UNIVERSITETI I EVROPËS JUGLINDORE | **FAKULTETI I DREJTËSISË**

SOUTH EAST EUROPEAN UNIVERSITY | **FACULTY OF LAW**

УНИВЕРЗИТЕТ НА ЈУГОИСТОЧНА ЕВРОПА | **ПРАВЕН ФАКУЛТЕТ**

STUDIMET PASDIPLOMIKE – CIKLI I DYTË

DREJTIMI PENAL

TEZA:

“HETIMI DHE ZBULIMI I KRIMINALITETIT KOMPJUTERIK NË BOTËN BASHKËKOHORE”

KANDIDAT:

Egzon Ahmeti

MENTOR:

Doc. Dr. Vedije Ratkoceri

Tetovë, 2021

DEKLARATA E AUTORËSISË

Unë Egzon Ahmeti nën përgjegësin time personale, deklaroj se përmbajtja e temës së magjistraturës së paraqitur me titull: **"Hetimi dhe zbulimi i kriminalitetit kompjuterik në botën bashkëkohore"** është punë origjinale e shkruar prej meje, e cila nuk është prezantuar asnjëherë para ndonjë institucioni tjetër për vlerësim dhe nuk është botuar i tëri ose pjesë të veçanta të tij. Të gjitha referencat dhe citimet në tekst janë bërë në bazë të burimeve të paraqitura në fusnota.

Me respekt

Egzon Ahmeti

_____

FALËNDERIMET

Para së gjithash, dua të falënderoj Zotin tonë të plotfuqishëm, të cilit i jam mirënjohës që më dha dhe siguroi shëndetin, inteligjencën, dëshirën dhe vendosmërinë për të arritur këtë qëllim, për realizimin e suksesshëm të këtij hulumtimi.

Falënderoj thellësisht nga zemra njerëzit më të rëndësishëm në jetën time, prindërit e mi të adhuruar dhe të përkushtuar, të cilëve u jam shumë mirënjohës dhe falënderues për dashurinë, kujdesin dhe sakrificat e tyre në edukimin e mirëfilltë dhe përgatitjen time për të ardhmen si dhe duke më besuar dhe duke më qëndruar pranë gjatë çdo hapi të sukseseve të mia. Poashtu, do të doja të përcillja mirënjohjen për familjen time në përgjithësi për mbështetjen dhe inkurajimin e tyre që më ndihmuan të përfundoj studimet.

Një falënderim i veçantë shkon për mentoren time Doc.Dr. Vedije Ratkoceri, e cila ka qenë gjithmonë e gatshme për të më ofruar ndihmë dhe ka qenë e disponueshme për të më këshilluar, mbështetur dhe udhëzuar në çdo kohë, duke më nxitur për punimin dhe realizimin e këtij hulumtimi në mënyrë sa më profesionale. Poashtu, faleminderit për të gjithë profesorët e tjerë që kontribuan me njohuritë e tyre gjatë studimeve master.

PËRMBAJTJA

ABSTRAKTI 6

АПСТРАКТ 7

ABSTRACT 8

HYRJE 9

KAPITULLI I PARË 10

1. Njohuri të përgjithshme mbi kriminalitetin kompjuterik 10

1.1 Përkufizimi i kriminalitetit kompjuterik 10

1.2 Historiku i paraqitjes së kriminalitetit kompjuterik 14

1.3 Mënyrat e përdorimit të kompjuterit si mjet për kryerjen e krimit kompjuterik 18

1.4 Sfidat e krimit kompjuterik 20

1.5 Viktimat e krimeve kompjuterike 23

KAPITULLI I DYTË 25

2. Format më të përhapura të kriminalitetit kompjuterik në botën bashkëkohore 25

2.1 Kategoritë dhe llojet e kriminalitetit kompjuterik 25

2.1.1 DDoS (Distributed Denial of Service) - Sulmet e shpërndara për mohimin e ofrimit të shërbimit) 29

2.1.2 Hakingu (hacking) 30

2.1.3 Viruset kompjuterike (computer viruses) 31

2.1.4 Terrorizmi kibernetik (cyberterrorsim) 32

2.1.5 Vjedhja e identitetit (identity theft) 33

2.1.6 Pornografia e fëmijëve (child pornography) 34

2.1.7 Ngacmimi në internet (cyberbullying) 35

2.1.8 Fishingu (phishing) 36

2.2 Kryerësit e krimeve kompjuterike 37

2.3 Faktorët që ndikojnë në kryerjen e krimeve kompjuterike 38

2.3.1 Faktorët objektiv 38

2.3.2 Faktorët subjektiv 39

KAPITULLI I TRETË 40

3. Hetimi dhe zbulimi i kriminalitetit kompjuterik 40

3.1 Metodika e hetimit dhe zbulimit të kriminalitetit kompjuterik 40

3.1.1 Roli i hetuesve të krimeve kibernetike 42
3.1.2 Roli i policisë në hetimin e krimeve kibernetike 43
3.1.3 Roli i prokurorëve në hetimin e krimeve kibernetike 44
3.2 Mjetet dhe teknikat e hetimit dhe zbulimit 45
3.2.1 Forenzika kompjuterike 46
3.2.2 Modelet hetuese të forenzikës kompjuterike 47
3.2.3 Mjetet e nevojshme të forenzikës kompjuterike 49
3.2.4 Provat kompjuterike dhe karakteristikat e tyre 52
3.3 Hetimi i krimeve dhe sulmeve në internet 54
3.3.1 Hapat dhe qëllimet e hetimit të krimeve në internet 54
3.3.2 Sigurimi dhe vlerësimi i vendit nga ku është kryer krimi kibernetik 56
3.3.3 Dokumentimi dhe mbledhja e provave në internet 57
3.4 Parandalimi dhe luftimi i kriminalitetit kompjuterik 58
3.4.1 Sfidat e luftimit të krimit kompjuterik 58
3.4.1 Korniza juridike ndërkombëtare kundër krimit kompjuterik (Konventa e Budapestit) 60
KAPITULLI I KATËRT 61
4. STUDIM EMPIRIK 61
4.1 Analiza dhe prezantimi i të dhënave statistikore nga Enti shtetëror statistikor i RMV-së bazuar në kërkime empirike lidhur me veprat penale të krimeve kompjuterike 61
4.2 Statistika për krimin kibernetik në SHBA 63
4.3 Statistika në Europë (Hollandë) 66
4.3.1 Rastet e regjistruara të krimit kibernetik në Belgjikë 68
4.3.2 Statistika të zbulimit të sulmeve kibernetike 70
PËRFUNDIMET DHE REKOMANDIMET 71
BIBLIOGRAFIA 74

ABSTRAKTI

Krimi kompjuterik apo krimet në internet janë fenomene të rrezikshme dhe kërcënime që kryhen për qëllime të ndryshme, më së shumëti për përfitime financiare nga kriminelët kibernetik të cilët janë persona shumë inteligjent dhe shumica prej tyre kanë njohuri të mëdha për kryerjen e këtyre krimeve nëpërmjet përdorimit të kompjuterit i cili mund të përdoret si mjet për kryerjen e atij krimi apo si objekt sulmi. Krimi kibernetik është vazhdimisht në rritje dhe prandaj është shtuar nevoja që të hulumtohet më tepër ky problem shqetësues në botën bashkëkohore.

