Fall 9-2014

KRIMINALITETI KOMPJUTERIK

Arsim Peci
University for Business and Technology - UBT

Programi Juridik

Punim Diplome
Viti akademik 2010 – 2011

Arsim Peci

KRIMINALITETI KOMPJUTERIK

CYBERCRIME

Mentori: Mr.sc.Liridon Shurdhani

Shtator / 2014

Ky punim është përpiluar dhe dorëzuar në përmbushjen e kërkesave të pjesshme për Shkallën Bachelor

ABSTRAKT

Në këtë punim do të përqendrohemi kryesisht në shmangien që i bëhet qëllimit primar të përdorimit të kësaj teknologjie (komunikimit). Keqpërdorimi i saj nga elementë kriminelë njihet me emrin krim kompjuterik ose krim kibernetikë.

Në praktikën e përditshme konstatohen dy lloj sjelljesh përballë fenomenit të krimit kibernetikë. Në njërën anë kemi përdoruesin e përditshëm i cili udhëhiqet shumë shpesh nga ideja që "e keqja shkon gjithmonë tek të tjerët". Në anën tjetër, kemi specialistët e fushës që udhëhiqen diametralisht nga kundërta, domethënë që " të tërë jemi të barabartë, të paktën në terma matematike, ndaj probabilitetit të të qenit objekt i një sulmi kriminel". Ndryshe nga përdoruesi i zakonshëm, specialisti i kushton kohë analizës së fenomenit për të kuptuar funksionimin e tij.

Duhet theksuar fakti që në asnjë moment dhe në asnjë rrethanë nuk duhet të biem pre e idesë që një ditë këtë probabilitet mund ta bëjmë zero.

Përdorimi i teknologjive të reja të informacionit dhe veçanërisht i Internetit ka marrë një rëndësi të veçantë në jetën e përditshme. Ky fenomen prek jo vetëm aktivitetet e një organizmi qoftë ai shtetëror apo privat, i implikuar në sferën e biznesit apo të një aktiviteti jo fitimprurës, por mund te prekë dhe njeriun e thjeshtë në aktivitetin e tij të përditshëm, në sferën e tij private apo profesionale.

Si çdo teknologji e re e vënë në dispozicion të një numri të madh përdoruesish, Interneti paraqet jo vetëm të mira dhe përfitime, por në të njëjtën kohë dhe një sërë problemesh. Duke qenë një teknologji "e liberalizuar" prej disa kohësh, siç përdoret në zhargon, nuk ia vlen të zgjatemi në diskutimin e përfitimeve që sjell përdorimi i kësaj teknologjie. Anën e përfitimeve mund ta përmbledhim për momentin në një frazë te vetme: komunikim (në kuptimin e gjerë të fjalës) i shpejtë, i pakushtueshëm dhe tërësisht i pavarur nga nocioni i distancës.

Fjalët kyçe: krimi kompjuterik, teknologji, sulm, vepër penale.

ABSTRACT

In this paper we will focus mainly on the avoidance that is done to the primary goal of using this technology (communication). Its misuse by criminals known as computer crime or cybercrime.

In everyday practice are found two kinds of behavior confront the phenomenon of cybercrime. On the other hand we have the everyday user who often is guided by the idea that "the evil always goes to others".On the other hand, we have experts of this field led diametrically by the opposite, meaning that "we all are equal, at least in mathematical terms, to the probability of being the subject of a criminal attack." Unlike an ordinary user, the expert devotes time on the phenomenon analysis to understand its functioning.

It should be noted the fact that at no time and under no circumstances must not fall prey to the idea that one day we can make this probability zero.

The use of new information technologies and the Internet in particular has taken a special importance in everyday life. This phenomenon affects not only the activities of an organization whether public or private, involved in the field of business or a nonprofit activity, but can affect also the ordinary person in his everyday activity, in his private or professional area.

Like any new technology available to a large number of users, the Internet presents not only the good and benefits, but at the same time a series of problems. Being a"liberalized" technology for quite some time, as used in slang, not worth to discuss further for the benefits of using this technology.Side benefits may be summarized at the moment in a single phrase: communication (in the broad sense of the word) fast, affordable, and completely independent of the notion of distance.

Key words: Cyber-crimes, technology, attack, criminal act.

MIRËNJOHJE/FALENDERIME

Ky punim vjen si një punim përmbyllës të një ciki studimesh Bechelor në Fakulteti Juridik .

Me shumë kënaqësi do të doja të shprehja falënderimet e mia të sinqerta për të gjithë ata që më ndihmuan, konsultuan dhe më mbështetën moralisht gjatë realizimit të kësaj teme.

Fillimisht dua të falënderoj personat më të afërt për mua, familjen time që me mirëkuptimin e tyre më kanë ndihmuar në realizimin e këtij punimi.

Mirënjohje dhe falënderim te veçantëshkon për udhëheqësin e temës Prof.Msc.Liridon Shurdhani i cili me kontributin , profesionalizmin dhe përkushtimin e tij më ka dhënë të gjithë suportin e nevojshëm për përfundimin e këtij punimi.

Përpunimi dhe kompletimi i këtij punimi nuk ishte aspak një detyrë e thjeshtë. Faktorët e ndryshëm siç janë ata ekonomik domosdoshëm për finalizimin e këtij punimi.

Përmbajtja

FJALORI I TERMAVE

1.SRI -(*Stanford Researches Institute*),

2. OECD- Organizata Evropiane për Bashkëpunim dhe Zhvillim Ekonomik

3. IGC- Institutin për Komunikimin Botëror

4. FBI- Byrosë Federale te Hetimeve

HYRJE

Forma e krimit kompjuterik dhe teknologjik, si dukuri ka filluar të shfaqet edhe në Kosovë. Sipas Policisë së Kosovës kjo formë e krimit, ndonëse ka filluar të shfaqet tash vonë, është duke u përhapur me të madhe dhe ka shtrirje gati në gjithë vendin.

Krimi kompjuterik, ose i njohur si formë e krimit kibernetik, tanimë ka filluar të shfaqet edhe në vendin tonë. Vetëm gjatë vitit të kaluar Policia e Kosovës ka regjistruar tetë raste të tilla. Kryesit e këtyre veprave përdorin teknologji të sofistikuar.

Sot, teknologjia informatike prek çdo sferë të jetës sonë, pa marrë parasysh vendndodhjen e saj në rruzullin tokësor. Aktivitetet e përditshme njerëzore në fushën e biznesit dhe fusha të tjera, janë pjesë e përfitimit të këtij revolucioni informatikë. Revolucioni informatikë edhe përkundër të mirave që ka ofruar, megjithatë ka edhe anën e vetë negative. Kur themi këtë, kemi parasysh faktin se të arriturat e teknologjisë së lartë në këtë fushë, i kanë hapur derën disa dukurive dhe sjelljeve kriminale, që më parë nuk kanë qenë të mundura.

Është interes dhe obligim i çdo shteti dhe individi që në mënyrë aktive dhe gjithëpërfshirëse t'i kundërvihet çdo forme të kriminalitetit, e sidomos atij kompjuterik, duke u angazhuar për ndërmarrjen e masave preventive dhe represive që kanë për qëllim parandalimin dhe luftimin e kësaj forme të re të kriminalitetit të organizuar, si brenda shtetit ashtu edhe në aspektin ndërkombëtar, dukuri kjo që përditë e më shumë po tregon shenja mjaft brengosësh me përmasa të rritjes dhe përhapjes së saj si në vendet ekonomikisht të zhvilluara ashtu edhe ato që gjenden në fazat e ndryshimeve.

Kriminaliteti si dukuri e dëmshme dhe e rrezikshme për shoqërinë që nga kohërat më të las hta ka zgjuar interesim ndër çarqet e ndryshme shoqërore. Lidhur me këtë dukuri, çysh më herët janë bërë përpjekje për të shpjeguar shkaqet dhe natyrën e saj. Për kriminalitetin që ng a kohërat e hershme janë çfaqur mendime dhe ide të ndryshme lidhur me mënyrat e pengim it dhe luftimit të kësaj dukurie.

KAPITULLI I

KUPTIMI I KRIMINALITETIT KOMPJUTERIK

1.1. Definicioni i Kriminalitetit Kompjuterik

Edhe përkundër angazhimeve të shumta të autorëve të ndryshëm për përcaktimin e definicionit të kriminalitetit kompjuterik, deri më tani nuk ekziston ndonjë definicion i pranueshëm botërisht. "Kjo formë e kriminalitetit për dallim nga format tjera, nuk paraqet ende një kategori përmbledhëse fenomenologjie dhe për këtë arsye është e pamundur të përcaktohet një definicion preciz.

Vështirësitë e definimit të kriminalitetit kompjuterik janë edhe pasojë e llojllojshmërisë së f ormave nëpërmjet të cilave paraqitet dhe shpejtësisë me të cilën ajo përhapet. Këto angazhi me kanë çuar deri te konstatimi se kriminaliteti kompjuterik ende nuk paraqet një kategori t ë përbashkët fenomenologjike.

