*2009*
Индија	*Information Technology Act*	*2000*
Ирска	*Regulation on Unsolicited Communications*	*2008*
Италија	*Legge Anticriminalità*	*2008*
Јапан	*Law No. 128 of 1999 - Unauthorized Computer Access Law*	*1999*
Јужна Африка	*Electronic Communications and Transactions Act*	*2002*
Камерун	*Cybersécurité et la Cybercriminalité au Cameroun*	*2010*
Кенија	*Kenya Communications (Amendment) Act*	*2009*
Малезија	*Computer Crimes Act*	*1997*
Маурицијус	*Computer Misuse and Cybercrime Act*	*2003*
OECD	*OECD Guidelines for the Security of Information*	*2002*

	Systems and Networks	
Пакистан	*Prevention of Electronic Crimes Ordinance, 2008 (Ordinance No. IX of 2008)*	*2008*
Португалија	*Lei 109/91 - Lei da Criminalidade Informatica*	*1991*
Румунија	*Provisions on Preventing and Fighting Cybercrime*	*2003*
Савет Европе	*Guidelines for the Cooperation between Law Enforcement and Internet Service Providers against Cybercrime*	*2008*
Савет Европе	*Convention on Cybercrime*	*2004*
Савет Европе	*Guidelines for the Cooperation between Law Enforcement and Internet Service Providers against Cybercrime*	*2008*
Савет Европе	*Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems*	*2006*
Савет Европе	*Convention on Cybercrime*	*2004*
Сингапур	*Computer Misuse Act*	*1993*
Тајланд	*Computer Crime Act*	*2007*
Тонга	*Computer Crimes Act*	*2003*
Турска	*Regulation of Internet Publications and Combating Crimes Committed through such Publications*	*2007*
Уједињени Арапски емирати	*Federal Law n. 2/2006 - Prevention of Information Technology Crimes*	*2006*
Уједињене Нације	*Cybercrime: an Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*	*2008*
Уједињене Нације	*18 U.S.C.*	*1986*
Уругвај	*Ley n. 17.838 - Proteccion de Datos Personales para ser Utilizados en Informes Comerciales y Accion de Habeas Data*	*2004*

Чиле	*Ley 19223/1993 - Ley Relativa a Delitos Informaticos*	*1993*
Шпанија	*Royal Decree 3/2010*	*2010*
Шри Ланка	*Computer Crime Act*	*2007*

ЛИТЕРАТУРА

1. Алексић Ж, Шкулић М, ,,Криминалистика", Правни факултет Универзитета у Београду и Јавно предузеће ,,Службени гласник", Београд, 2007
2. Armytage W H G, A social history of engineering, Универзитет Калифорније,1961
3. Alshalan A., "Cyber-crime fear and victimization: An analysis of a national survey" Diss. Mississippi State University, 2006
4. Атанацковић Д, Кривично право, Посебни део, Београд, 1978
5. Бабић В., "Компјутерски криминал: методологије криминалистичких истраживања, разјашњавања и сузбијања компјутерског криминалитета", Сарајево, 2009
6. Бабовић М., Рачунарска превара и Интернет превара, IV општински суд у Београду, Зборник, 2004
7. Bainbridge D, Computers and the Law, Pitman Publishing ,London,1990
8. Balkan S, Berger R, J.Schmidt, Crime and deviace in America, A crecital approach, California, 1977
9. Бановић Б, ,, Обезбеђивање доказа у криминалистичкој обради кривичних дела привредног криминалитета", Виша школа унутрашњих послова, Београд-Земун, 2002
10. Bequi, A, Computer Crime, Lexinton Books, USA, 1978
11. Bhasin S, Web Security Basics, Premier Press, Ohio, 2003
12. Bossler A, Holt T, Malware Victimization, A routine activities framework, CRS Press, Taylor and Francis Group,Unitet States of America, 2011
13. Bouyat-Pinatel J, Traite de droit penal et de criminologe, Paris, 1970
14. Бошковић М, ,,Криминалистичка методика 2", Полицијска академија,, Београд, 1996
15. Brenner S. W., *State Cybercrime Legislation in the United States of America: A Survey*, 7 RICH. J.L. & TECH. 28, Winter 2001, *at* http://www.richmond.edu/jolt/v7i3/article2.html.
16. Brenner, S. W. "Cybercrime investigation and prosecution: the role of penal and procedural law", Murdoch University Electronic Journal of Law 8.2 ,2001
17. Брвар Б., Појавне облике злорабе рачуналника", Ревија за криминалистико ин криминологијо, Љубљана, бр 2/1982
18. Будимлић М, Пухарић П, ,,Компјутерски криминалитет- криминолошки, кривичноправни и сигурносни аспект", Факултет за криминалистику, криминологију и сигурносне студије, Сарајево, 2009
19. Бујуклић Ж., Форум Романум, Римска држава, право, религија и митови,Правни факултет Универзитета у Београду и Службени гласник,Београд, 2007

20. Buchanan, J., Grant, A., Investigating and Prosecuting Nigerian Fraud, U.S. Attorneys' Bulletin, Vol 49, No 06, USA, 2001

21. Vacca J, Computer Forensics -Computer Crime Scene Investigations, Charles River Media, Hingham, Massachusetts, USA, 2002

22. Водинелић В, Методика откривања, доказивања и разјашњавања рачунарског криминалитета, Приручник, 4/1990