Qëllimi i hulumtimi në këtë punim është analiza dhe diskutimi i metodave dhe strategjive të ndryshme për hetimin dhe zbulimin e krimit kibernetik, të përdorura nga shtete më të zhvilluara që duhet ti marrim shembull në të cilët ky krim është më tepër i përhapur. Poashtu edhe nga agjencionet ose organizatat e ndryshme që merren me luftimin e krimit kibernetik në masa më të gjëra dhe se çfarë mënyrash zbulimi përdorin në një proces hetimi, analizimi dhe rikuperimi të të dhënave digjitale kriminalistike për gjetjen e autorëve të këtyre veprave dhe qëllimet e tyre aktuale si dhe për të menaxhuar rreziqet dhe kërcënimet e sigurisë nga llojet e ndryshme të këtyre krimeve.

Të gjitha këto për të ofruar kujdes për liritë themelore dhe sigurimin e informacionit apo të dhënave individuale dhe për të arritur në përfundim se çfarë efektesh kanë masat që përdoren dhe çfarë masash tjera duhet të ndërmarrin, cilat janë problemet me të cilat përballen këto autoritete dhe se çka duhet të bëjnë më shumë që të parandalohet, zbulohet dhe sanksionohet ky krim për një internet më të sigurt dhe një të ardhme më të mirë.

Fjalët kyçe: krimi kompjuterik, internet, hetim, organizatat, autoritetet, zbulim

АПСТРАКТ

Сајбер криминал или злосторствата на Интернет се опасни феномени и закани кои се извршуваат за различни цели, главно за финансиска корист од сајбер -криминалци кои се многу интелигентни луѓе и повеќето од нив имаат големо знаење за извршување на овие злосторства преку употреба на компјутер што може да се користи како алатка за извршување на тој криминал или како објект на напад, сајбер криминалот постојано се зголемува и затоа се зголеми потребата за понатамошно истражување на овој вознемирувачки проблем во современиот свет.

Целта на истражувањето во овој труд е да се анализираат и дискутираат различни методи и стратегии за истражување и откривање на компјутерски криминал, користени од поразвиените земји што треба да се земат како пример во кој ова злосторство е по присутно. Исто така, од агенции или разни организации кои се занимаваат со компјутерски криминал во поголем обем и какви начини за откривање користат во процесот на истрага, анализа и обновување на дигитални форензички податоци за да се откријат сторителите на овие дела и нивните сегашни цели, како и да управуваат безбедносни ризици и закани од различни видови на овие кривични дела.

Сето ова е за да се грижи за основните слободи и да се обезбедат индивидуални информации или податоци и да се заклучи какви ефекти имаат користените мерки и кои други мерки треба да се преземат, кои се проблемите со кои се соочуваат овие власти и што треба повеќе да се направи за да се спречи, откривање и санкционирање на овој криминал за побезбеден интернет и подобра иднина.

Клучни зборови: сајбер криминал, интернет, истрага, организации, власти, откривање

ABSTRACT

Cybercrimes or crimes on internet are dangerous phenomena and threats that are committed for various purposes, mostly for financial gain by cybercriminals who are very intelligent people and most of them have great knowledge of committing these crimes through the use of computer which can be used as a tool to commit that crime or as an object of attack, cybercrime is constantly increasing and therefore the need has increased to further research this troubling problem in the contemporary world.

The purpose of the research in this paper is to analyze and discuss different methods and strategies for investigating and detecting cybercrime, used by more developed countries that should be taken as an example in which this crime is more prevalent. Also from agencies or the various organizations that deal with cybercrime on a larger scale and what ways of detection they use in a process of investigating, analyzing and recovering digital forensic data to find the perpetrators of these acts and their current purposes as well as to manage security risks and threats from different types of these crimes.

All this to provide care for fundamental freedoms and the provision of individual information or data and to conclude what effects the used measures have and what others measures should be taken, what are the problems faced by these authorities and what more need to be done to prevent, detect and sanction this crime for a safer internet and a better future.

Keywords: cybercrime, internet, investigating, organizations, authorities, detection

HYRJE

Teknologjia ka revolucionarizuar botën dhe jetën tonë të përditshme me kalimin e viteve. Teknologjia ka krijuar mjete dhe burime mahnitëse, duke vendosur informacion të dobishëm në majë të gishtave tanë për një kohë të shkurtër vetëm me disa klikime në internet. Kompjuterët janë gjithnjë e më të shpejtë, më të lëvizshëm dhe me energji më të lartë se kurrë më parë. Teknologjia gjithashtu e ka bërë jetën tonë më të thjeshtë, më të shpejtë, më të sigurt dhe më të këndshme me të gjitha këto revolucione, por nga ana tjetër përkundër avantazheve që i ka siguruar interneti botës bashkëkohore, ai është gjithashtu i mbushur me rreziqe që lidhen me elemente të padëshirueshme që dëshirojnë të keqpërdorin përdorimin e tij, duke kryer forma të ndryshme të krimeve kompjuterike më së shumëti për përfitime financiare.

Duke vënë në konsideratë faktet më lartë, në këtë temë lëndë hulumtimi do të jenë mënyrat, metodat dhe mjetet e hetimit dhe zbulimit të kriminalitetit kompjuterik në rajone të ndryshme të botës duke përfshirë edhe vendin tonë.

Në këtë temë masteri do të analizohen dhe diskutohen poashtu edhe legjislacionet e shteteve të ndryshme që trajtojnë krimin kompjuterik, kodet penale, burimet e rëndësishme globale që japin rregulla për trajtimin e këtij krimi, siç është Konventa për krimin kibernetik e marrë nga Këshilli i Evropës dhe plani i veprimit i Komisionit Evropian, si dhe të tjera. Do të shqyrtohen forma të veçanta të krimit kibernetik dhe karakteristikat e tyre, gjithashtu llojet e krimeve kibernetike që paraqiten në RMV dhe në vende tjera të botës gjatë viteve të fundit, metodat dhe mjetet më komplekse që përdoren për të luftuar këto aktivitete kriminale, cilët janë viktimat nga këto krime, si ndikojnë këto krime në jetën e njerëzve, çfarë dëmesh u shkaktohen dhe a i raportojnë këto dëme në institucionet përkatëse. E gjitha kjo për të arritur në një përmbledhje se cilat janë sfidat, mundësit dhe bashkëpunimet e përbashkëta të shteteve në botën bashkëkohore për luftimin e këtyre veprave të paligjshme.

KAPITULLI I PARË

1. Njohuri të përgjithshme mbi kriminalitetin kompjuterik

1.1 Përkufizimi i kriminalitetit kompjuterik

Çdo ndryshim inovativ bart me vete disa çështje të papritura. Krimet kompjuterike janë veprimtari të tilla të dëmshme që kryhen duke përdorur kompjuterin dhe internetin dhe që mund ti shkaktojnë dëme financiare si dhe dëme të tjera të ndryshme një personi, një shteti, institucioneve apo kompanive duke keqpërdorur teknologjinë kompjuterike. Ku kryerësit e këtyre krimeve gjithmonë eksplorojnë metoda të reja për kryerjen e veprimtarive të tyre të paligjshme ku përveç kompjuterit mund të përdorin edhe paisje tjera digjitale të ndryshme sepse ky lloj krimi inkorporon një spektër të gjërë aktivitetesh me synim të keq.