Autori Don Parker, ka konstatuar se"kjo është një formë nëpërmjet të së cilës paraqitën lloj e të ndryshme të veprimeve kriminale, lloje këto të cilat në të ardhmen do të jenë dominant. Për këto arsye në teori dhe në praktikë, janë prezentë qasje të ndryshme në zgjidhjen e problemit të përcaktimit të kuptimit të kriminalitetit kompjuterik.

Sa i përket përcaktimit të kuptimit të kriminalitetit kompjuterik, në praktikë janë prezente d y çasje themelore. Të parët përcaktohen dhe japin definicionin ekzaktë, derisa të tjerët përkr ahin një çasje deskriptive, duke përcaktuar definicionin e kriminalitetit kompjuterik në mën yrë të tërthortë.

Në vijim, do të trajtohen mendimet e disa autorëve të cilët i përkasin grupit të cilët në mën yrë ekzakte e përcaktojnë definicionin e kriminalitetit kompjuterik, e që në numër janë më t ë shumtë. Bazuar në raportin e përgatitur për Statistikat e Byrosë së Ministrisë së Drejtësisë të SHBA-ve, SRI (*Stanford Researches Institute*), thuhet se kriminaliteti kompjuterik definohet si: "çdo krim për të cilin kryesi duhet të ketë njohuri teknike mbi kompjuterët, me qellim që në ta të ndërhyjë".

Sipas doracakut të përgatitur për prokurorë (*Computer Crime, Criminal Justice Manual, 1979)*, kriminaliteti kompjuterik definohet si: "çdo akt ilegal për të cilin ndjekja është e suksesshme si dhe njohja esenciale e teknologjisë kompjuterike".

Ky definicion i cituar më lartë është zgjeruar, në punimet e seminarit të organizuar nga e Interpolit në Francë më 1981, në të cilin thuhet: "kriminalitet kompjuterik është çdo akt ilegal ku për kryerjen e suksesshme të tij, hetimin, ndjekjen ose dënimin, nevojitet njohje esenciale e teknologjisë kompjuterike" . Po ashtu, edhe një delegacion suedez i cili merrte pjesë në konferencën e dytë Nordike mbi debatin rreth kriminalitetit ekonomik, i mbajtur në vitin 1983 në Helsinki, ka prezantuar definicionin se: "kriminaliteti kompjuterik është krim i kryer kundër ose me ndihmën e sistemit kompjuterik, nga dikush që në kryerjen e veprës kriminale, shfrytëzon njohuritë mbi teknologjinë kompjuterike".[1]

Edhe Organizata Evropiane për Bashkëpunim dhe Zhvillim Ekonomik OECD, në Paris në v itin 1983, ka dhënë definicionin lidhur me kriminalitetin kompjuterik të cilin e trajton si: "ç do veprim ilegal, joetikë dhe sjellje të pa autorizuar në përpunimin e të dhënave ose bartjen e tyre në mënyrë automatike".

Lidhur me definicionin e kriminalitetit kompjuterik, Policia Federale Gjermane në vitin 198 3, për herë të parë kishte trajtuar kriminalitetin kompjuterik, në konstatimin e saj thuhet: "m e kriminalitet kompjuterik kuptohen të gjitha sjelljet në të cilat paisjet për përpunimin e të d hënave shfrytëzohen si mjete për arritjen e rezultateve të dënueshme, ose si cak direkt i vep rimit të dënueshëm".

Kah fundi i vitit 1983, definicioni i përmendur ka pësuar ndryshime duke u shndruar në një definicion të ri më të kompletuar dhe më të kuptueshëm ku thuhet se: "kriminaliteti kompju terik përmban mashtrimin kompjuterik, spiunazhin kompjuterik si dhe keqpërdorimin komp juterik".Sipas konstatimeve të disa autorëve, kriminaliteti kompjuterik definohet vetëm për ato vepra penale, të cilat nuk mund të kryhen pa një njohuri të veçantë, apo ato vepra të cila t nuk mund të kryhen pa ndihmën e kompjuterit.

Lidhur me këtë, ekziston definicioni sipas të cilit: "kriminaliteti kompjuterik përmbanë të g jitha ato vepra të kryera me ndihmën e dijës së veçantë mbi shfrytëzimin profesional të tekn ologjisë kompjuterike".Mendim të njëjtë ka çfaqur edhe autori Taber, i cili konstaton se "de

[1]NedžadKorajlić "KriminalistićaMetodika", Sarajevo 2008,faqe 82

likti kompjuterik duhet të përmbajë operacione të larta profesionale në kompjuterë, nën kus htet kur deri të shkelja nuk mund të vihet në ndonjë mënyrë tjetër"

Autori Urlich Sieber, ka paraqitur definicionin e tij lidhur me kuptimin e kriminalitetit kom pjuterik, në të cilin thuhet: "se kriminaliteti kompjuterik përfshinë shkeljet e kundërligjshm e të pronës, tek të cilat të dhënat e përpunuara në mënyrë elektronike me vetëdije ndryshohe n (manipulimi kompjuterik), shkatërrohen (sabotazhi kompjuterik), në mënyrë të paautorizu ar shfrytëzohen (spiunazhi kompjuterik).[2]

Në mesin e autorëve, ka edhe të atillë të cilët konstatojnë se këto delikte nuk ekzistojnë, nga se këto keqpërdorime mund t'i nënshtrohen inkriminimeve ekzistuese. Konstatimet e tilla n uk mund të jenë të pranueshme, duke pasur parasysh specifitetin dhe objektin e vepres si dh e format e kryerjes.[3]

Edhe autori Dragicevic, këto konstatime i konsideron si jo të qëndrueshme, nëse jo për diçk a tjetër, atëherë për atë se nuk llogaritet për specificitetin e objekteve jo trupore (të dhënave kompjuterike dhe programeve) integritetin dhe fshehtësinë e të cilave duhet mbrojtur.

Lidhur me kuptimin e kriminalitetit kompjuterik, eksperti i njohur botëror në fushën e krim inalitetit kompjuterik Don Parker, vëmendjen e tij e kishte përqëndruar në trajtimin shkenco r të këtij problemi. Ky autorë, kriminalitetin kompjuterik e definon si: "çdo veprim në lidhje me përdorimin e teknologjisë kompjuterike, me të cilin viktima përjeton ose mund të përjetoj humbje, ndërsa kryesi vepron me qëllim që vetës t'i krijoj përfitim"

Duke trajtuar mendimet e autorëve të ndryshëm nga literatura e disponueshme lidhur me ku ptimin dhe definicionin e kriminalitetin kompjuterik, autori V.Vula ka konstatuar se ''krimi naliteti kompjuterik është një formë e veçantë e kriminalitetit, në të cilën kompjuteri paraqit et si mjet për kryerjen e veprimit ilegal apo si objekt sulmi, i drejtuar nga personat të cilët posedojnë njohuri dhe prirje të veçanta për sistemet kompjuterike, me qëllim që vetës apo të tjerëve tu sjellin përfitime''.[4]

[2]NedžadKorajlić "KriminalistićaMetodika", Sarajevo 2008,faqe 83,
[3]Mr. sc. FatosHaziri "E Drejta E Policisë", Prishtinë 2010, faqe 17,
[4] file:///F:/Kriminaliteti%20kompjuterik%20dhe%20historiku%20i%20tij_ppt.htm

1.2. Trajtimet Teorike E Juridike Të Kriminalitetit Kompjuterik

Kriminaliteti si dukuri e dëmshme dhe e rrezikshme për shoqërinë që nga kohërat më të las hta ka zgjuar interesim ndër çarqet e ndryshme shoqërore. Lidhur me këtë dukuri, çysh më herët janë bërë përpjekje për të shpjeguar shkaqet dhe natyrën e saj. Për kriminalitetin që ng a kohërat e hershme janë çfaqur mendime dhe ide të ndryshme lidhur me mënyrat e pengim it dhe luftimit të kësaj dukurie.

Gjatë fazave të ndryshme të zhvillimit të shoqërisë, për shkaqet dhe karakterin e kriminalite tit, janë dhënë mendime dhe konstatime të ndryshme e shpeshherë edhe të gabuara.

Kriminaliteti si dukuri shoqërore negative, me kalimin e periudhave të ndryshme kohore ës htë paraqitur në forma të ndryshme, të cilat kanë lënë pas vete edhe veçoritë dhe karakterist ikat e veta të veçanta. Në këtë drejtim, janë për tu përkrahur, mendimet e autorëve në literat urën kriminologjike, në të cilën theksohet se: ”vëllimi, format e krimeve dhe sjelljeve krimi nale, kanë qenë të lidhura ngushtë me zhvillimin dhe transformimin e shoqërive dhe sistem eve të caktuara shoqërore-ekonomike.

Ky proces i varëshmërisë së formave të kriminalitetit nga transformimet e veçanta shoqëror e, veçmas vërehet në shoqëritë bashkëkohore, ku brenda afateve të shkurta kohore në vende t e ndryshme, ose në të njëjtin vend, vërehen forma dhe lloje të reja të manifestimit të krimi nalitetit.