23. Водинелић В, Научни проблеми на релацији доказни извор-доказ -доказивање у кривичном процесном праву, Анали правног факултета бр. 3-4, Правни факултет, Београд, 1994

24. Вујовић И, Превара у савременом уговорном праву- докторска дисертација, одбрањена на Правном факултету Универзитета у Београду, 2009

25. Вулетић Д., Безбедност у сајбер простору, „ Одбрана", Београд, 2012

26. Вулетић Д., Сајбер криминал и могућност његовог откривања (докторска дисертација), Факултет организационих наука, Београд, 2008

27. Вучковић В, Кривично дјело преваре, Обод, Цетиње, 2003

28. Gaines L, Miller R, Criminal Justice in Action (second edition), Wadsworth/Thomson Learning, Belmont, The United States of America, 2003

29. Gercke, M. "Understanding Cybercrime: A Guide for Developing Countries"ITU, 2011.

30. Gordon S.,Ford R. "On the definition and classification of cybercrime", Journal in Computer Virology 2.1, 2006

31. Gerraud R, Traite theorique et pratique de droit penal francais, Paris, 1924

32. Група аутора, Organizing for Computer Crime> Investigation and Prosecuting, Nacional Institute of Justice USA, 1990

33. Dashora K., "Cyber crime in the society: Problems and preventions", Journal of Alternative Perspectives in the Social Sciences 3.1 , 2011

34. Denning D,. The United States v Craig Neidorf, Communications of ACM, vol 34, No 3/91

35. Denning D, A Dialog on Hacking and Security, Edicija> Computers Under Attack, Intruders, Worms and Viruses , New York, ACM Press, 1990

36. Димитријевић П, Право информационе технологије, Internet Law,Sven,Ниш, 2011

37. Драгичевић, Д, : Компјутерски криминалитет и информацијски сустави, Информатор, Загреб, 1999

38. Дракулић М, Основи компјутерског права, Друштво операционих истраживача Југославије, Београд, 1996

39. Дракулић М, Дракулић Р, Сајбер криминал, www.bos.org.yu/cepit/idrustvo/sk/cyberkriminal.pht

40. Dyrud, M., I brought You a good news An analysis of Nigerian 419 Letters, Proceedings of 2005 Annual Association for Business Communication, Convention Association for Business Communication, USA ,2005

41. Edwards C, Savage N, Walden I,, Information Technology & The Law, Basingstoke, Macmillan Publicers LTD, 1990

42. Живановић, Т. Кривично право, Београљд, Гундулић, 1935

43. Zekos G, State cyberspace juristiction and personal cyberspace juristiction, International Journal of Law and InformationTechnology, Oxford University Press, London, Vol.15 No 1,2007

44. Зиројевић М, Употреба нових информатичких и комуникационих медија у сврхе тероризма", Ревија за безбедност-стручни часопис о корупцији и организованом криминалу, Центар за безбедносне студије, година 2, бр. 11/2008, Београд

45. Ивковић М, Ђорђевић Б, Субић З, Миланов Д, Интернет маркетинг & електронско пословање, Технички факултет „Михајло Пупин", Зрењанин,2011

46. Игњатовић Ђ, „Појмовно одређење компјутерског криминалитета", Анали Правног факултета, бр 1-3/1991

47. Ериксен Т, Тиранија тренутка: брзои споро време у информационом друштву, библиотека XX век, Београд, 2003

48. Јерковић Р, „ Борба против високотехнолошког криминалитета у Србији", Телекомуникације-научно-стручни часопис Републичке агенције за телекомуникације бр 3/2009

49. Јерковић Р, „Високотехнолошки криминал: актери и жртве", Ревија за безбедност-стручни часопис о корупцији и оргаизованом криминалу, Центрар за безбедносне студије, бр 3/2009, година 3, стр 27-34, Београд, 2009

50. Jescheck H.H., Lehrbuch des Strafrechts, Berlin, 1972

51. Јовановић Ж, Кривично право, Посебни део, Београд, 1979

52. Јовашевић Д, Хашимбеговић Т:,, Кривичноправна заштита безбедности рачунарских података", http://www.singipedia.singidunum.ac.rs/content/974-Krivicnopravna-zatita-bezbednosti-racunarskih-podataka

53. Jones S, Virtual Culture-Identity and Communication in Cybersociety, SAGE Publications, London, 1997

54. Казић Е., Вируси, Рачунари, Београд, бр. 59/90

55. Kane P, V.I.R.U.S. Protection, Vital Information Resources Under Siege, Includes dr Panda Utilites, New York, Bantam Books, 1989

56. Karyda M, Mitrou L, Internet Forensics,Legal and Technical Issues, Second International Workshop on Digital Forensics and Incident Analysis, IEE Computer Society, 2007

57. Kent K, Chevalier S, Grance T, Dang H, Guide to Integrating Forensics into Incident Response (Special publication 800-86), National Institute of Standards and Technology, Gaithersburg, 2006

58. Kerstein P.: How Can We Stop Phishing and Pharming Scams?, http://www.csoonline.com

59. Кештеровић Ж, ,,Интернет као оруђе теориста", Ревија за безбедност – стручни часопис о корупции и организованом криминалу, Центар за безбедносне студије, Година 2, бр 4/2008, Београд, 2008