Kriminaliteti kompjuterik në dekadën e fundit është në rritje të shpejtë dhe është bërë pothuajse një shqetësim global tek i cili paraqiten probleme dhe sfida të ndryshme në hetimin dhe zbulimin e këtij krimi, prandaj është rritur nevoja që të hulumtohen dhe të implementohen në praktikë metodat ekzistuese si dhe të zbulohen metodat të reja për luftimin dhe parandalimin e këtij problemi për mbrojtjen e shoqërisë dhe shtetit nga kërcënime të tilla. Ndërsa teknologjia zhvillohet çdo ditë e më shumë, ligji duhet tu përgjigjet këtyre zhvillimeve të reja për të parandaluar ata që do të abuzojnë dhe keqpërdorin teknologjinë e re.

Bota bashkëkohore sot përballet me arritjet më të mira të ngjarjeve të specializuara inovative, të cilave u bashkohet zhvillimi i shpejtë i inovacionit të të dhënave dhe kompjuterizimi i masave të punës në të gjitha qarqet e jetës shoqërore dhe financiare. Ky përparim në shoqërinë bashkëkohore ka mirëpritur ndihma dhe lehtësime të panumërta nga njëra anë, ndërsa nga ana tjetër abuzimi i planifikuar i këtyre arritjeve ka krijuar çështje dhe rreziqe të ndryshme për shoqërinë në përgjithësi ku pa marrë parasysh se ku ndodhen, këto krime mund të kryhen globalisht nga katër anët e botës[1].

[1] Vula, Veton, "Kriminaliteti Kompjuterik" Prishtinë, 2010, fq.26

Ekzistojnë përkufizime të ndryshme për kriminalitetin kompjuterik nga organizata dhe autorë të ndryshëm të cilët studiojnë këtë fenomen të rrezikshëm dhe të dëmshëm.

Dukuria dhe nocioni i kriminalitetit kompjuterik është paraqitur në SHBA, punimi i parë shkencor mbi këtë krim është shkruar nga autori Von zur Muhlen (1973) i cili përdori definicionin e gjerë mbi këtë fenomen, ku sipas tij përfshin të gjitha sjelljet në të cilat kompjuteri është mjet dhe qëllim i veprimtarisë kriminale[2].

Ndërkaq, përkufizimi i kriminalitetit kompjuterik nga ana e Komisionit Europian të cilët referohen se krimi kompjuterik konsiston në aktivitete kriminale që kryhen në internet duke përdorur rrjetet e komunikimeve elektronike dhe sistemet e informacionit[3]. Është një problem pa kufij që mund të kategorizohet në tre përkufizime të gjëra:

"-Krime specifike në internet, të tilla si sulmet kundër sistemeve të informacionit ose fishing (p.sh faqet e internetit të rreme të bankave për të kërkuar fjalëkalime që mundësojnë hyrjen në llogaritë bankare të viktimave).

-Mashtrimet dhe falsifikimet në internet. Mashtrimi në shkallë të gjërë mund të kryhet në internet përmes instrumenteve të tilla si vjedhja e identitetit, fishing, spam dhe kodi me qëllim të keq.

-Përmbajtja ilegale në internet, përfshirë materialin e abuzimit seksual të fëmijëve, nxitjen e urrejtjes racore, nxitjen e akteve terroriste dhe nxitjen e dhunës, terrorizmin, racizmin dhe ksenofobinë[4]."

Agjenica e Unionit Europian për bashkëpunim në zbatimin e ligjit – EUROPOL-i në dokumentin për krimin e organizuar në internet vlerësimin e kërcënimeve të vitit 2018, krimin kompjuterik apo kibernetik e përkufizon si çdo krim që mund të kryhet vetëm duke përdorur kompjuter, rrjete kompjuterike ose forma të tjera të teknologjisë së komunikimit të

[2] Latifi, Vesel. & Demolli, Haki. "Kriminalistika" Prishtinë, 2019, fq.541
[3] Përkufizimi i kriminalitetit kompjuterik nga Komisioni Europian: https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en (Qasur më 17.11.2020)
[4] Po aty;

informacionit[5]. Në thelb, pa internet kriminelët nuk mund t'i kryejn këto krime. Ai përfshin një veprimtari të tillë si krijimi dhe përhapja e viruseve malware, hakimi për të vjedhur të dhëna personale ose të industrisë dhe mohimi i sulmeve të shërbimit për të shkaktuar dëme financiare dhe dëmtim të reputacionit[6].

Konventa e krimit kompjuterik apo Konventa e Budapestit, e cila u miratua nga Këshilli i Europës në vitin 2001, definon disa terme në kapitullin e parë në lidhje me sistemet dhe të dhënat kompjuterike ku sipas saj:

> "-sistem kompjuterik do të thotë çdo pajisje ose një grup pajisjesh të ndërlidhura me to, të cilat në përputhje me një program, kryejn përpunimin automatik të të dhënave;
>
> -të dhënat kompjuterike nënkuptojn çdo paraqitje të fakteve, informacioneve ose koncepteve në një formë të përshtatshme për përpunim në një sistem kompjuterik, duke përfshirë një program të përshtatshëm për të shkaktuar një sistem kompjuterik për të kryer një funksion[7]."

Profesoresha Marije T. Britz jep disa sqarime në lidhje me termet e ndryshme se si definohet ky krim ku sipas saj krimi kompjuterik zakonisht është karakterizuar si çdo demonstrim kriminal i kryer përmes PC-së pa ndihmën e internetit[8]. Krimet kibernetike në përgjithësi njihen si krime të kryera nëpërmjet PC-së të lidhur me internet që sjellin fatkeqësi të drejtpërdrejta shoqëruese. Më në fund, krimi digjital, një term i ri i moderuar përfshin çdo aktivitet të paligjshëm që përfshin aksesin e pa aprovuar, shpërndarjen, kontrollin, shkatërrimin e të dhënave apo informacioneve të vendosura elektronikisht, si dhe shkelje të tjera[9].