Bazuar në literaturën e cila trajton format e ndryshme të kriminalitetit të organizuar, hasim në një formë të re të manifestimit të kriminalitetit në botën bashkëkohore, atë të kriminalitet it kompjuterik. [5]

1.3. Krimet Tradicionale Dhe Krimet Kompjuterike

Në dallim nga krimet tradicionale, krimi kompjuterik është një krim global. Këto lloj krimesh, kryhen përmes hapësirave dhe rrjeteve kompjuterike dhe nuk ndalojnë në kufijtë konvencionale shtetërorë. Ato mund të parapërgatiten nga kudo dhe kundër një përdoruesi kompjuteri në një vend çfarëdo të globit.

[5] file:///F:/Kriminaliteti%20kompjuterik%20dhe%20historiku%20i%20tij_ppt.htm

Përveç rritjes së shkallës së aktivitetit kriminal në shkeljet me natyrë të krimeve kompjuterike, ka një tendencë për t'iu shmangur kategorive tradicionale të shkeljeve. Kur një pjesë e kategorive konsiston në përdorimin e teknologjive të informacionit për të kryer një krim tradicional, krimi kompjuterik mund të manifestojë veten si një varietet i ri i aktivitetit, i cili nuk mund të ndiqet duke iu referuar kategorive tradicionale të shkeljeve.[6]
Rasti "Virusi i Dashurisë " e ka vërtetuar këtë. Ekspertët shumë shpejt zbuluan virusin që vinte nga Filipinet. Duke përdorur informacionin e marrë prej një Shërbimi Shpërndarës të internetit, hetuesit e Agjencisë Kombëtare të Hetimit në Filipine dhe ata të FBI-së, identifikuan personat e dyshuar për shpërndarjen e virusit. Megjithatë, pati disa probleme lidhur me hetimin, për shkak të mungesës së ligjeve specifike, kështu që krijimi dhe përhapja e një virusi nuk ishte një krim. Në këtë rast, hetuesit nuk kishin kohën dhe mundësitë e duhura për të hetuar, gjetur prova dhe dënuar autorin.
Papërshtatshmëria e ligjeve aktuale apo mungesa e tyre, për të vepruar mbi format e reja të aktiviteteve antishoqërore, si krimet kompjuterike, si dhe mangësitë e ligjeve ekzistuese penale në këtë drejtim, krijojnë një sfidë permanente për të gjithë ligjvënësit e botës .Nga ana tjetër, shkelësit kanë aftësinë për të shfrytëzuar boshllëqet e ligjeve të vendeve të tyre, por edhe të tjera, për të viktimizuar qytetarët, duke mbetur kështu pa u ndëshkuar. Në këtë kuptim, krimi kompjuterik është një krim global.[7]

Të ndodhur para këtyre problemeve, shumë vende orvaten të caktojnë kufijtë e tyre përmes mekanizmave filtrues dhe ndërtimit të pengesave elektronike. Vende të tjerë kanë shpallur, me të shpejtë, të drejtën për të rregulluar të gjitha rrugët e komunikimit të drejtpërdrejt, sa një gjë e tillë mund të duket si një kontroll kundër qytetarëve. Aktualisht, në Shqipëri, ka një mungesë serioze të kornizës ligjore mbi këto lloj krimesh.[8]

[6]By Michael Barrett, Andy Steingruebl, Bill Smith, Principles, Policies, and Programs | April 2011, faqe 100,

[7]By Michael Barrett, Andy Steingruebl, Bill Smith, Principles, Policies, and Programs | April 2011, faqe 101,

[8]http://sq.wikipedia.org/wiki/Krimi_kompjuterik

KAPITULLI II

KRIMI KIBERNETIK – SFIDË PËR SHOQËRINË E SOTME

2. KRIMI KIBERNETIK – SFIDË PËR SHOQËRINË E SOTME

Ky fenomen prek jo vetëm aktivitetet e një organizmi qoftë ai shtetëror apo privat, i implikuar në sferën e biznesit apo të një aktiviteti jo fitimprurës, por mund te prekë dhe njeriun e thjeshtë në aktivitetin e tij të përditshëm, në sferën e tij private apo profesionale. Si çdo teknologji e re e vënë në dispozicion të një numri të madh përdoruesish, Interneti paraqet jo vetëm të mira dhe përfitime, por në të njëjtën kohë dhe një sërë problemesh. Duke qenë një teknologji "e liberalizuar" prej disa kohësh, siç përdoret në zhargon, nuk ia vlen të zgjatemi në diskutimin e përfitimeve që sjell përdorimi i kësaj teknologjie. Anën e përfitimeve mund ta përmbledhim për momentin në një frazë te vetme: komunikim (në kuptimin e gjerë të fjalës) i shpejtë, i pakushtueshëm dhe tërësisht i pavarur nga nocioni i distancës.[9]

Në këtë artikull do të përqendrohemi kryesisht në shmangien që i bëhet qëllimit primar të përdorimit të kësaj teknologjie (komunikimit). Keqpërdorimi i saj nga elementë kriminelë njihet me emrin krim kibernetikë (*cybercrime*). Në praktikën e përditshme konstatohen dy lloj sjelljesh përballë fenomenit të krimit kibernetikë. Në njërën anë kemi përdoruesin e përditshëm i cili udhëhiqet shumë shpesh nga ideja që "e keqja shkon gjithmonë tek të tjerët". Në anën tjetër, kemi specialistët e fushës që udhëhiqen diametralisht nga kundërta, domethënë që " të tërë jemi të barabartë, të paktën në terma matematike, ndaj probabilitetit të të qenit objekt i një sulmi kriminel". Ndryshe nga përdoruesi i zakonshëm, specialisti i kushton kohë analizës së fenomenit për të kuptuar funksionimin e tij. Duhet theksuar fakti që në asnjë moment dhe në asnjë rrethanë nuk duhet të biem pre e idesë që një ditë këtë

[9]ElmedinMuratbegoviq, ParandalimiiKriminalitetit(Compendium of Crime Prevention and Crime Control), Sarajevë / Prishtinë, prill 2007, faqe 56,

probabilitet mund ta bëjmë zero.[10] Ky pohim merr një rëndësi të madhe kur ka të bëjë për më shumë me teknologjitë e reja dhe me sigurinë informatike.

Pra ç ’është krimi kibernetikë, nga vjen, çfarë e ndihmon të jetë kaq i përhapur, si mundemi ta parandalojmë dhe a jemi të përgatitur përballë këtij fenomeni? Këto janë disa pyetje që specialistët, qofshin këta njohës të informatikës, specialistë të sistemeve të informacionit, kriminologë, juristë, ekonomistë e të tjera, mundohen t’i trajtojnë në aktivitetin e tyre të përditshëm.

Në fakt krimi kibernetikë duhet distancuar pak nga një nocion i përgjithshëm i asaj që quhet krimi informatikë. Ky i fundit lidhet me një aktivitet kriminal që ka si objekt apo si mënyrë të kryerjes së krimit, kompjuterin. Krimi kibernetikë pra është në këtë prizëm një nën kategori e krimit informatikë dhe ka të bëjë me veprimtarinë kriminale të zhvilluar në rrjet (*network*). Interneti është një nga rrjetet më globalë dhe më të përdorur sot.

Pas këtij saktësimi mundemi te evidentojmë që qenia në rrjet na ekspozon ndaj rrezikut të një sulmi të mundshëm. Do të ishte joprofesionale këshilla e një shkëputjeje nga rrjeti, sepse në strukturën ekonomike të sotshme gjithnjë e më shumë globale, shkëputja do të shndërronte organizmin në një organizëm jo konkurrent.

Një aspekt tjetër që duhet trajtuar për të kuptuar fenomenin e krimit kibernetikë është dhe teknologjia e përdorur. Një përdoruesi të zakonshëm kompjuteri apo Interneti, që nga momenti që çdo gjë funksionon normalisht për të, nuk i intereson më se çfarë veprimesh, përllogaritjesh apo protokollesh kryen kompjuteri për të arritur në këtë rezultat. Nga ana tjetër prodhuesit e programeve, pajisjeve, ISP etj., nuk është se kanë një vullnet spontan të informojnë përdoruesin mbi mënyrën e funksionimit dhe për të qenë koherentë kjo gjë do të ishte jo realiste. Pra si përfundim teknologjia mbetet pak a shumë jo transparentë për përdoruesin.[11]

Përsa i përket Internetit, disa faktorë të tjera bëjnë që kjo teknologji të jetë e cenueshme dhe për rrjedhojë një terren shumë përshtatshëm për zhvillimin e krimit.

[10]Sam Lumpkin Senior Security Architect, 2AB, Inc. Internet Security and CyberCrime, faqe 20,

[11]Sam Lumpkin Senior Security Architect, 2AB, Inc. Internet Security and CyberCrime, faqe 21,

- Nga një këndvështrim teknologjik mund të përmendim faktin që Interneti është një teknologji publike dhe e hapur për të tërë. Historikisht, rrjeti komunikues u zhvillua si një mjet i fushës ushtarake për t'u përdorur më pas nga universitarët për të lehtësuar komunikimin ndërmjet tyre.