60. Koenig D, ,,Investigation of Cybercrime and Technology-related Crime, http/www.neiassociates.org/cybercrime. Htm

61. Kollock P, Smith M, ,,Communities in cyberspace, Routledge, New York, 2001

62. Коментар Кривичног закона Србије, група аутора, Београд, 1995

63. Кораћ, С, ,,Сузбијање дечије порнографије на Интернету: ЕУ стандарди", Ревија за безбедност -стручни часопис о корупцији и организованом криминалу, Центар за безбедносне студије, година 2, бр. 11/2008, Београд

64. Крапац, Д, Компјутерски криминалитет, Правни факултет, Загреб, 1992

65. Kshetri N, Pattern of global cyber war and crime-A conceptual framework, Journal of International Management, The Fox Scholl of Business and Management-Temple University, Greensboro (USA), No 11,2005

66. Kshetri N.,"Cybercrime and Cybersecurity in the Global South", Palgrave Macmillan, Houndmills, 2013

67. Кузнецов, Р. Н. "Киберпреступность как элемент сетевой теневой экономики", Вестник магистратуры 6, 2013

68. Кукрика М, Управљање сигурношћу информација, INFOhome Press, Београд, 2002

69. Лазаревић Љ, Коментар Кривичног законика Републике Србије, Савремена администрација, Београд, 2006

70. Латинковић Б., Информационе технологије, Паневропски универзитет Аперион, Бања Лука, 2007

71. Laudon, C.K. Et al. E -commerce: Business, Technology, Society, Addison Wesley, Boston, 2001

72. Levi M., "Organized fraud and organizing frauds -Unpacking research on networks and organization", Criminology and Criminal Justice 8.4, 2008

73. Lipner S, Kalman S, Computer Law, Cases and Materials, Columbus, Merrill Publishing Company, 1989

74. Lobel J., Foiling the System Breakers, Computer Security and Access Control, New York, McGraw-Hill Book Company, 1986

75. Longe, B., Chiemeke, C., Cyber Crime and Criminality in Nigeria – What Roles are Internet Access Points in Playing?, European Journal of Social Sciences – Volume 6, Number 4, Great Britain,2008

76. Lucas J, Moeller B, Effective Incident Response Team (e book), Addison Wesley, Indianapolis, Formatig the puzzle, 2003

77. Мадоян, В. В. "Виды компьютерной преступности и меры по их противодействию в России", Новый университет, Москва 2012

78. Матијашевић Ј, Кривичноправна регулатива рачунарског криминала, Универзитет привредна академија у Новом Саду, Нови Сад, 2013

79. Милосављевић М., Грубор Г., "Истрага компјутерског криминала: методолошко-технолошке основе", Универзитет Сингидунум, Београд, 2009

80. Mitnik K D., Sajmon V. L., Уметност обмане: утицај људског фактора на безбедност, Микро књига, Београд, 2003

81. Mitnik K D., Sajmon V. L.,, Умеће провале", Микро књига, Београд, 2005

82. Морс М, "Сајбер пределu, контрола и трансценденција: естетика виртуелног", Култура бр. 107-108, Завод за проучавање културног развитка, Београд, 2004

83. Mohay G, Anderson A, Collie B and others, Computer and Intrusion Forensics, Artech House, London 2003

84. McCusker R. "Transnational organised cyber crime: distinguishing threat from reality", Crime, law and social change, 2006.

85. Nelson B, Philips A, Enfinger F, Steuart C, Guide to Computer Forensics and Investigations, Thomson Course Tehnology, Boston, 2006

86. Nigel P.,Hodges M., "Cybercrime: the reality of the threat", Nigel Phair, 2007

87. Николић К, Гвозденовић Р, Радуловић С, Милосављевић А, Јерковић Р, Живковић В, Живановић С, Рељановић М, Алексић И, „Сузбијање високотехнолошког криминала", Удружење јавних тужилаца и заменика јавних тужилаца Србије, Београд, 2010

88. Номоконов В. А., Тропина Т. Л., "Киберпреступность: угрозы, прогнозы, проблемы борьбы", Information Technology and Security , 2013

89. OECD, Shaping Policies for the Future of Internet Economy, Paris, 2008

90. Осипенко А.Л. Сетевая компьютерная преступность. Омск, 2009.

91. Павловић Ш, Компјутерска казнена дјела у Казненом законику-основе хрватског информацијског права" хрватски љетопис за казнено право и праксу, вол 10- бр. 2/2003, Загреб,2003

92. Parker D, Fighting Computer Crime, New York, Charles Scribneirs Sons, 1981

93. Parker D, ,,Fighting computer crime``, New York, 1983

94. Parker D, ,,Computer Abuse``,Springfielf, 1973

95. Parker D. Nycum S, Aura S, Computer Abuse, Stanford Research Institute, Menlo Park, California, 1973

96. Pastore M, Security +Study Guide, Sybex, London, 2003

97. Peckitt R, Computers In General Practice, Wilmslow, Sigma Press, 1989

98. Петровић С, ,,Компјутерски криминал", Безбедност, МУП РС, бр 1/94

99. Петровић С, ,,Компјутерски криминал", Војноиздавачки завод, Београд,2004

100. Петровић С, ,,,О информационој револуцији у контексту злоупотребе информационе технологије" file:///C:/Users/0020578/Desktop/ZT04%20-%20O%20informacionoj%20revoluciji%20u%20kontekstu%20zloupotrebe%20informacione%20tehnologije.pdf