Sipas konstatimeve të disa autorëve, "krimi kibernetik" ose "krimi i teknologjisë digjitale" është një dukuri e emëruar apo e zgjidhur kohë më parë, megjithatë zhvillimi i rrjetit

---

[5] EUROPOL, Definimi i krimit kibernetik, IOCTA 2018: https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018 (qasja e fundit 17.11.2020)
[6] Po aty;
[7] Konventa për Krimin Kibernetik, Këshilli i Evropës, Budapest, 2001. https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (qasja e fundit 17.11.2020)
[8] Britz T. Marjie, "Computer Forensics and Cyber Crime an Introduction", Pearson, 2013, fq.5
[9] Po aty;

në të gjithë botën është i pasigurt lidhur me avancimin e krimit kibernetik bashkëkohorë. Një kuptim i përmbledhur i këtij krimi mund të jetë "veprim i paligjshëm ku kompjuteri është ose një instrument ose shënjestër ose të dyja" [10]. Poashtu ata theksojnë se "Krimi kibernetik është përdorur për të përshkruar një gamë të gjërë të veprave penale, duke përfshirë veprat penale kundër të dhënave kompjuterike dhe sistemeve të tilla si pirateria, falsifikimi dhe mashtrimit në lidhje me kompjuterin, shkeljet e përmbajtjes të tilla si shpërndarja e pornografisë fëmijëve dhe veprat e të drejtës së kopjimit, të tilla si shpërndarja e përmbajtjes së vjedhur"[11].

Myriam Quemener, në bazë të ligjit Francez dhe Bashkimit Europian që përqëndrohen në krimin kibernetik, e karakterizon krimin kibernetik si krime të drejtuara për sulme në internet me përdorimin e metodave të teknologjisë së internetit, këto veprime të gabuara i ndajnë në dy klasifikime: ato që përfshijnë hyrjen e pa aprovuar të informacionit dhe kornizat për qëllime kriminale dhe ato që përfshijnë falsifikimin, mashtrimin, keqpërdorimet me anë të administrimit në internet, etj[12]. Poashtu Raporti i Këshillit Kombëtar Suedez për parandalimin e krimit në lidhje me inovacionin e të dhënave dallon, si llojet më të njohura të krimit kibernetik, viruset kompjuterike, ndërhyrjet e ndryshme kompjuterike, kontrollin dhe vjedhjen e infromacionit si dhe mashtrimin[13].

Donn B. Parker thekson se "Krimet e lidhura me kompjuterin janë një kategori më e gjerë të cilat shkelin ligjin penal dhe që përfshijnë njohuri të teknologjisë kompjuterike për kryerjen, hetimin ose ndjekjen penale të tyre" [14]. Përkundër faktit se këto krime që lidhen me kompjuterin janë krejtësisht vepra penale të klasës së mesme, çdo lloj aktiviteti i paligjshëm i varur nga një kuptim i keqpërdorimit të risive teknologjike mund të jenë poashtu krime lidhur me kompjuterin, ata madje mund të jenë shkelje të dhunëshme dhe të ashpëra që asgjësojnë kompjuterët ose substancën e tyre dhe në këtë mënyrë rrezikojnë jetën njerëzore p.sh të individëve që sigurojnë mirëqenien e tyre nga puna me kompjuter. Shumëzimi dhe shfrytëzimi i

[10] Ch, Mohamed. & D, Ashraf. & K. A. Mohammad. & T, Sapna. "Cybercrime, Digital Forencsics and Jurisdiction", Vol 593, Springer, 2015, fq.3/4
[11] Po aty;
[12] C, Glenn. & D, Ronald. & E, Seth. & I, Noel. & M, Carl. & S, Eric. & S, Taru. & S, Tomoko. "Cybercrime: an annotated bibliography of select foreign-language academic literature", Library of Congress, 2009, fq.1
[13] Po aty;
[14] Parker, B. Donn, "Computer Crime: Criminal Justice Resource Manual" Washington D.C. 1989, fq. 2

kompjuterëve i bëjnë këto abuzime apo shkelje të ligjit më të përhapura apo endemike në gjithë botën bashkëkohore[15].

1.2 Historiku i paraqitjes së kriminalitetit kompjuterik

Rastet e para të krimit kompjuterik apo kibernetik janë kryer para se të shfaqej interneti duke përfshirë vjedhen e informacioneve. Kompjuterët dhe rrjetet kompjuterike janë krijuar për grumbullimin dhe lëvizjen e të dhënave qeveritare dhe organizatave të cilat ishin të rëndësishme për individët e duhur. Prodhimi i një teknike të digjitalizuar mund ta ketë shtyrë botën bashkëkohore përpara me të mirat e sajë, por gjithashtu bëri të njëjtën gjë për kriminelët të cilët filluan që ti kryejnë këto krime të dëmshme për përfitime personale[16].

Historia e paraqitjes së kompjuterëve të parë u imagjinua apo u shpikë nga kinezët para 800 viteve të cilët fillimisht i karakterizonin si një vegël e përdorur për të përcaktuar një shumë numrash apo veprime të llogaritjes ose vlerësimit të diçkaje. Këto vegla, të njohura si pajisje matematikore, ishin instrumente jo të sofistikuara të planifikuara vetëm për llogaritje numerike, të cilat ishin të përbëra nga kolona të pikave të ngjyrosura dhe ishin të vlefshme për punë më të thjeshta. Sidoqoftë, paraardhësit e PC-ve bashkëkohor nuk u krijuan deri në shekullin e 19-nëntëmbëdhjetë[17].

Sipas autorëve Anthony Reyes, Jim Steele dhe të tjerë krimi kibernetik sfondin historik të kthesës së ngjarjeve e ka kur nisi që të përparoj përdorimi i teknologjisë, në periudhën kur filluan të prodhohen kompjuterët e parë modern bashkëkohor nga mesi i shekullit 20-njëzetë, ato ishin një risi e re dhe kishin një kosto të lartë për blerjen e tyre, kështu që mund ti blenin dhe ti përdornin klasat më të larta të individëve apo organizatave që përballonin koston e tyre, prandaj kishte mënyra të kufizuara me të cilat ato mund të keqpërdoreshin apo që të

[15] Po aty;
[16] Burime nga interneti për hisotrinë e krimit kibernetik: https://www.le-vpn.com/history-cyber-crime-origin-evolution/ (qasja e fundit 23.11.2020)
[17] Britz T. Marjie, "Computer Forensics and Cyber Crime an Introduction", Pearson, 2013, fq.26

përdoreshin si mjet për të ndihmuar aktivitetet kriminale[18]. Kuptimi i fazës së hershme të shkeljeve ligjore nga ana e krimeve kompjuterike ishte vërtet e kufizuar pothuajse zero, pak më vonë filluan që të përhapen viruset dhe hakimi i kompjuterëve të qeverisë. Meqenëse kishte më pak individë me një prani personale më të vogël në internet, kishte më pak dyer të hapura për të kryer këto krime[19].

Autori Chuck Easttom dhe detektivi Jeff Taylor theksojnë se fillimet më të sakta të krimeve kompjuterike vitet 1960 dhe 1970, ishin jashtëzakonisht të qeta nga pikëpamja e këtyre krimeve, shumica e dukurive në të vërtet ishin shaka të luajtura në kornizat e kompjuterëve në kolegje nga student kurioz dhe inteligjent, të cilët në përgjithësi nuk kanë shkaktuar dëme dhe nuk ka pasur ligje kundër ushtrimeve të tilla, kështu që ato në kuptimin e vërtetë nuk kanë qenë shkelje. Në atë kohë nuk kishte asnjë vend publik për qasje në internet, individët kryesor që kishin ndonjë leje për përdorimin e kompjuterëve ishin edukatorët e kolegjit, studentët dhe hulumtuesit. Pasi që zhvillimi i internetit morri një hov të madh dhe frekuentimi në internet u bë më i zakonshëm, kështu filluan të rriten edhe aktivitet kriminale dhe shkeljet ligjore[20].