Ky vizion mbi përdorimin bëri që në fillesat e saj, teknologjia e Internetit të mos përfshinte aspektin e sigurisë përderisa komunikimi (si në rastin ushtarak ashtu dhe në atë universitar) bëhej ndërmjet njerëzve që njiheshin e që kishin besim tek njëri tjetri. Teknologjia e Internetit është një teknologji që ofron mundësi më të mira. Kjo do të thotë që në konceptimin e saj "bëmë atë çka mundëm" për të arritur në rezultatin e dëshiruar, pa imagjinuar se çfarë devijimi mund t'i bëhej përdorimit të tij.

- Nga një këndvështrim i rrjetit dhe i sistemit, në rastin e Internetit kemi të bëjmë me një liri të madhe përsa i përket konfigurimit, mënyrës së trajtimit në segmentet e sigurisë dhe ç 'është më e rëndësishme në rastin tonë, mungesës totale të kontrollit. Jo më kot Interneti identifikohet si "rrjeti i rrjeteve" dhe shpesh struktura e tij krahasohet me rrjetën e merimangës.

- Nga një këndvështrim legal, Interneti është i konceptuar dhe funksionon në një mënyrë të tillë, që për të nocioni i kufijve nuk ekziston. Në fushën juridike një krim në radhë te parë sanksionohet nga një ligj. Ky ligj i përket një shteti të caktuar dhe zbatohet nga një gjykate kompetente e një shteti të caktuar. Nocioni i shtetit është i lidhur ngushtë me nocionin e territorit pra me kufijtë shtetërore. Kjo ndikon shumë në fazën e përndjekjes së krimit. Imagjinoni një pirat informatikë që kryen aktin e tij kriminal nga Kina le të themi, duke sulmuar një bankë në Zvicër dhe duke derdhur shumën e vjedhur në formë elektronike në Itali. Cili institucion gjyqësor dhe cili ligj është kompetent në këtë rast? Kina vendi nga i cili autori kreu krimin, Zvicra vendi ku ndodhet viktima apo Italia vendi ku u realizua rezultati? Tre vende kaq të ndryshme përsa i përket vendndodhjes, kulturës juridike dhe perceptimit të nocionit të krimit a do të munden të bien dakord për përndjekjen dhe gjykimin e këtij akti? Përgjigjja nuk është shumë evidente.

- Së fundmi, në qoftë se konsiderojmë problemin nga një këndvështrim i përdoruesit atëherë kemi prekur thembrën e Akilit.

A është përdoruesi i ndërgjegjshëm për pasojat që mund t'i sjellë përdorimi i Internetit? Përgjigjja është negative në më të shumtën e rasteve.[12]

Në një emision të transmetuar së fundmi në një nga televizionet shqiptare, një drejtues banke solli si argument faktin që programet bankare janë aq të sofistikuara sa është shumë e vështirë të "thyhen", gjë që paraqet një pjesë të së vërtetës.

Në momentin që operacionet bankare kryhen në rrjet, siç është dhe rasti i e-banking i cili po fillon të praktikohet dhe në Shqipëri, përdoruesi është i cenueshëm pavarësisht nga forca dhe algoritmet e përdorura në software-t e bankës. Ka dhe një fakt tepër të rëndësishëm që duhet theksuar : krimi do të kërkojë të godasë viktimën më të dobët, më të papërgatitur, pra shënjestrën më tërheqëse për të.

Eksperienca na tregon që mbi 50% e sulmeve kanë si objekt personin. Por edhe nëse marrim në konsideratë organizmin e bankës më vete dhe faktin e software-ve të sofistikuar, eksperienca në fushën e krimit kibernetikë ka treguar se mbi 70% e sulmeve kanë zanafillë të brendshme. Kjo mund të vijë nga një vartës i pakënaqur, një vartës i pirur thjesht nga përfitimi etj. Lista e motivimeve është e gjatë. Në këtë aspekt kompleksiteti teknologjik nuk ndihmon shumë dhe është struktura menaxheriale e institucionit dhe gjithë aspektet përbërëse të saj që marrin një rëndësi të veçantë. Në emisionin në fjalë u soll si shembull më të drejtë niveli i kontrollit shumë rigoroz mbi personelin që njihet si "menaxhimi nëpërmjet frikës" (*fear management*). Por në të njëjtën kohë rezultatet e kësaj strategjie janë shumë të diskutueshme në rrethet e profesionistëve të burimeve njerëzore. Për mendimin tonë, duke konsideruar shkallën e lartë të rëndësisë së sistemeve të informacionit në mbarëvajtjen dhe mbijetesën e organizmit, do kishim anuar më shumë në një stil menaxhimi të fokusuar mbi komunikimin, edukimin dhe sensibilizimin e vartësve mbi pasojat si në nivel personal ashtu dhe atë profesional. Kjo, duke shpjeguar se teknologjia nuk mundet të zgjidhë e vetme problemet që lidhen me sigurinë informatike dhe me krimin informatikë dhe që faktori human ka një rëndësi të rangut të parë.[13]

[12]Sam Lumpkin Senior Security Architect, 2AB, Inc. Internet Security and CyberCrime, faqe 22,

[13]Doc. Dr. sc. Nedžad Korajlic, Metodika Kriminalistike(deliktet e gjakut, seksuale, pasurore)Sarajevë / Prishtinë 2007FSK/S - 15/06, faqe 80,

Për t'ju rikthyer nocionit të krimit kibernetikë dhe për të kuptuar atë që quhet *modus operandi* të kryerjes së krimit duhet t'i referohemi teorisë së trekëndëshit që citohet shpesh në literaturën e kriminologjisë. Kjo teori na tregon se për të kryer një krim duhet që në të njëjtën kohë të kemi një koordinim të tre faktorëve: të një krimineli të motivuar, të një objekti vulnerabil të cilët ndodhen në të njëjtin vend, në të njëjtën kohë.[14]

Duke u nisur nga kjo teori dhe duke konsideruar elementët që cituam më sipër:
- njohjen e kufizuar të Internetit nga ana e përdoruesit,
- motivimin, mundësinë dhe lehtësimet që kanë kriminelët për të kryer aktin kriminal nëpërmjet Internetit,
- vendin e takimit ideal dhe konstant siç është rrjeti mund të kolaudojmë që krimi kibernetikë është dhe do të bëhet gjithnjë e më shumë një terren shumë tërheqës për kriminalitetin. Praktika tregon që krimi i organizuar ka kuptuar tashmë rëndësinë dhe përfitimin nga fenomeni i krimit kibernetikë. Anonimiteti që ofron Interneti bën që krimi i organizuar po fillon dalëngadalë të interesohet dhe të marrë ne dorë frenat e këtij fenomeni. Si shembull, mund të marrim rastin e Bankës së Sicilisë në vitin 2000, ku një grup prej 20 personash, natyrisht me njohuri specifike në fushën e informatikës dhe të lidhur me disa familje mafioze, arritën të krijonin një klon të sistemit e-banking të bankës. Kështu arritën në këtë mënyrë të përvetësonin shumën prej 400 milionë $ të vëna në dispozicion nga Komuniteti Evropian për zhvillimin rajonal. Pasi përvetësuan shumën në fjalë, ata përdorën sisteme të tjera bankare *on-line* për t'i pastruar këto para dhe për të humbur gjurmët duke implikuar banka të njohura si Bankën e Vatikanit, disa banka në Zvicër dhe në Portugali. Në këtë stad duhet theksuar dhe fakti që për të mos rënë në sy, shumat e përvetësuara nga krimi kibernetikë, janë në më të shumtën e rasteve, shuma të vogla parash.[15] Sipas raportit IC3 2004 Internet Fraud – Crime Report 43% e shumave të përvetësuara nuk janë më shumë se 100 $ për akt dhe 25.6% nuk e kalojnë 1000$. Pra është shumë e vështirë për të tërhequr vëmendjen e specialistëve apo për të justifikuar një procedurë gjyqësore.

[14]Jonathan Clough, Principles Of Cybercrime, Faculty of Law, MonashUniversity, Jonathan Clough 2010, faqe 55,

[15]Jonathan Clough, Principles Of Cybercrime, Faculty of Law, MonashUniversity, Jonathan Clough 2010, faqe 56,

Është e kuptueshme që një artikull nuk mund të trajtojë në detaj gjithë përbërësit e fenomenit të krimit kibernetikë. Mesazhi i cili deshëm të përcillnim është që krimi kibernetikë është një fenomen që prek një sërë kompetencash, si ato në fushën e informatikës, kriminologjisë, ekonomisë, drejtësisë etj. Krimi kibernetikë është pra, një fenomen kompleks dhe e vetmja mënyrë për t'i bërë ballë do të ishte një mënyrë globale e trajtimit të problemit. Për këtë duhet një bashkëpunim i gjithë ekspertëve të fushave të sipërpërmendura për të shmangur zgjidhjet segmentare.