101. Прља Д., Ивановић З. , Рељановић М., "Кривична дела високотехнолошког криминала", Институт за упоредно право, Београд, 2011

102. Путник Н, Сајбер простор и безбедносни изазови, Факултет безбедности, Београд, 2009

103. Ранђеловић Д, Високотехнолошки криминал, Криминалистичко-полицијска академија, Београд, 2013

104. Ранђеловић Д, Поповић Б, Злонамерни програми, Техника, 5/2010, Електротехника (59), број .5, Београд, 2010

105. Raymond E, Steel G, The New Hackers Dictionary, Cambridge, MIT Press MA, 1991

106. Roberts R, Kane P, Computers Computer Security , Greensboro, Computer Books, 1989

107. Rothchild J, Protecting the Digital Consumer-The Limits of Cyberspace Utopinism, Indiana Law Journal, 1999, vol 74

108. Russell S., Grabosky P., Urbas G."Cyber criminals on trial",Criminal Justice Matters 58.1, 2004

109. Салмон К, Сторителинг или причам ти причу, Clio, Београд, 2011Владица Бабић, Компјутерски криминал, Рабић,Сарајево, 2009

110. Samociuk M, Hacking, Edicija The protection of Computer Software, its technology and applications, Cambridge University Press, The British Computer Society, 1989

111. Setiadi Farisya, An Overview of the Development Indonesia National Cyber Security, International Journal of Information Technology & Computer Science (IJITCS) (ISSN No : 2091-1610) Volume 6 : Issue on November / December , 2012

112. Sieber, U, Computer Crime and Criminal Justice, Koln, 1977

113. Sieber U, The International Handbook of Computer Crime, Chichester, John Wiley&sons, 1991

114. Sieber, U , The International Emergence of Criminal Information Law, Carl Heymanns Verlag KF, Koln, 1992

115. Сингер, М, Криминологија, Накладни завод Глобус, Загреб, 1994

116. Smith, R., Holmes, M., Kaufmann, P., Nigerian Advance Fee Fraud, Trends and Issues in crime and criminal justice, Australian Institute of Criminology, Australia,1999

117. Спасић В, „Актуелна питања у области сајбер криминала", Билтен судске праксе Врховног суда Србије, Интермекс, бр 1/2006, Београд,2006

118. Spafford E. H., Heaphy K.A., Ferbache D.J.,A Computer Virus Primer, Computers Under Attack, Intruders, Worms and Viruses, New York, ACM Press, 1990

119. Stephenson P, Investigating Computer-related Crime-A Handbook for Corporate Investigators, CRC Press, New York, 2000

120. Stephenson P., Keith G. "Investigating computer-related crime",CRC Press, 2013.

121. Shinder D, Scene of the Cybercrime-Computer Forensics Handbook, Syngress Publishing, Inc. Rockland (USA), 2002

122. Таховић Ј, Кривично право, Посебни део, Београд, 1953

123. Taylor, P, Hackers-Crime in the Digital Sublime, Routledge, 1 edition

124. Tipton H, Krause M, Information Security management Handbook (fifth edition), CRC Press, New York, part Welch T, Computer Crime Investigation and Computer Forensics, 2004

125. Tnnies F ,*The Present Problems of Social Structure* ,*The* American Journal of Sociology, vol. 10, 1905, no. 5

126. Томић З, „Сајбер простор и проблеми разграничења", Култура, бр 107-108, Завод за проучавање културног развитка, Београд, 2004

127. Требејшанин Ж, Речник психологије, Стубови културе, Београд, 2004

128. Tropina, T. Cybercrime and Organized Crime, Freedom from Fear Magazine. – 2010. – Issue 3.

129. Tropina, T., "Self- and Co-regulation in Fighting Cybercrime and Safeguarding Cybersecurity", "Current Issues in ITU Security", Duncker & Humblot, Berlin, 2012

130. Turban E et al., Electronic Commerce-A Managerial Perspektive, Prentice Hall, New Jersey, 2000

131. Ћировић Д, Јанковић Н, Лађевић М, „ Cyber подземље у Србији", Репортер, 16.11.2005

132. Удружење јавних тужилаца и заменика јавних тужилаца, Сузбијање високотехнолошког криминала, АТС, Београд, 2010

133. Уљанов С, Урошевић В, Ивановић З, „Високотехнолошки криминал из угла међународне сарадње криминалистичке полиције", Зборник радова са међународног научно-

стручног скупа „Међународна и национална сарадња и координација у супротстављању криминалитету” вол.3, бр.1, стр. 530-541, Интернационална асоцијација криминалиста, Бања Лука, 2010

134. Фејеш И, „Компјутерски криминалитет-криминалитет будућности, изазов садашњости”, Правни живот-часопис за правну теорију и праксу, Удружење правника Србије, бр. 9/2000, година 2, књига 452, Београд,2000

135. Forensic Examination of Digital Evidence/ A Guide for Law Enforcement, National Institute of Justice, Washinghton, 2004

136. Forester T, Morrison P, Computer Ethics, Cautionary Tales and Ethical Dilemmas in Computing, London, Basil Blackwell, 1994

137. Herweg R, Bases of Computer Viruses, Koln, Datakontext-Verlag, 1991

138. Хестер М., Форд П., "Компјутери и етика у сајбер добу: приступ преко студије случаја", Службени гласник, Београд, 2009