Fillimet e krimeve kibernetike janë vendosur në komunikimet mediatike nga "hakerët" siç i njohim sot duke filluar me "mashtrimet telefonike" nga vitet 70-ta e mëtej, ku filluan të keqpërdorin edhe telefonin, ku kornizat e hershme të telefonit u kthyen në një objektiv ku disa persona inteligjentë duke kërkuar dhe duke bërë hulumtime të panumërta në pajisjet telefonike dhe në të dhënat e tyre për të zbuluar informacione sekrete si dhe për të kuptuar se si ti keqpërdorin ato, gjetën kodet e duhura që i përdorën për të thirrur dhe për të folur falas në distanca të gjata. Padyshim që u pa se kornizat kompjuterike ishin në dispozicion për kryerjen e

[18] R, Anthony. & O, Kevin. & S, Jim. & H, R. Jon. & J, R. Benjamin. & R, Thomas. "Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcment, and Prosecutors", Syngress Publishing, 2007, fq.32
[19] Po aty;
[20] E, Chuck. & T, Jeff. "Computer Crime, Investigation, and the Law", Course Technology, 2011, fq.33

aktiviteteve kriminale dhe u bë e qartë nevoja për vendosjen e ligjeve dhe hetuesve të këtyre krimeve për të cilat krime u zhvilluan më shumë mundësi për kryerjen e tyre[21].

Tërësia e përvojave dhe zvhillimi i krimit kibernetik janë lehtë për tu ndjekur dhe harmonizuar me përparimin e vetë internetit. Shkeljet e para kryesore ishin padyshim të drejtëpërdrejta për të mbledhur të dhëna nga organizatat, megjithatë pasi që interneti filloj të përhapej më shumë, po kështu filluan të përhapen edhe sulmet, ku në vazhdim do të paraqesë disa çështje apo sulme kibernetike nga kohët e mëhershme e deri në ditët e sotme, të paraqitura në një blog nga një universitet privat Florida Tech Online[22]. Këto janë disa prej tyre:

Viti 1971 – "Cap'n Crunch" – John Draper, një krijues telefonash, përdor një bilbil lodrash nga një kuti drithërash për të sulmuar sistemin telefonik Amerikan dhe për të bërë thirrje falas në distanca të gjata. Drapers fiton pseudonimin kapiteni Crunch.

Viti 1973 – "Embezzlement" apo "Përvetësimi" – një tregat në një bankë lokale të Nju Jorkut përdor një kompjuter për të përvetësuar më shumë se 1.5 milion dollarë.

Viti 1981 – Dënimi i parë i krimit kibernetik – Ian Murphy, është personi i parë i dënuar për një krim kibernetik. Murphy pushtoi rrjetin e kompanisë telefonike amerikane dhe ndryshoj orët e brendshme, në mënyrë që përdoruesit të mund të bënin thirrje falas[23].

Viti 1982 – Virusi i parë kompjuterik – Elk Cloner është krijuar si një shaka nga një nxënës 15-vjeçar i shkollës së mesme. Ai i infektoi kompjuterët Apple II përmes floppy disketave[24].

Viti 1986 – E ashtuquajtura "taktika e tenxheres së mjaltit" – Clifford Stoll tërheq hyrësit më tej në rrjet, mblidhte të dhëna dhe gjurmonte ndërhyrjet, përpjekjet e tij përfundimisht çuan në arrestimin e Markus Hess dhe disa të tjerëve në Gjermaninë Perëndimore, të cilët ishin duke vjedhur dhe shitur fjalëkalime ushtarake, softuere dhe të dhëna tjera të KGB-së.

[21] The Evolution of Cybercrime, by Connor Madsen. Burim nga interneti: https://www.webroot.com/blog/2019/04/23/the-evolution-of-cybercrime/ (qasja e fundit 23.11.2020)
[22] A Brief History of Cyber Crime. Burim nga interneti: https://www.floridatechonline.com/blog/information-technology/a-brief-history-of-cyber-crime/ (qasja e fundit 24.11.2020)
[23] Po aty;
[24] Po aty;

Viti 1989 – Kodi i parë infektues në internet – Robert Morris, një student i diplomuar në Cornell, lëshon virusin Morris. Virusi u përhap në rreth 6,000 kompjuterë përmes një rrjeti të lidhur që i paraprinte internetit që njohim sot. Ky kod infektoi kompjuterët brenda NASA-s, Pentagonit dhe universiteteve duke përfshirë MIT, Berkley dhe Stanford.

Viti 1999 – Virusi i parë nëpërmes mesazheve me email – Virusi Melissa ndërpret më shumë se 1 milion llogari emailash në të gjithë botën dhe shkakton dëme prej rreth 80 milion dollarë. Krijuesi i virusit, programuesi kompjuterik i New Jersey, David L. Smith, mbajti 20 muaj burg federal dhe u gjobit me 5,000 dollarë.

Viti 2000 – Hakeri i parë i mitur në burg – Jonathan James në moshën 16 vjeç u deklarua fajtor për hakimin e paligjshëm të NASA-s, Pentagonit dhe Departamentit të Mbrojtjes.

Viti 2010 – Vjedhja e Google – Prona intelektuale e Google është vjedhur gjatë një sulmi shumë të sofistikuar nga hakerët kinezë.

Viti 2014 – Thyerja e Yahoo – Kriminelët kibernetik vjedhin informacionin e llogarisë nga të paktën 500 milion përdorues të Yahoo-së. Informacionet e përdoruesve si emrat, adresat e postës elektronike, numrat e telefonit, fjalëkalimet si dhe të tjera ishin të rrezikuara gjatë kësaj shkelje, e cila nuk u zbulua deri në dy vjet më vonë në 2016.

Viti 2017 – “WannaCry Hack” – WannaCry Hack, një sulm global ndalon sistemet kompjuterike në më shumë se 150 vende, duke prekur më shumë se 300,000 njerëz.

Viti 2018 – Universitetet e SHBA-ve ishin nën sulmin kibernetik – 144 universitetet me qendër në SHBA dhe 21 vende të huaja sulmohen nga hakerat iranianë. Fushata tre vjeçare rezultoi 3 miliardë dollarë humbje të pronës intelektuale me 31 terabajt informacion të vjedhur. Shumë prej sulmeve përdornin teknika të sofistikuara që kishin shënjestër më shumë se 10,000 profesorë dhe 47 kompani në sektorin privat u sulmuan gjithashtu.

Siç shihet nga rastet e paraqitura më lartë në të kaluarën ka pasur sulme apo krime kompjuterike më të lehta ku është dashur që sulmuesi të jetë dhe vetë prezent në vendin e ngjarjes dhe ka qenë më vështirë, kurse me ardhjen dhe përhapjen e internetit në vitet në vijim

sulmet janë rritur dhe dëmet janë bërë shumë më të mëdha për arsye se hakerët mund ti kryejnë sulmet nga katër anët e botës. Meqenëse kornizat e kompjuterëve dhe paisjeve tjera digjitale janë bërë jetike për punën e përditshme të organizatave, qeverive dhe njerëzve të cilët vendosin të dhëna të rëndësishme në to dhe të cilat janë apo konsiderohen gjëra me vlerë, do të jenë vazhdimisht një objekt sulmi për kriminelët kibernetik.