Për këtë është e rëndësishme të konceptojmë një arkitekturë globale të sigurisë së informacionit që të marrë në konsideratë brenda saj dimensionin teknik dhe operacional, dimensionin juridik dhe rregullator, dimensionin organizativ dhe ekonomik duke mos harruar dimensionin human.[16]

2.1. Kriminaliteti Kompjuterik Si Formë E Re E Fenomenologjisë Kriminale

Pra, siç u tha më lartë, shfrytëzimi i kompjuterit si mjet për fshehjen, planifikimin, organizimin dhe realizimin e veprimeve kriminale, është i një rëndësie të veçantë. Me ndihmën dhe përdorimin e kompjuterëve, individëve apo grupeve kriminale u lehtësohen punët në lidhje me udhëheqjen dhe kontrollin e veprimtarive të tyre ilegale, në kuptim të realizimit të qëllimeve të tyre kriminale, në mënyrë të shpejtë dhe kualitative, kjo veçanërisht shprehet kur janë në pyetje transaksionet e mëdha financiare miliona dollarësh.[17]

2.2. Kompjuteri si mjet për fshehje, planifikim, organizim dhe udhëheqje në Realizimin e veprimit kriminal

Një nga zbulimet më të rëndësishme të zhvillimit dhe civilizimit tekniko-teknologjik është kompjuteri. Mirëpo, pavarësisht nga përparësitë dhe mundësitë që i ka sjellë, kompjuteri

[16] "http://sq.wikipedia.org/w/index.php?title=Krimi_kompjuterik&oldid=1325191,
[17] Carter L.D."Computer Crime Categories:"How Techno-criminals Operate" FBI Law Enforcement

shumë shpejt është gjendur si vegël për keqpërdorim në duart e grupeve apo organizatave të ndryshme.

"Duke iu falënderuar mundësive të mëdha që ofron kompjuteri, ai mund të shfrytëzohet si vegël shumë e fortë dhe precize në planifikimin, organizimin dhe udhëheqjen e veprimeve kriminale, qoftë nga ana e individit apo edhe e organizatave kriminale. Në këtë drejtim kompjuteri gjithnjë e më shumë shfrytëzohet në fushën e kriminalitetit të organizuar posaçërisht në fazën e përgatitjes dhe të planifikimit të veprimtarisë kriminale si dhe në procesin e kontrollit dhe të mbikëqyrjes së realizimit të procesit të fundit e veçanërisht në realizimin e efekteve financiare."[18] Mund të thuhet se shfrytëzimi i kompjuterit nga ana e individëve apo grupeve, ka mundësuar atyre që veprimet e tyre kriminale t'i planifikojnë dhe organizojnë në mënyrë të shpejtë, precize dhe kualitative. Kjo bëhet sidomos në rastet kur është në pyetje mbajtja dhe kontrolli i sistemit të madh bankar të nëntokës.[19]

"Kompjuteri mund të ndihmojë që veprimet kriminale të kryhen shpejt dhe saktë, duke mundësuar përpunimin e një vëllimi të madh informacionesh dhe duke e bërë të vështirë identifikimin dhe zbulimin e këtyre veprimeve. Në këto veprime kriminale hyjnë: udhëheqja e librave të kontabilitetit (librat e dyfishta), larja e "parave të ndyta", afarizmi i paligjshëm bankar dhe veprime të tjera"[20]

"Rol gjithnjë e më të madh në këtë kontest po luan edhe Interneti me shërbimin e vet të postës elektronike (E-mail), i cili ofron mundësi të mëdha të komunikimit të shpejtë dhe të sigurt, në çdo kënd të botës që për krimin e organizuar ka rëndësi të madhe".[21]

---

[18] Dr.Vesel Latifi: Kriminalistika, Prishtinë, 2004, fq. 288.

[19]CyberCrime@IPA Projekt i Përbashkët BE/KiE për Bashkëpunimin Rajonal kundër Krimit Kompjuterik, Dubrovnik, Kroaci, 15 shkurt 2013, faqe 13,

[20] Carter L.D."Computer Crime Categories:"How Techno-criminals Operate" FBI Law Enforcement

[21] http://www.nsi.org/Library.Compsec/crimecom.html

KAPITULLI III

TERRORIZMI DHE SPIUNAZHI KOMPJUTERIK

3.1. TERRORIZMI KOMPIUTERIK

Terrorizmi kompjuterik është një ndërthurje e terrorizmit dhe hapësirës kompjuterike. Ai është përkufizuar si një sulm i paramenduar, politik, i motivuar kundër informacionit, sistemeve a programeve kompjuterike, dhe të dhënave të cilat pasojnë në dhunë, kundër shënjestrave nga grupeve ndërkombëtare apo agjentë klandestinë. Sulmet që shkaktojnë vdekje, dëmtime trupore, shpërthime, rënie avionësh, kontaminim uji apo humbje të ndryshme ekonomike, mund të jenë shembuj. Sulme të rrezikshme mund të kryhen ndaj infrastrukturës dhe të jenë krime kompjuterike, në varësi të impaktit të tyre. Hapësira kompjuterike është nën presion. Spiunët kompjuterikë, hajdutët, sabotatorët, të cilët me një energji të paparë kërkojnë të futen në sisteme kompjuterike, të dhënat personale dhe ato sekrete, keqpërdorin faqet e internetit, shërbimet e shpërndarjes, sabotojnë të dhënat dhe sistemet, lëshojnë veruesekompjuterike, kryejnë transaksione mashtruese, dhe ngacmojnë individë apo kompani. Këto sulme janë lehtësuar me rritjen dhe përdorimin e mjeteve elektronike të fuqishme, të cilat janë lehtësisht të kapshme në dorë përmes shërbimeve të ndryshme të web siteve apo internetit.[22]

Shumë prej sulmeve janë serioze dhe me dëme. Në 1998, protestues Spanjollë bombarduan" Institutin për Komunikimin Botëror, IGC, me qindra e-mail false. Ato ishin të lidhur dhe ishin të padeshifrueshëm për ISP-të e përdorueseve, dhe përdornin linja që kishin lidhje me njerëz që nuk mund të gjenin e – mailet e tyre. Po këtë vit, një 12 vjeçar piratoi në mënyrë të suksesshme në kontrollin e digave të njohura Rossvelt Dam, mbi Lumin Salt në Arizona. Ai mund të lëshonte portat e digës, të cilat mund të kishin përmbytur pa frikë banorët përreth, duke kërcënuar rreth 1 milion njerëz.

[22]Prosecuting Computer Crimes Computer Crime and Intellectual Property Section Criminal Division, See United States v. Caceres, 440 U.S. 741 (1979),faqe 82,

3.2. Dukuria Shoqërore E Terrorizmit Kompjuterik Nuk Është Më Një Mit, Por Një Realitet

Gjatë njëzet viteve të fundit, përdoruesit e zgjuar të kompjuterit, duke përdorur kompjuterët e tyre për të kryer krime kanë shtangur botën dhe kanë krijuar një ndjenjë të çuditshme, të përbërë nga admirimi dhe frika. Industria e argëtimit i ka kuptuar këto emocione shpejt dhe për këtë arsye vazhdimisht ka botuar dhe lëshuar në qarkullim libra të rinj, filma dhe shfaqje që përfaqësojnë kriminelët kompjuterikë që janë në veprim dhe duke kërcënuar botën nga kompjuterët e tyre.

Në shoqërinë aktuale, varësia nga teknologjia kompjuterike është ne rritje e sipër dhe ka marrë një zhvillim të hovshëm. Digjitalizimi i proceseve të punës në të gjitha sferat e jetës shoqëroro-ekonomike në kohët e sotme është një fenomen i vërtetë dhe në avancim e sipër. Zhvillimi i tregtisë botërore gjithnjë e më shumë anon nga zhvillimi i teknologjive të kompjuterit dhe internetit. Në zhvillim të vazhdueshëm të kësaj industrie, është bërë një ndjeshmëri e veçantë ndaj shfrytëzimit të kompjuterëve për krime të ndryshme kompjuterike dhe terrorizëm kompjuterik.[23]

Në bazë të studimeve të kryera, janë arritur përkufizime të ndryshme të terrorizmit edhe përmes internetit. Kuptimi primar që mund t'i atribuohet terrorizmit kompjuterik është etimologji që origjinën e ka nga idetë e themeluara në hapësirën kompjuterike dhe të terrorizmit.

Terrorizmi kompjuterik është një sulm që synon pikën e ndërprerjes midis botës materiale apo botës së konsiderueshme dhe botës virtuale. Në epokën e tanishme, integrimi i botës virtuale dhe teknologjike me botën që ne e jetojmë, është shumë e qartë se ka mjetet e përbashkëta. Kjo tendencë, në fakt është bërë, si kornizë për krijimin e shumë agjencive dhe organizatave për mbrojtje nga terrorizmi kompjuterik. Për këtë arsye, ato janë bërë objekt i sulmeve të terrorizmit kompjuterik. Krejt kjo është për shkak të faktit se qëllimi për shkatërrimin e sistemit që funksionon, mund të bëjë realizimin e qëllimeve të autorëve me më pak përpjekje dhe me më pak shpenzime.