139. Holt T., Schell B., "Corporate Hacking and Technology-Driven Crime : social dynamics and implications", Information Science Reference, Hershey 2011

140. Carrier B, File System Forensic Analysis, Addison Wesley Profesional, Indiana, 2005

141. Mohay G, Anderson A, Collie B and others, Computer and Intrusion Forensics, Artech House, London 2003

142. Casey E, Digital Evidence and Computer Crime-Forensic Science, Computers and the Internet (second edition), Academic Press, London, 2004

143. Casey E., "Digital Evidence and Computer Crime : forensic science, computers and the Internet", Academic Press, Waltham, 2011

144. Clandos R., "Eye on cybercrime", IEEE Security & Privacy Magazine 1.4, 2003

145. Clough J., "Principles of cybercrime", Cambridge University Press, 2010

146. Comer D. Internet working with TCP/IP Vol. I: Principles, Protocols, and Architecture. Purdue University, 1995.

147. Cohen, F . "Computer Viruses Theory and Experiments," Computers and Security, vol. 6,1987.

148. Coyne, R , Designing information technology in the postmodern age-From method to metaphor, MIT Press, Cambridge, 1995

149. Chaffey, D, E -Businees and E-Commerce Management, Prentice Hall, London, 2002

150. Chawki, M, Anonymity in Cyberspace: Finding the Balance between Privacy and Security, Revista da Faculdade de Direito Milton Campos, Nova Lima, Brazil, vol 11,2009

151. Chawki, M., Nigeria Tackles Advance Fee Fraud, Journal of Information, Law & Technology, University of Warwick, Great Britain, (1), стр. 1-20. СТРУЧНИ РАДОВИ 12 БЕЗБЕДНОСТ 3 / 2009

152. Choi K., "Risk Factors in Computer-Crime Victimization", LFB Scholarly Publishing LLC, El Paso,2010.

153. Чејовић Б, Кривично право, Посебни део, Београд, 2002

154. Чејовић, Б, Кривично право у судској пракси, Посебни део, књига друга, Београд, 1986

155. Шкулић М, Кривично процесно право-општи део, Правни факултет/ Службени гласник, Београд, 2007

156. Xingan L, Cybercrime-An Introduction, www.studycrime.come/crime/cybercrime.php

157. Tulloch M, Microsoft Encyclopedia of Security, Microsoft Press, Washington, 2003

158. Walden I."Computer Crimes and Digital Investigations", Oxford University Press, Oxford 2007

159. Wall D.S. "Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace ",Police Practice and Research, 8:2, 1, 2007.

160. Wagner B, Electronic Jihad, National Defense, National Defense Industrial Association, July 2007

161. Wellman B, Gullia M, ,,Virtual communities as communities- Net surfers dont ride alone``, Kollock P, Smith M, ,,Communities in cyberspace, Routledge, New York, 2001

162. Welzel H, Deutsches Strafrech, Berlin, 1954

163. Westby J, Међународни водич за борбу против компјутерског криминала, Продуктивност АД, Београд, 2004

164. Westland C, Valuing Technology-the new science of Wealth in the Knowledge Economy, John Wiley and sons, 2002

ЛЕКСИКОНИ, РЕЧНИЦИ

1. Алексић Ж, Миловановић З, Лексикон криминалистике, Глосаријум,Београд, 1995
2. Вујаклија Милан, Лексикон страних речи и израза, “Штампар Макарије”, Београд, 2011
3. Encarta encyclopedia, htpp/encyclopedia.msn.com /encyclopedia_761582824/Cyberspace.html

4. Joint Publication 1-02, DOD Dictionary of Military and Associated Terms, www.dtic.mil./doctrine/jel/new_pubs/1_02.pdf
5. Клаић Б, Рјечник страних ријечи: туђице и посуђенице, Накладни Завод Матице Хрватске, Загреб 1988
6. Мимица А, Богдановић М, Социолошки речник, Завод за уџбенике, Београд, 2007
7. Origins of the word cyberspace, http/encyclopedia.thefreedictionary.com/cyberspace
8. Правна енциклопедија, Савремена администрација, Београд, 1985
9. Речник српскохрватског књижевног језика (књига пета), Матица српска, Нови Сад, 1973
10. Речник српскохрватског књижевног језика (књига трећа), Матица српска, Нови Сад, 1969
11. Социолошки лексикон, Савремена администрациа, Београд, 1982
12. Тасић В, Беуер И, Речник компјутерских термина, Микро књига, Београд, 2003
13. The Free Dictionary http/www.thefreedictionary.com/cyberspace
14. Hutchinson encyclopedia, http/encyclopedia.farlex.com/cyberspace
15. Collin B, The Future of Cyberterrorism, http/afgen.com/terrorism1.html
16. Computing Dictionary http/computingdictionary.thefreedictionary.com/cyberspace