1.3 Mënyrat e përdorimit të kompjuterit si mjet për kryerjen e krimit kompjuterik

Kategorikisht siç dihet kompjuterët janë bërë pajisjet thelbësore më të specializuara që prekin çdo fushë të jetës së njeriut në botën bashkëkohore, kështu që mund të thuhet se kornizat e kompjuterëve janë bërë pjesa më e domosdoshme e mënyrës së jetesës, ku autori Veton Vula thekson se "kompjuteri paraqitet 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 vehtes apo të tjerëve tu sjellin përfitime"[25].

Funksionet e kompjuterëve mund të jenë të llojllojshme që mvaren nga veprimet ose qëllimet e grupeve apo një individi i cili dëshiron ta përdori kompjuterin në dobi pozitive apo ta keqpërdor atë në mënyrë negative për kryerjen e aktiviteteve kriminale dhe të pasurohet në mënyrë të paligjshme apo tu shkaktojë dëme të mëdha apo të vogëla organizatave apo personave tjerë. Përveç një numri të madh të mirash që na ofrojnë kompjuterët në botën bashkëkohore, ata poashtu luajnë një rol të rëndësishëm në kryerjen e krimeve kibernetike të cilat i kryejnë persona me një inteligjencë të lart të quajtur "haker", të cilët kanë njohuri të madhe për kryerjen e formave të ndryshme të këtyre krimeve, pra kompjuteri mund të përdoret apo shfyrtëzohet për role dhe funksione të ndryshme[26].

Për të kuptuar dukurinë e krimit kompjuterik plotësisht, është me rëndësi të karakterizohen metodat e përdorimit të kompjuterit, puna dhe vendi. Në këto aspekte Donn Parker studio evolucionin dhe rrjedhshmërin e krimeve në lidhje me kompjuterin ndër vite ku sipas tij ekzistojnë katër kategori të mënyrave të përdorimit të kompjuterit të cilat janë:

---

[25] Vula, Veton, "Kriminaliteti Kompjuterik", Prishtinë, 2010, fq.31

[26] Role of Computers in Crime, Burim nga interneti: https://www.geeksforgeeks.org/role-of-computers-in-crime/ (qasja e fundit 25.11.2020)

"-Një kompjuter mund të jetë objekt i një krimi, kur ai ndikohet nga akti kriminal p.sh kur një kompjuter është i vjedhur apo i shkatërruar.

-Kompjuteri mund të jetë subjekt i një krimi, kur ai është ambienti në të cilën është kryer krimi p.sh kur një kompjuter është infektuar nga një virus ose dëmtohet në ndonjë mënyrë tjetër për shqetësimin e personit që e përdor atë.

-Kompjuteri mund të përdoret si mjet apo instrument për kryerjen ose planifikimin e një krimi, p.sh kur përdoret për të falsifikuar dokumente ose për të hakuar kompjuterë tjerë.

-Vetë simboli i kompjuterit mund të përdoret për të kërcënuar ose për të mashtruar[27]."

Në studimin e tij shkencor për kuptiminm e kriminalitetit kompjuterik poashtu prof.dr Vesel Latifi paraqet një ndarje përafërsisht të njëjtë ku thekson se funksioni i kompjuterit nga aspekti kriminalistik mund të manifestohet në katër forma themelore të cilat janë:

- "kompjuteri si mjet i kryerjes së veprës penale, ku kryerësi e përdor kompjuterin për ta kryer veprëne caktuar penale, më së shpeshti mashtrimin, vjedhjen, shpërdorimin;
- kompjuteri si objekt i atakimit, me ç'rast kompjuterët dhe informacionet e vendosura në të janë qëllimi i atakimit kriminal;
- kompjuteri si mjet për organizimin, planifikimin, udhëheqjen dhe realizimin e aktiviteteve kriminale;
- kompjuteri, si mjet të cilin e shfrytëzon policia në parandalimin, sqarimin dhe të provuarit e veprave penale[28];"

Kompjuterët mund të jenë objektiv i një krimi apo një vend me kapacitete të mëdha për të mbajtur informacione të ndryshme në lidhje me një krim si dhe është instrument i mirëfilltë i përdorur për të kryer aktivitete të ndryshme kriminale. Një nga krimet më të përhapura janë viruset që lëshohen nëpërmjet postave elektronike nga hakerët në mënyrë të shpejtë dhe që

[27] Casey, Eoghan. "Digital Evidence and Computer Crime: Forensic science, Computers, and the Internet", Academic Press, 2011, fq.40

[28] Latifi, Vesel. "Kriminalistika", Prishtinë, 2014, fq.474

shkatërrojn kornizat ekzistuese të kompjuterëve duke shkaktuar dëme të mëdha miliona dollarësh organizatave dhe njerëzve. Kompjuterët poashtu janë objekte sulmi për hakerët të cilët marrin të dhëna të rëndësishme në mënyrë të palejuar si për shembull nga bankat ku mbahen informacionet e kartelave kreditore etj[29].

1.4 Sfidat e krimit kompjuterik

Në ditët e sotme krimet kompjuterike pasqyrojnë një nga sfidat më domethënëse për njerëzimin dhe hetuesit në përgjithësi. Këto shkelje nuk kërcënojn vetëm aktivitetet e administratave publike dhe private, megjithatë mund të rrezikojnë individin në veprimtaritë e tij të përditëshme. Rrjetet, si një risi tjetër e përshtatshme për përdorim nga klientë të panumërt, përveç ndikimeve pozitive, megjithatë sjellin edhe çrregullimin e çështjeve të ndryshme. Arritjet e jashtëzakonshme në këtë fushë hapën dyer të reja për sjellje armiqësore ndaj shoqërisë dhe krimit që më herët në të kaluarën nuk ishin të arritëshme[30].

Vitet 1990 – Ishin vitet kur filluan të paraqiten sfidat e reja të kriminalitetit kompjuterik. Paraqitja e ndërfaqes grafike "www" u shoqërua me një zhvillim të shpejtë të numrit të klientëve shfrytëzues të internetit që shkaktoi vështirësi të reja. Të dhënat e bëra ligjërisht të arritshme në një komb ishin tashmë të arritshme në të gjithë botën, madje edhe në kombet ku shpërndarja e të dhënave të tilla ishte e dënueshme. Një sfidë tjetër lidhur me shërbimet në internet që u testua veçanërisht në ekzaminimin e krimeve ndërkombëtare ishte shpejtësia e shkëmbimit të të dhënave. Ndërsa shkeljet të kryera me kompjuter ishin lokale, interneti i shëndrroi këto shkelje në krime ndërkombëtare. Më pas bashkësit kombëtare filluan që ti trajtojnë këto çështje më seriozisht[31].