[23] CyberCrime@IPA Projekt i Përbashkët BE/KiE për Bashkëpunimin Rajonal kundër Krimit Kompjuterik, Dubrovnik, Kroaci, 15 shkurt 2013, faqe 66,

Bazuar në studimet e deritashme mbi terrorizmin përmes internetit, terrorizmi kompjuterik është "përdorim i paramenduar i aktiviteteve shkatërruese, që kanë për qëllim objektivat sociale, ideologjike, fetare, politike ose të ngjashme, ose edhe për të trembur çdo person" në lidhje me objektivat e lartpërmendura. Ekziston një nevojë për të rritur vetëdijen e popullsisë së përgjithshme në lidhje me kuptimin e terrorizmit përmes internetit dhe kërcënimeve të mundshme që ai mund të sjellë për shkak të përdorimit të teknologjisë nga terroristët, e që me kohë është duke fituar edhe pushtetin.

Sipas Byrosë Federale te Hetimeve (FBI), terrorizmi kompjuterik është sulm i paramenduar me motive politike kundër sistemeve kompjuterike, sistemeve të informacionit, programeve kompjuterike, objektivave ushtarake dhe të dhënave të cila rezultojnë me dhunë kundër objektivave luftarake kombëtar nga agjentët e fshehtë. Ndryshe nga një virus bezdisës, një sulm kompjuterik terrorist është projektuar për të shkaktuar dhunë fizike ose të dëmtojë në mënyrë ekstreme shërbimet financiare.[24]

Sipas Komisionit Amerikan të Mbrojtjes së Infrastrukturës Kritike (U.S. Commission of Critical Infrastructure Protection), objektivat e mundshme të terrorizmit kompjuterik përfshijnë industrinë bankare, instalimet ushtarake, termocentralet, qendra e trafikut ajror, dhe sistemet e ujit.

Terrorizmi kompjuterik është referuar disa herë si terrorizmi elektronike ose lufta e informacionit.

Thjesht terrorizmi kompjuterik është përdorimi i sistemit kompjuterik dhe i rrjetit të internetit që përmes tyre të dizajnohet dhe ndërmerret një sulm terrorist. Është fakt i kohës që ndokush apo disa grupe do të përdorin metodat e kompjuterit të bëjnë një sulm ushtarak apo sulm terrorist kundër caqeve te caktuara.

Terrorizmit kompjuterik, apo krimit elektronik, i referohet çdo krim që përfshin një kompjuter dhe një rrjet. Kompjuteri mund të ketë qenë përdorur në kryerjen e një krimi, ose ajo mund të jetë objektiv. Terrorizmi kompjuterik i referohet shfrytëzimit penal të internet.

[24]CyberCrime@IPA Projekt i Përbashkët BE/KiE për Bashkëpunimin Rajonal kundër Krimit Kompjuterik, Dubrovnik, Kroaci, 15 shkurt 2013, faqe 67,

Krime të tilla terroriste mund të kërcënojnë shëndetin e një kombi dhe sigurinë financiare. Çështjet që lidhen me këtë lloj krimi janë bërë të profilit të lartë, veçanërisht ato plasaritjet përreth, e drejta e autorit, pornografinë e fëmijëve, dhe trafikimi me qeniet njerëzore. Ka edhe probleme të intimitetit kur konfidencialiteti i informacionit është humbur apo përgjuar në formë të paligjshme apo ndryshe.

Terrorizmi kompjuterike është kërcënim serioz i krahasuar me armët bërthamore, bakteriologjike dhe kimike dhe është një krim që ende nuk ka mundur të hetohet deri në fund. Për ta zbuluar dhe neutralizuar ketë formë virtuale të terrorizmit është shumë e vështirë për shkak se këtu nuk mbeten shumë gjurmë nëse krahasohet me boten reale ku gjurmët mbeten mjaft shumë. Sikurse terroristët e zakonshëm që për arritjen e qëllimeve përdorin eksploziv ose një armë të vogël, terroristët kompjuterikë përdorin teknologjinë dhe sistemet moderne të informacionit, rrjetet e sistemeve kompjuterike, softuerë të posaçëm të paautorizuar ligjërisht për arritjen e qëllimeve të caktuara.

Janë me dhjeta vende që tashmë kanë përjetuar goditjet sporadike dhe të egra nga terrorizmi i segmenteve të caktuara të një vendi dhe nga ai i sponsorizuar nga shtete të ndryshme. Në dallim nga terrorizmi i mëhershëm për nga tiparet, terrorizmi i sotëm ka filluar të përdorë një variant të ri të luftës lidhur me teknologjinë, viktimizimet, kërcënimet dhe reagimet.

Masakra shkatërrimtare terroriste më e madhe e regjistruar ndonjëherë ndodhi më 11 shtator 2001 në SHBA. Njëmbëdhjetë terroristë rrëmbyen katër avionë pasagjerësh, dy nga të cilët i përplasën në Kullat Binjake në Qendrën Botërore të Tregtisë në Nju-Jork, një në Pentagon, në Arlington, në Virxhinia dhe një në një vend të tretë në një fushë të Shenksvillit, Pansilvani, që nuk ishte objekt i synuar. Humbje në njerëz, përfshirë pasagjerët e ekuipazhin të avionëve dhe njerëzit e vrarë në Nju Jork e Pentagon arritën në rreth tre mijë të vdekur e mijëra të plagosur. Ky sulm i paparë ndonjëherë më parë dhe rrethanat e tij të rënda shkaktuan një varg të ri shqetësimesh për sigurinë që preken mbarë kombet e qytetëruara. Madje, vitet që do të vijnë, ekziston frika se do të ndodhin jo vetëm ngjarje tronditëse si ato të 11 shtatorit, por do të ketë edhe autorë të ndryshëm (p.sh: shtete, organizata e individë) që do të kenë synimin dhe aftësitë për të përdorur “super terrorizmin” biologjik, kimik dhe bërthamor. Mjafton të përmendim rastin e Ramsi Jusefit, i cili

organizoi sulmet më 11 shtator 2001 dhe përmes teknologjisë së kompjuterëve mori udhëzime dhe mesazhe për organizimin e aktit terrorist ku deshifroi të gjitha kodet direkt në fletore.

Duke përdorur teknologji të reja, terroristët mund të orvaten të ndërmarrin sulme të kompjuterizuara kundër sistemeve më të qenësishme të infrastrukturës dhe të bazave ekonomike.

Pas kësaj qasjeje sektoriale, bashkësia ndërkombëtare ka miratuar disa konventa sektoriale kundër terrorizmit kompjuterik, të cilat janë të hapura për ratifikimin nga të gjitha shtetet: Në literaturë gjenden dy fjalë të ngjashme "krimi kompjuterik" dhe "krimi kibernetikë". A janë këto dy fjalë sinonime të përsosura? Në të vërtetë, jo. Mendoj ndryshe nga siç është thënë deri me tash, se këto dy fjali e përshkruajnë të njëjtën ide.[25] Krimet kibernetike janë krime të kryera me kompjuter në një kontekst të kulturës kibernetike.

Si një fenomen ligjor penal, terrorizmi kompjuterik ka karakter ndërkombëtar dhe në përputhje me një linjë të dokumenteve ndërkombëtare që ka të bëjë me numrin e krimeve ndërkombëtare.

Të gjitha tendencat dhe analizat ndërkombëtare deri më tash vlerësojnë se terrorizmi kompjuterik është në rritje e sipër nga viti në vit. Numri i përdoruesve të internetit është në rritje vazhdimisht.

Sistemi i Internetit sot mbulon tërë botën si me aplikimin e teknologjive te reja (përdorim të pajisjeve mobile satelitore të komunikimit) ku lidhja në internet nga çdo pikë e globit është e mundur. Në qoftë se flasim për infrastrukturë të zhvilluar në kontekst të tillë, interneti mbulon më shumë se 180 vende në tërë botën (në tërë botën ekzistojnë 196 shtete të pavarura). Me futjen në përdorim të teknologjisë moderne të informacionit ka rezultuar edhe shfaqja e llojeve të reja të krimeve siç janë kriminaliteti dhe terrorizmi kompjuterik, ndërhyrjet e paligjshme në rrjetet dhe sistemet e kompjuterëve, grabitjet e të dhënave kompjuterike,transferime të paligjshme etj.

[25]CyberCrime@IPAProjektiPërbashkët BE/KiEpërBashkëpuniminRajonalkundërKrimitKompjuterik, Dubrovnik, Kroaci, 15 shkurt 2013, faqe 69,

Sipas eksperteve të Këshillit te Evropës, vetëm me karta të kreditit çdo vit vidhen rreth 400 milionë dollarë. Viruset shkaktojnë rreth 12 miliardë dollarë në vit dëme, në të drejtën pronësore shkaktojnë humbje rreth 250 miliardë dollarë. Problemet e kriminalitetit kompjuterik dhe të terrorizmit kompjuterik po pengojnë organet e zbatimit të ligjit për funksionimin serioz te të gjitha shtetet ndërkombëtare.[26]

Grupet terroriste në mënyrë aktive përdorin internetin dhe një email adresë për rekrutimin e anëtareve të rinj. Ish-drejtori i CIA-s, George Tenet, kishte deklaruar se grupet terroriste përfshirë Heisbullahun, Hamasin, Abu Nidalin dhe organizatën që ishte nën udhëheqjen e Bin Ladenit "Al Queda" janë më aktive në përdorimin e kompjuterëve për aktivitetet e tyre. Këto sfida konvencionale dhe jokonvencionale kundër stabilitetit në mbarë botën kërkojnë përpjekjet të efektshme kombëtare, rajonale e globale për të përballuar të gjitha format e terrorizmit përfshirë edhe formën më të re - terrorizmin kompjuterik.