ПРАВНИ ПРОПИСИ

1. German Criminal Code -Criminal Code in the version promulgated on 13 November 1998, Federal Law Gazette [Bundesgesetzblatt] I p. 3322, last amended by Article 1 of the Law of 24 September 2013, Federal Law Gazette I p. 3671 and with the text of Article 6(18) of the Law of 10 October 2013, Federal Law Gazette I p 3799. http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p1710
2. Закон о играма на срећу ("Сл. Гласник РС", бр. 84/2004 i 85/2005 – др. закон)
3. Закон о изменама и допунама Кривичног законика "Службени гласник РС", бр. 72/2009 од 3.9.2009. године.
4. Закон о организацији и надлежности државних у борби против високотехнолошког криминала "Сл. Гласник РС", бр. 61/2005 и 104/2009
5. Казнени законик (КЗ-1), Уредни лист Републике Словеније, шт. 55/2008, issn 1318-0576, година XVII

6. Конвенција о високотехнолошком криминалу (Закон о потврђивању Конвенције о високотехнолошком криминалу, објављен у "Сл.гласнику РС", бр. 19 од 19. марта 2009 године)
7. Кривични законик Републике Србије "Сл.гласник РС", бр. 85/2005, 88/2005 - испр., 107/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013 и 108/2014
8. Laws of Malaysia- REPRINT Act 563 Computer Crimes Act 1997 Incorporating all amendments up to 1 January 2006 Published By The Commissioner of Law Revision, Malaysia Under The Authority of The Revision of Laws Act 1968 In Collaboration With Percetakan Nasional Malaysia Bhd 2006 http://www.agc.gov.my/Akta/Vol.%2012/Act%20563.pdf
9. Recommendation No. R (89)9, adopted by the Committee of Ministers of the Council of Europe on September13,1989 and Report by the European Committee on Crime Problems> Computer-related crime - https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2
10. Recommendation No. R (95) 13, approved by the European Committee on Crime Problems-(CDPC) at its 44th plenary session May 29-June 2,1995-Concerning problems of criminal procedural law connected with information technology, http://www.coe.int/t/dghl/standardsetting/media/doc/cm/rec(1995)013_EN.asp
11. Уголовный кодекс РФ от 13 июня 1996 г. N 63-ФЗ (внесены правки от 27 мая, 25 июня 1998 г., 9 февраля, 15, 18 марта, 9 июля 1999 г., 9, 20 марта, 19 июня, 7 августа, 17 ноября, 29 декабря 2001 г., 4, 14 марта, 7 мая, 25 июня, 24, 25 июля, 31 октября 2002 г., 11 марта, 8 апреля, 4, 7 июля, 8 декабря 2003 г., 21, 26 июля, 28 декабря 2004 г., 21 июля, 19 декабря 2005 г., 5 января, 27 июля, 4, 30 декабря 2006 г., 9 апреля, 10 мая, 24 июля, 4 ноября, 1, 6 декабря 2007 г., 14 февраля, 8 апреля, 13 мая, 22 июля, 25 ноября, 22, 25, 30 декабря 2008 г., 13 февраля, 28 апреля, 3, 29 июня, 24, 27, 29 июля, 30 октября, 3, 9 ноября, 17, 27, 29 декабря 2009 г., 21 февраля, 29 марта, 5, 7 апреля, 6, 19 мая, 17 июня, 1, 22, 27 июля, 4 октября, 29 ноября, 9, 23, 28, 29 декабря 2010 г., 7 марта, 6 апреля, 4 мая, 11, 20, 21 июля, 7, 21 ноября, 6, 7 декабря 2011 г., 29 февраля, 1 марта, 5 июня, 10, 20, 28 июля, 16 октября, 12, 29 ноября, 3, 30 декабря 2012 г., 4 марта, 5 апреля, 28, 29 июня, 2, 23 июля, 21 октября, 2, 25 ноября, 21, 28 декабря 2013 г., 3 февраля, 5 мая, 5, 28 июня, 21 июля, 24 ноября, 22, 31 декабря 2014 г., 3 февраля, 8, 30 марта, 23 мая, 8, 29 июня, 13 июля 2015 г.) http://www.uk-rf.com/

12. U.S. Code § 1030 - Fraud and related activity in connection with computers,https://www.law.cornell.edu/uscode/text/18/1030
13. U.S. Code § 1362 - Communication lines, stations or systems
14. https://www.law.cornell.edu/uscode/text/18/1362
15. 18 U.S. Code § 2511 - Interception and disclosure of wire, oral, or electronic communications prohibited
16. https://www.law.cornell.edu/uscode/text/18/2511
17. U.S. Code § 2701 - Unlawful access to stored communications
18. https://www.law.cornell.edu/uscode/text/18/2701
19. Казнени законик (КЗ-1) , Уредни лист Републике Словеније, шт. 55/2008, issn 1318-0576, година XVII
20. Казнени закон, Народне новине Републике Хрватске, бр. 110/97,27/98, 50/00, 129/00, 51/01,111/031, 190/03, 105/04,71/06, 110/07, 152/08
21. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f259a

ИНТЕРНЕТ ИЗВОРИ

1. Facebook integriše WhatsApp u svoju Android aplikaciju?http://www.informacija.rs/Mobilni-telefoni/Facebook-integrise-WhatsApp-u-svoju-Android-aplikaciju.html
2. Koliko svetsku ekonomiju košta sajber kriminal http://www.informacija.rs/Vesti/Koliko-svetsku-ekonomiju-kosta-sajber-kriminal.html
3. Посебно тужилаштво за високотехнолошки криминал http://www.beograd.vtk.jt.rs/
4. Draft Board and Dow Chemical Raids (1969) http://www.hippy.com/modules.php?name=News&file=article&sid=79
5. Компјутерски криминал све опаснији,http://www.vesti.rs/Hronika/Kompjuterski-kriminal-sve-opasniji.html
6. Компјутерски криминалитет,APIS Security Consulting, APIS Group, http\\www.apisgroup.rg|sec.html|Knjige|UMOB|sec.html?id=29
7. MARKEN, Jacob Cornelis van,https://socialhistory.org/bwsa/biografie/marken
8. Društveni inženjering – Stoljeće medijske manipulacije čovječanstva http://blog.vecernji.hr/ratko-martinovic/drustveni-inzenjering-stoljece-medijske-manipulacije-covjecanstva-3948