Vitet 2000 – Në këtë shekull të ri, vazhduan të gjendeshin modele të reja në kryerjen e krimeve kibernetike, i cili shekull ishte i mbingarkuar me krime tashmë moderne dhe strategji të

[29] Lexo më shumë: Krimi Kibernetik – Kompjuterët si shënjestër ose mjete kriminale – Burim nga interneti: https://law.jrank.org/pages/11983/Cyber-Crime-Computers-targets-or-criminal-tools.html#ixzz6ekk8qWGv (qasja e fundit 25.11.2020)
[30] Nuredini, Ahmet, "Challenges in combating the cyber crime", Vol.5 No.19, Rome-Italy, 2014, fq.592
[31] ITU – International Telecommunication Union, "Understanding Cybercrime: Phenomena, Challenges and Legal Response", United Nations PUBN, 2012, fq.13

reja në të cilat paraqiteshin më shumë sfida për hetuesit në luftimin e këtyre krimeve, për shembull u përhapën krimet si "phishing" dhe "sulmet botnet" si dhe të tjera të cilat përdornin zhvillimin e teknologjisë me teknika të reja të pa zbuluara që ishin të vështira për tu hetuar dhe zbuluar. Kryerësit e këtyre krimeve u bënë të aftë ti automatizojnë sulmet, sasia e veprave dhe sfidave u zgjerua dhe u rrit më shumë nevoja për hetimin dhe zbulimin e krimeve kibernetike[32].

Krimi kibernetik vazhdon që të jetë një rrezik i përhershëm i cili prek të gjitha vendet si me zhvillim të ulët ashtu edhe ato me zhvillim të lartë. Kombet në të gjithë botën vazhdojnë të luftojnë pushtimin e këtij krimi që ka prekur institucionet qeveritare, shoqërinë e përbashkët, organizatat si dhe qytetarët në përgjithësi ku përballen me sfida të shumëta në këtë fushë.

Në bazë të revistës së zbatimit kibernetik me çështje të veçanta e publikuar në partneritet me gazetën e ligjit dhe politikës së sigurisë kombëtare në SHBA:

> "Në vitin 2008, kishte rreth 1.5 miliard shfrytëzues të internetit në të gjithë botën, kurse në vitin 2018 Bashkimi Ndërkombëtar i Telekomunikacionit e vendosi atë numër në 3.9 miliardë – më shumë se gjysma e popullsisë globale. Numri i pajisjeve të rrjetit vlerësohet të rritet në më shumë se trefishi i popullsisë globale deri në vitin 2022. Ndërsa kompanitë e sigurisë vazhdojnë të zhvillojnë mjete për ti mbajtur shfrytëzuesit më të sigurt, kriminelët kibernetik vazhdimisht aplikojnë teknologji të reja dhe metoda sulmi për tu shmangur identifikimit dhe për ti kryer krimet e tyre me lehtësi"[33].

Ka diskutime të shumëta në lidhje me sfidat e luftimit të kriminalitetit kompjuterik, mirëpo profesori Ajeet Singh Poonia i thekson disa prej tyre të cilat janë:

a) "Mungesa e vetëdijes dhe kulturës së sigurisë kibernetike, si në nivelin individual ashtu edhe në atë organizativ.
b) Mungesa e fuqisë punëtore të trajnuar dhe të kualifikaur për të zbatuar kundër masat.

[32] Po aty;
[33] Statistika nga Gazeta e ligjit dhe politikës së sigurisë kombëtare në SHBA, Burim nga interneti: https://www.thirdway.org/report/countering-the-cyber-enforcement-gap-strengthening-global-capacity-on-cybercrime (qasja e fundit 27.11.2020)

c) Asnjë rregullë e llogarive e-mail sidomos për forcat mbrojtëse, policinë dhe personelin e agjencisë së sigurisë.
d) Sulmet kibernetike vinë jo vetëm nga terroristët por gjithashtu nga vendet fqinje në kundërshtim me interesat kombëtare.
e) Tek vendet me zhvillim të ulët mungon njohuria e nevojshme nga ana e policisë për sektorin e kompjuterëve, kështu që ata janë pothuajse analfabetë ndaj krimit kibernetik.
f) Shpejtësia e ndryshimeve të teknologjisë kibernetike gjithmonë e mund progresin e qeverisë dhe sektoreve tjera që ata mos jenë në gjendje të identifikojnë origjinën e këtyre krimeve.
g) Forcat e sigurisë dhe autoritetet e zbatimit të ligjit nuk janë të pajisur mjaftueshëm për të adresuar krimet e teknologjisë së lartë.
h) Protokollet aktuale nuk janë të mjaftueshme, gjë që identifikon përgjegjësinë hetimore për krimet që shtrihen ndërkombëtarisht.
i) Buxhetet nga qeveria për qëllime të sigurisë kibernetike veçanërisht për trajnimin e zbatuesve të ligjit dhe hetuesve janë më pak në krahasim me krimet e tjera[34].”

Agjencia e Unionit Europian për bashkëpunim në zbatimin e ligjit e njohur si EUROPOL, së bashku me EUROJUST apo Agjencinë e Unionit Europian për bashkëpunim me drejtësinë penale kanë identifikuar disa sfida të përbashkëta të shteteve në luftimin e krimit kibernetik në bazë të analizave me ekspertë të ndryshëm si dhe nga praktika e zbatuesëve të ligjit dhe nga perspektiva juridike. Këto sfida të identifikuara ndahen në pesë kategori të cilat janë:

“1. humbja e të dhënave; 2. humbja e lokacionit; 3. sfidat e shoqëruara me kornizat ligjore ndërkombëtare; 4. pengesat për bashkëpunim ndërkombëtar dhe 5. sfidat e partneritetit publik-privat[35].”

[34] Poonia, S, Ajeet, *“Cyber Crime: Challenges and its Classification”*, *Vol.3,* Issue 6*,* 2014, fq.119 https://www.ijettcs.org/Volume3Issue6/IJETTCS-2014-12-08-96.pdf
[35] Europol and Eurojust Public Information, “Common challenges in combating cybercrime”, JOINT REPORT, 2019, fq.3, (https://www.eurojust.europa.eu/common-challenges-combating-cybercrime-identified-eurojust-and-europol qasja e fundit 30.11.2020)

Padyshim që ka më shumë vështirësi dhe sfida të luftimit të krimit kibernetik në shtrirje më të gjërë që kërkojnë aktivitetet të ndryshme, përfshirë një shumëllojshmëri të rrugëve në eksplorimin dhe hetimin e tyre. Sfida më e mirëfilltë dhe më e madhe nga të gjithë është konsolidimi i këtyre aktiviteteve në një tërësi plani apo projekti për përpjekje të vazhdueshme në trajtimin e vështirësive të luftimit të krimit kibernetik në bashkëpunim ndërkombëtar për një periudhë më të gjatë kohore, që këto plane të arrijnë një efektivitet të lartë duke pasur ndikim pozitiv për një internet më të sigurtë.