Gjatë sulmeve të tilla terroriste, veprimet që e cenojnë sigurinë janë shumë të ndërlidhura njëra me tjetrën, por janë bërë nga autorë të ndryshëm. Në një skenar të tillë, roli i teknologjisë kompjuterike doli me avantazhet e tij në efikasitetin për realizimin e qëllimit.[27]

Në shoqërinë që po ndërtohet gjithnjë e më tepër në baza teknologjike dhe kompjuterike, rolet e botës virtuale në ekzistencën e përditshme janë duke u bërë gjithnjë e më shumë thelbësore. Nëpërmjet avantazheve që ofron teknologjia kompjuterike në profesion, treg dhe në qeveri, përdorimin dhe aplikimin e teknologjisë kompjuterike e ka përfshirë tani një rritje e rrezikut. Kjo është në lidhje me krimet që ndodhin në tërë botën përmes internetit.

Të dy akteret qeveritarë dhe joqeveritarë duhet të angazhohen ndërkombëtarisht për të parandaluar dhe luftuar terrorizmin kompjuterik, duke luftuar spiunazhin, vjedhjet financiare dhe krimet e tjera ndërkufitare. Tejkalimi i kufijve ndërkombëtarë që cenon

[26]CyberCrime@IPAProjektiPërbashkët BE/KiEpërBashkëpuniminRajonalkundërKrimitKompjuterik, Dubrovnik, Kroaci, 15 shkurt 2013,faqe 73,

[27]ZamirPoda "Krimi I OrganizuarTransnacional", ShtëpiaBotuese "Morava", Tiranë, faqe 38,

interesat e një shteti është referuar disa herë si luftë kompjuterike. Në Gjykatën Ndërkombëtare Penale sistemi ligjor ndërkombëtar është duke u përpjekur për të dënuar akteret që kanë përgjegjësi për veprimet e tyre. Është shumë e rëndësishme dhe e nevojshme që të përcaktohet terrorizmi në të drejtën ndërkombëtare penale. Kështu, traktatet ndërkombëtare të së drejtës penale që kërkojnë për të parandaluar, dënuar dhe ndëshkuar veprimtarit terroriste, kërkojnë përkufizime të sakta.

Përkufizimi i veprës në traktate ndërkombëtare dhe në ligjin penal luan disa role. I pari dhe më kryesori është se ajo ka rolin simbolik, normativ për të shprehur dënimin e njerëzve në shoqërinë në të cilën kryejnë vepra të ndaluara. Së dyti, ai lehtëson marrëveshjet ndërkombëtare. Një përkufizim i saktë i terrorizmit detyron shtetet të deklarohen që janë të gatshme për të marrë përsipër detyrime të rrepta në çështjet që lidhen me ushtrimin e juridiksionit të tyre të brendshëm, gjithashtu kufizon fushëveprimin e këtyre detyrimeve, bënë marrëveshje më pak të kushtueshme. Së treti, ai u jep një bazë të mirë - subjektive për zbatimin reciprok të detyrimeve ligjore në gjyqësor dhe krijon bashkëpunim policor më të letë ndërkombëtar. Ky funksionim është i një rëndësie të veçantë në traktatet e ekstradimit ku shumica e sistemeve ligjore kërkojnë që terrorizmi të jetë i dënueshëm si në shtetin kërkues dhe në shtetin e kërkuar. Së katërti, ajo ndihmon që shtetet të miratojnë legjislacionin e brendshëm për të zbuluar dhe të dënojë aktet terroriste të përcaktuara në traktate dhe në përputhje me detyrimet e të drejtat e tyre njerëzore.

Nullum crimen parimi i sine lege kërkon, në veçanti, që shtetet të përcaktojnë saktësisht se cilat veprime janë të ndaluara, para se dikush mund të ndiqet penalisht ose të dënohet për kryerjen e këtyre akteve në formë të njëjtë në të gjitha shtetet.

Në fund të fundit, është obligim moral i të gjitha shteteve që të harmonizojnë legjislacionet e tyre për të parandaluar dhe luftuar terrorizmin kompjuterik.

Për të parandaluar dhe ndëshkuar terrorizmit ndërkombëtar duhet përpunuar një bazë ligjore efektive, jo vetëm duke punuar si një shtet i vetëm. Bashkësia ndërkombëtare ka miratuar gjithashtu një qasje sektoriale që ka për qëllim identifikimin e shkeljeve që u përkasin aktiviteteve të terroristëve dhe atyre që punojnë jashtë traktateve, në mënyrë që të merren me kategorizimin specifik të tyre.

Në tërësi, konventat mbi qasjen sektoriale konfirmojnë supozimin se disa vepra mund të konsiderohen në vetvete si vepra me interes ndërkombëtar, pavarësisht nga synimi apo qëllimi i ndonjë terroristi. Në të vërtetë, merita kryesore e qasjes sektoriale është se ajo shmang nevojën për të përcaktuar terrorizmin apo aktet e terroristëve kompjuterikë, sepse është e përcaktuar në këtë konventë sektoriale. Për aq kohë sa implementimet qasja sektoriale nuk ka nevojë për ta definuar terrorizmin kompjuterik, sepse është i definuar aty. Një përkufizim i vetëm do të jetë i nevojshëm në qoftë se veprat penale përkatëse janë bërë të kushtëzuara nga ekzistenca e një synimi terrorist të veçantë, por kjo do të ishte kundër produktive, duke qenë se ai do të rezultojë në goditjen e tyre padrejtësisht.

Në lidhje me jetën problematike të terrorizmit kompjuterik mund të pohohet në mënyrë të sigurt se kjo dukuri shoqërore shumë e rrezikshme nuk është më një mit, por një realitet si për botën ndërkombëtare ashtu edhe për shtetin tonë.

Tranzicioni i madh që përfshin modernizimin e të gjitha sferave të jetës dhe menaxhimin elektronik të proceseve teknologjike edhe në vendin tonë do të rezultojnë lloje të reja të krimeve, përfshirë edhe terrorizmin kompjuterik.[28]

3.3 Spiunazhi Kompjuterik

Spiunazhi kompjuterik ka të bëjë me zbulimin e "informacionit", apo "evidencave". Një spiun industrial mund të kërkojë të zbulojë informacione sekrete mbi një laptop të një menaxheri projektesh të Mikrosoftit, i cili në mënyrë specifike ka të bëjë me të ardhmen e kompanisë duke neutralizuar sistemet operuese. Në varësi të informacionit, ai mund të përpunohet në evidenca të caktuara. Veç informacionit dhe evidencave, ka dy koncepte të rëndësishme në spiunazhin kompjuterik : Aktiviteti është tipikisht i panjohur dhe i paautorizuar. Në shumë prej rasteve, viktima nuk shkon të japë lejë të saktë apo të nënkuptuar për të lejuar dikë të fusë hundët në kompjuterin e tij. Përjashtime mund të jenë rastet e vendeve të punës, në të cilat të punësuarit monitorohen.[29]

[28] BE , Europol , kriminaliteti kompjuterik

29 http://sq.wikipedia.org/wiki/Krimi_kompjuterik

3.4. Lufta e "Specializuar" Ndaj Krimit Modern(Krimi Kompjuterik)

Sulmet e hackerave ndaj institucioneve qeveritare, shoqërive apo kompanive më të mëdha në botë, është kthyer në një hobi të vërtetë. Pirateria nëpërmjet internetit përbën sot një shqetësim global dhe me pasoja ekonomike në shkallë shqetësuese. Edhe në vendin tonë krimi kibernetikë nuk mund të quhet më sporadik. Ai po gjen përhapje graduale dhe po kthehet në një kërcënim serioz dhe real. Vjedhjet nëpërmjet internetit dhe veçanërisht vjedhja e llogarive bankare apo kartave të kreditit kanë gjetur terren të përshtatshëm edhe te ne. Por, këtij fenomeni nuk duket se po i kushtohet vëmendja e duhur. Rrjetet kompjuterike të ditëve të sotme ofrojnë mundësi të reja dhe moderne për shkeljen e ligjit duke krijuar potenciale që shtyjnë subjektet në kryerjen e formave të ndryshme të kriminalitetit tradicional në mënyrë jo tradicionale. Përhapja dhe përdorimi i internetit nuk është shoqëruar me mekanizmat e mjaftueshëm juridikë të mbrojtjes ndaj krimit në internet. Si rrjedhim, individët, institucionet (publike dhe private) rrezikojnë dhe janë pamjaftueshmërish të mbrojtur nga ky krim. Pirateria zhvillohet tërësisht në kushte anonimiteti dhe kjo e vështirëson shumë punën hetimore të organeve kompetente.[30]