9. On Facebook, You Are Who You Know http://www.psmag.com/books-and-culture/on-facebook-you-are-who-you-know-10385
10. Najuspešnije Facebook prevare u 2014.http://www.informacija.rs/Drustvene-mreze/Najuspesnije-Facebook-prevare-u-2014.html
11. Da li postoji tipičan psihološki profil žrtve Facebook prevara? http://surfujbezbedno.com/zanimljivosti/da-li-postoji-tipican-psiholoski-profil-zrtve-facebook-prevara/
12. Your favorite IT-Security Conference- https://www.troopers.de/events/troopers15/461_the_science_of_security_awareness_building_a_better_awareness_program/
13. Melissa Macro Virushttps://www.cert.org/historical/advisories/CA-1999-04.cfm?
14. MyDoom worm spreading fast, Sophos warns users to be wary of viral email and hacker attack https://www.sophos.com/en-us/press-office/press-releases/2004/01/va_mydoom.aspx
15. Fake Flash update installs feared banking Trojan http://www.nbcnews.com/technology/fake-flash-update-installs-feared-banking-trojan-1B8202115
16. http://www.kurir.rs/internet-prevara-platio-telefon-dobio-igracke-clanak-1140329
17. Polovina korisnika se ne oseća bezbedno tokom onlajn kupovine http://novaekonomija.rs/sr/vesti-iz-zemlje/polovina-korisnika-se-ne-ose%C4%87a-bezbedno-tokom-onlajn-kupovine
18. Draft Board and Dow Chemical Raids (1969) http://www.hippy.com/modules.php?name=News&file=article&sid=79
19. http://www.slobodnaevropa.org/content/oniline-prevare-u-srbiji-platis-kompjuter-dobijes-cepanicu/24893683.html
20. Компјутерски криминал све опаснији,http://www.vesti.rs/Hronika/Kompjuterski-kriminal-sve-opasniji.html
21. http://www.b92.net/tehnopolis/internet.php?nav_id=425012
22. I Srbija među zemljama koje su tražile informacije o korisnicima Twitter naloga http://www.informacija.rs/Ostalo/I-Srbija-medju-zemljama-koje-su-trazile-informacije-o-korisnicima-Twitter-naloga.html
23. Da li nas država špijunira http://www.informacija.rs/Vesti/Da-li-nas-drzava-spijunira.html
24. DriveSpy - Digital Intelligence https://www.digitalintelligence.com/software/disoftware/drivespy/
25. http://www.e-fense.com/

26. Forensic Toolkit (FTK) | AccessData
http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk
27. How To Digital Forensic Imaging In VMware ESXi - SANS
https://digital-forensics.sans.org/blog/2010/10/04/digital-forensic-imaging-vmware-esxi
28. Ruski hakeri ukrali 25 miliona dolara od banaka i sa bankomata
http://www.informacija.rs/Vesti/Ruski-hakeri-ukrali-25-miliona-dolara-od-banaka-i-sa-bankomata.html
29. Slučaj "Eurograbber": Kako je malver ukrao 36 miliona evra sa bankovnih računa evropskih korisnika
http://www.informacija.rs/Vesti/Slucaj-Eurograbber-Kako-je-malver-ukrao-36-miliona-evra-sa-bankovnih-racuna-evropskih-korisnika.html
30. Stručnjaci upozoravaju: "Bankarski" Trojanci i ransomware za Android u porastu,
http://www.informacija.rs/Mobilni-telefoni/Strucnjaci-upozoravaju-Bankarski-Trojanci-i-ransomware-za-Android-u-porastu.html
31. 'Money mules': Kriminalci ili žrtve bankarskih prevara na internetu
http://www.informacija.rs/Clanci/Money-mules-Kriminalci-ili-zrtve-bankarskih-prevara-na-internetu.html
32. Chart of signatures and ratifications of Treaty 185
Convention on Cybercrime Status as of 28/10/2015- http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures
33. Cyber Law in Malaysia http://malaysiancyberwarriors.blogspot.rs/2013/03/introduction-of-cyber-law-acts-in.html
34. CYBERWELLNESS PROFILE PORTUGUESE REPUBLIC https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Portugal.pdf
35. Weisser Bettina, Cyber Crime –The Information Society and Related CrimesSection 2 –Special Part National Report on Germany, University of Muenster
http://www.penal.org/sites/default/files/files/RM-8.pdf
36. Regulation of criminal activities on the Internet in Austria
(November, 25th, 2002) http://www.juridicum.su.se/iri/masterIT/vls/rep/it-crime/Austria.htm
37. Cyber Crime law France http://www.cybercrimelaw.net/France.html
38. UK law introduces life sentence for cybercriminals http://www.wired.co.uk/news/archive/2014-06/06/cybercrime-bill-life-sentence
39. U.S. FEDERAL CYBERCRIME LAWS http://digitalenterprise.org/governance/us_code.html