Pirati dhe viktima e tij mund të jenë në vende krejtësisht të ndryshme nga njëri-tjetri dhe kjo e bën akoma më të vështirë investigimin, duke pasur parasysh ligjet e ndryshme që mund të kenë shtetet dhe qasjen ndaj këtij lloj krimi. Karakteri specifik i krimit kompjuterik dhe rrezikshmëria e lartë shoqërore kërkon vërtet që këto problematika të rregullohen me ndryshimet e duhura ligjore, por ligji nuk mjafton! Nevojiten edhe disa rregulla të tjera për parandalimin dhe luftën ndaj këtij krimi, pasi format e reja në fushën e krimit kompjuterik janë një sfidë e vazhdueshme për të gjitha qelizat e shoqërisë. Për këto arsye, duhet që të vazhdohen përpjekjet maksimale për plotësimin dhe azhurnimin e kuadrit ligjor përkatës dhe rregullimin juridiko-penal, në mënyrë të veçantë për inkriminimin e disa veprimeve të keqpërdorimit të kompjuterit si krime/vepra kriminale. Vëmendje e veçantë duhet t'i kushtohet krijimit apo mirëfunksionimit të seksioneve që marrin pjesë në zbulimin, hetimin

[30]Zamir Poda "Krimi I Organizuar Transnacional", Shtëpia Botuese "Morava", Tiranë, faqe 85,

dhe procedimin e veprave penale lidhur me krimin kompjuterik. Seksioni i veçantë i krijuar në Prokurori në Drejtorinë e Krimit Ekonomik, duhet domosdoshmërish të përbëhet nga persona ekspertë të përdorimit të kompjuterëve. Duhet investuar akoma më shumë për trajnimin dhe aftësimin e oficerëve apo personave të cilët merren me zbulimin e këtyre krimeve, pasi këto krime kryhen nga persona me aftësi të spikatura dhe që ecin me ritme shumë më të shpejta. Kontrolli duhet të fokusohet intensivisht mbi email-et, mbi forumet interaktive, chat room, instant messaging etj. Duhet gjithashtu t'u jepet prioritet politikave të caktuara, të cilat ndihmojnë në mënyrë të ndjeshme në parandalimin dhe në luftën ndaj këtij lloj krimi. Në një të ardhme të afërt, këto politika do të mund të rrisin efektivitetin e reformave ligjore të ndërmarra dhe të minimizojnë ndjeshëm rrezikun e krimeve kibernetike në Shqipëri. Në qoftë se kuadri ligjor aktual duket modern, i plotë dhe në përputhje me standardet ndërkombëtare (edhe pse ka akoma vend për përmirësime), prioritet merr në këtë drejtim implementimi i tyre dhe mbrojtja nëpërmjet mjeteve efektive teknologjike dhe shtrënguese, të cilat mund të reduktojnë aktivitetin kriminal kompjuterik.[31]

Për shkak të përhapjes së kësaj dukurie, duket gjithashtu i pakontestueshëm një "aksion" me qëllim parandalimin dhe luftimin e këtij fenomeni në shoqërinë tonë bashkëkohore.

Nëse seksioni i veçantë në Prokurori nuk mund të përballojë këtë "fluks piraterie", atëherë prioritet merr krijimi i seksioneve të tjera funksionale dhe të specializuara për zbulimin, hetimin dhe procedimin e veprave penale lidhur me krimin kompjuterik. Një zgjidhje alternative e këtij problemi mund të jetë, siç u përmend edhe më lart, krijimi i një sektori të ri në Policinë e Shtetit: policia postare. Kjo mund të jetë një organikë me detyra të veçanta, me një autonomi funksionale dhe strukturale, në kuadër të sigurisë dhe rregullsisë së shërbimeve të telekomunikacionit, e specializuar për të gjitha aktivitetet e inspektimit për veprimtari të paligjshme të kryera nëpërmjet internetit.[32]Duhet cilësuar se ligjet dhe reformat institucionale të implementuara në të drejtën penale shqiptare nuk do të jenë të suksesshme nëse nuk shoqërohen edhe me masa të tjera të karakterit social dhe kulturor vendas. Në lidhje me këto krime nevojitet për të gjithë njohja e rreziqeve efektive dhe

[31]Burimi: Europe's Information Society "European Cybercrime Centre (EC3) opens on 11 January"

[32] Dr. ERJONA CANA July 30, 2011 Justicia

pasojatkonkrete që sjell krimi kompjuterik në të gjitha aspektet e jetës, dhe jo vetëm ato me karakter ekonomik. Shumë i rëndësishëm është raportimi në organet kompetente, i cili duhet bërë në çdo rast. Nga ana tjetër, duhet të theksohet ndërgjegjësimi dhe edukimi për monitorim vigjilent të sigurisë për mos vendosjen e kamerave apo skanerëve afër bankomateve (ose mikrokamerave të vendosura mbi ekran), si dhe pajisjeve shtesë përreth kornizave të bankomatit. Në lidhje me këtë, rekomandohet trajnimi dhe përkujdesja e veçantë që duhet të tregojë personeli i sigurimit, të cilët duhet të njoftojnë në të gjitha rastet organet kompetente. Kujdes të veçantë duhet të tregojnë të gjithë personat për të mos iu përgjigjur thirrjeve me email për të transmetuar të dhënat e tyre personale. Nevojitet gjithashtu nxitja e tëgjithë subjekteve në rast të keqpërdorimit kompjuterik për të lajmëruar organet kompetente. Krimi kompjuterik është padyshim një krim modern dhe lufta ndaj tij duhet të jetë e të njëjtës natyrë: intensive dhe me armë bashkëkohore![33]

[33]Posted in: Shkencat Penale Tags: crime, cybercrime, internet, kompjuter, krimi elektronik, krimi kinbernetik, krimi kompjuterik, krimi ne kompjuter

KAPITULLI IV

MEKANIZMAT MBROJTËS KUNDËR KRIMIT KOMPJUTERIK

5. MEKANIZMAT MBROJTËS KUNDËR KRIMIT KOMPJUTERIK

Mekanizmat mbrojtës kundër të gjitha formave të kriminalitetit kompjuterik janë të shumtë duke u nisur nga dokumentet ligjore vendore si dhe ndërkombëtare.

Mekanizmat mbrojtës të Republikës së Kosovës që trajton, rregullon dhe sanksionon çështjet e kriminalitetit kompjuterik qoftë në mënyrë specifike apo relevante me to janë të shumta.

Në luftë kundër kriminalitetit, Republika e Kosovës ka në fuqi një bazë të gjerë legjislative ku përfshihen, por nuk kufizohen vetëm në:

- Kushtetuta e Republikës së Kosovës,
- Kodi Penal i Kosovës,
- Kodi i Procedurës Penale të Kosovës,
- Kodi Doganor dhe i Akcizave të Kosovës,
- Ligji për Policinë,
- Ligji për Ekzekutimin e Sanksioneve Penale,
- Ligji për Prokurorinë Publike,
- Ligji për Parandalimin dhe Luftimin e Krimit në Kibernetikë.

Konkluzion

Përhapja e shpejtë dhe në rritje e përdorimit të teknologjisë. si ndihmë në kryerjen e aktivitetit kriminal dhe krimit kompjuterik. meritojnë më tepër vëmendje duke i dhënë prioritet miratimit dhe marrjes së masave të përshtatshme ligjore dhe implementimit të mjeteve efektive teknologjike dhe shtrënguese, që reduktojnë aktivitetin kriminal kompjuterik.

Tendencat aktuale tregojnë se në të ardhmen, krimi kompjuterik do të zërë vend si objekt kryesor në zbatimin e politikave globale për luftimin dhe parandalimin e kësaj forme të organizuar krimi, përmes shkëmbimit të informacionit, rritjes së shkallës së intelektit human, koordinimit të përpjekjeve ligjore në nivele kombëtare, rajonale dhe ndërkombëtare, si dhe krijimit të një rrjeti botëror në nivel të lartë të bashkëpunimit mes agjencive dhe institucioneve të zbatimit të ligjit.

Literatura

1. Agency: APIS Security Consulting, 31.03.2004,
2. S.Petroviq .
3. Dr.sc. Veton G. Vula “Kriminaliteti Kompjuterik”, Prishtinë 2009,
4. Prof. Dr. Skënder Begeja “Kriminalistika”, Botimi I 1989,
5. Mr. sc. Fatos Haziri “E Drejta E Policisë”, Prishtinë 2010,
6. Nedžad Korajlić “Kriminalistića Metodika”, Sarajevo 2008,
7. Prosecuting Computer Crimes Computer Crime and Intellectual Property Section Criminal Division, See United States v. Caceres, 440 U.S. 741 (1979),
8. Jonathan Clough, Principles Of Cybercrime, Faculty of Law, MonashUniversity, Jonathan Clough 2010,
9. Stein SchjolbergandSolange Ghernaouti-Helie, A Global Treaty onCybersecurity and CybercrimeSecond edition, 2011,
10. Understanding cybercrime:Phenomena, challenges andlegal response, September 2012,
11. Sam Lumpkin Senior Security Architect, 2AB, Inc. Internet Security and CyberCrime,
12. Europe's Information Society "European Cybercrime Centre (EC3) opens on 11 January“,
13. Dr. Erjona Cana July 30, 2011Justicia.