40. CYBERCRIME IN ASIA: A CHANGING REGULATORY ENVIRONMENT, http://asia.marsh.com/Portals/59/Documents/Cybercrime%20in%20Asia%20-%20A%20Changing%20Regulatory%20Environment_EN.pdf
41. CYBERCRIME IN China http://www.cybercrimelaw.net/China.html
42. Reporting and Policing Internet Crimes in China http://www.hg.org/article.asp?id=22958
43. The Cybercrime Carnival in Brazil: Loose Cyberlaws Make for Loose Cybercriminals http://www.darkreading.com/vulnerabilities---threats/the-cybercrime-carnival-in-brazil-loose-cyberlaws-make-for-loose-cybercriminals/a/d-id/1320441
44. http://www.crime-research.org/library/Criminal_Codes.html
45. The Real Story of Stuxnet How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet
46. Melissa (computer virus) https://en.wikipedia.org/wiki/Melissa_(computer_virus)
47. "Top Ten Most Destructive Computer Viruses of All Time". http://crunkish.com/top-ten-worst-computer-viruses/
48. History of Mac malware: 1982 – 2011 https://nakedsecurity.sophos.com/2011/10/03/mac-malware-history/
49. Kenzero Porn Virus Publishes Web History Of Victims On The Net--Unless They Pay http://www.huffingtonpost.com/2010/04/16/kenzero-porn-virus-publis_n_540133.html
50. German Government Fesses Up to Spying on Citizens With Trojan, Says It's Legal http://www.themarysue.com/german-gov-trojan/
51. Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, year 2000,, Background paper for the workshop on crimes related to the computer network-Crime fighting on the Net http://www.un.org/en/conf/crimecongress2010/pdf/55years_ebook.pdf
52. The Communication from the Commission to the Council , the European Parliament, the Economic and Social Committee and the Committee of the Reegions, January 26,2001 http//europa.eu.int
53. TROJANS AND BACKDOORShttp://www.webpronews.com/trojans-and-backdoors-2005-08/ 5,500 hentai pirates afflicted by blackmailing malware, http://www.geek.com/news/5500-hentai-pirates-afflicted-by-blackmailing-malware-1191821/
54. 250,000 Credit Cards Stolen in Wine Industry Hack http://svbwine.blogspot.rs/2015/07/250000-credit-cards-stolen-in-wine.html
55. Most common form of malware http://www.guinnessworldrecords.com/world-records/most-common-form-of-malware

56. Researchers Trace Structure of Cybercrime Gangs
http://www.pcworld.com/article/148416/article.html
57. Global studies on organized crime, United Nations office at Vienna, Global Studies on organized crime, http://www.globalinitiative.net/download/general/global/UN%20-%20Global%20studies%20on%20organized%20crime.pdf
58. Извештај Међународног удружења за казнено право:
http//www.uplink.com.au/lawlibrary/Documents/Docs/Doc122.html#fn0
59. Main problems related to the Cybercrime, 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders, http//www.justinfo.net/UPLOAD/docs/argentina.htm
60. A SUMMARY OF LAWRENCE KOHLBERG'S STAGES OF MORAL DEVELOPMENT
Copyright 2000 by Robert N. Barger, Ph.D.
University of Notre Dame Notre Dame, IN 46556
http://www.csudh.edu/dearhabermas/kohlberg01bk.htm
61. Inside the mind of Dark Avenger by Sarah Gordon
http://vxheaven.org/lib/static/vdat/ivdarkav.htm
62. Overview of the Open-Source Movement Copyright © 2000 by R. E. Wyllys
https://www.ischool.utexas.edu/~l38613dw/readings/OpenSourceOverview.html
63. UN Crime related to the computer networks http://www.unis.unvienna.org/pdf/05-82111_E_6_pr_SFS.pdf
64. The Council of Europe, the Report on Organized Crime: The threat of cyber crime from 2004http://www.coe.int/t/dghl/cooperation/economiccrime/organisedcrime/Organised%20Crime%20Situation%20Report%202004.pdf
65. https://www.facebook.com/james.stavridis
66. http://www.telegraph.co.uk/technology/9136029/How-spies-used-Facebook-to-steal-Nato-chiefs-details.html
67. https://fakers.statuspeople.com/http://twitblock.org/
a. https://barracudalabs.com/2012/02/attackers-use-fake-friends-to-blend-into-facebook/
68. https://www.indexoncensorship.org/2014/02/10-countries-facebook-banned/
69. https://en.wikipedia.org/wiki/Websites_blocked_in_mainland_China
70. Nigerijska šema (šema 419)
http://www.prevara.info/index.php?option=com_content&task=view&id=42
71. Lottery scam https://en.wikipedia.org/wiki/Lottery_scam
72. Congratulations, you've won! The reality behind online lotteries
https://securelist.com/analysis/publications/36450/congratulations-youve-won-the-reality-behind-online-lotteries/

73. http://www.mindpride.net/root/Extras/Viruses/computer_virus_history_1.htm
74. VB - Virus Bulletin https://www.virusbtn.com/pdf/magazine/1990/199003.pdf
75. 6 Computer Viruses That Changed The World http://www.makeuseof.com/tag/6-computer-viruses-changed-world/