1.5 Viktimat e krimeve kompjuterike

Për shkak të zhvillimit apo përmirësimit të internetit në dy dekadat e fundit numri i viktimave të këtij krimi është vazhdimisht në rritje. Krimet që më parë kryheshin "offline" tanimë kryhen gjithashtu në internet, duke lënë të kuptohet se krimi ka evoluar me rritje të madhe duke e përdorur internetin si mjet lehtësues për kryerjen e krimeve kompjuterike. Kjo i bën dukshëm krimet dhe kriminelët më të rrezikshëm, duke i fuqizuar ata që të arrijnë një numër më të madh të viktimave dhe të ndërhyjnë në privatësinë e tyre personale në mënyrë më të drejtpërdrejtë. Si viktima të krimeve kompjuterike mund të jenë: persona individual të moshave të ndryshme, qeveritë, organizatat, kompanitë, bizneset, institucionet shtetërore etj.

Hapësira e krimit kibernetik po rritet poashtu për shkak të komunikimit eksponencial, rritjes së njohurive mbi temën e këtij krimi, vetëdijes kulturore dhe elektronikës moderne, paisjeve të ndryshme, metodave dhe teknikave të reja të sofistikuara, ku me të gjitha këto padyshim që rritet edhe numri i aktiviteteve kriminale të paligjshme. Krimi kibernetik në krahasim me krimet tjera zakonisht ka nevojë për një shpenzim më të vogël dhe mund të kryhet nga vende të ndryshme, ku viktimat mund të sulmohen dhe dëmtohen nga këto krime pa ndonjë kufizim gjeografik nga katër anët e botës[36].

Viktimat e krimeve kompjuterike janë të moshave të ndryshme dhe vijnë nga të gjitha sferat e jetës, meqenëse këto krime kryhen pothuajse në heshtje, për fat të keq shumë viktima nuk janë në dijeni se janë mashtruar derisa shohin se llogaritë e tyre bankare janë vjedhur.

[36] Ch, Mohamed. & D, Ashraf. & K, A. Mohammad. & T, Sapna. "Cybercrime, Digital Forencsics and Jurisdiction", Vol 593, Springer, 2015, fq.10

Supozohet se afërsisht 1 në 10 persona janë prekur nga krimi kibernetik, të cilët janë më të rrezikuar apo kanë më shumë gjasa të vidhen nga një kriminelë duke përdorur kompjuterin jashtë vendit, sesa duke ecur në rrugë[37]. Në bazë të statistikave të numëruara në vitin 2015 kishte 6 milionë viktima të krimeve në internet duke përfshirë mashtrime me kartat bankare, vjedhje identiteti, mashtrimet në blerjet online, ngacmimet apo përndjekjet në internet etj[38].

Në të gjitha vendet e botës regjistrohet një numër i madh viktimash të cilët bien pre e formave të ndryshme të krimeve kiberernetike tek të cilët ndikojnë faktorë apo role të ndryshme siç janë: përdorimi i mjeteve digjitale bashkëkohore si kompjuterët dhe telefonat e mençur që i kryejnë të gjitha punët nga to dhe pothuajse përdorimi i tyre është bërë i domosdoshëm, interneti me shpejtësi të lartë, mungesa e vetëdijes apo njohuris për sigurinë e tyre në internet si dhe të tjera.

Prandaj është shumë e rëndësishme që çdo person që bëhet viktim nga këto krime të dijë se çfarë hapash duhet të ndërmarri në vazhdim të cilat janë të njejta pothuajse në gjithë botën. Këto janë disa nga veprimet që duhet të ndërmerren menjëher për të minimizuar rrezikun: shkëputja nga sistemi kompjuterik, ndërmarrja e veprimit ligjor, informimi i kontakteve dhe ndërmarrja e hapave parandaluese për të ardhmen.

Shkëputja nga sistemi kompjuterik – për të mos humbur të dhëna apo infromacione të mëtejshme, lëvizja e parë është shkëputja nga komjuteri dhe interneti.

Ndëmarrja e veprimit ligjor - Çështja duhet të raportohet në polici menjëherë dhe të gjitha specifikat siç janë: natyra e krimit, të dhënat përkatëse, dëmi i shkaktuar, si dhe të gjitha informacionet tjera duhet të raportohen, mos shtyhet apo vonohet procesi.

Informimi i kontakteve - Kriminelët mund të shfyrtëzojnë vjedhjen e identitetit ose të dhënat për të vjedhur informacione nga kontakte tjerë në internet, kështu që ata duhet të njoftohen për të zvogëluar dhe shmangur rrezikun e keqpërdorimeve të mëtejshme.

[37] Burim nga interneti: https://www.turremgroup.com/1-in-10-people-have-become-a-victim-of-cybercrime/ (qasja e fundit 1.12.2020)
[38] Po aty;

Ndërmarrja e hapave parandaluese për të ardhmen – Meqenëse këto shkelje vazhdojnë të jenë një kërcënim dhe askush nuk është i sigurt apo imun prej tyre, duhet marrë disa masa siç janë instalimi i anti-virusave në sistemin operativ, përdorimi i fjalëkalimeve të forta, mosdhënia e informacionit për kartat bankare etj. Marrja e masave të duhura sigurisht që ndihmojnë në zbutjen apo parandalimin e dëmit nëse ndërmerren në kohën e duhur[39].

KAPITULLI I DYTË

2. Format më të përhapura të kriminalitetit kompjuterik në botën bashkëkohore

2.1 Kategoritë dhe llojet e kriminalitetit kompjuterik

Interneti dhe numri i përdoruesve të internetit janë zgjeruar më shpejt sesa mund ta imagjinonim. Krimi në internet prek miliona njerëz çdo ditë në të gjithë botën. Ndërsa njerëzit përdorin pajisje të ndryshme në një shoqëri të orientuar teknikisht për ta bërë jetën më të lehtë dhe vazhdojnë aktivitetet e tyre në hapësirën kibernetike dhe bëjnë më shumë nga puna e tyre në internet, kjo ka krijuar mundësi masive për të kryer krime kibernetike. Këto aktivitetet përfshijnë kategori të reja të veprave penale dhe forma të reja të krimit siç janë vjedhjet e identitetit, krimet e pronës dhe mashtrimet në internet.

Efekti i globalizimit është se njerëzit në të gjithë botën janë të lidhur njëri me tjetrin në çdo kohë. Përdorimi i vazhdueshëm i teknologjisë ka pasur një efekt rrënjësor në mënyrën se si njerëzit angazhohen dhe kryejnë punët e tyre të përditshme. Interneti në mënyrë të arsyeshme poashtu lidh ekonomikisht individ dhe biznese nga katër anët e globit. Sidoqoftë, interneti dhe makineritë kanë paraqitur dhe do paraqesin rreziqe të tilla që mund të kenë një efekt të dëmshëm mbi civilizimin.

[39]Action against Cyber Theft, DBS, Burim nga interneti: https://www.dbs.com/act/4-important-steps-that-all-cyber-crime-victims-must-take.html (qasja e fundit 2.12.2020)

Krimi kibernetik më parë është kryer kryesisht nga individë apo grupe të vogëla. Aktualisht është vrejtur se rrjetet kriminale kibernetike shumë të sofistikuara i bashkojnë individët në kohë reale për të kryer krime në një nivel global. Kriminelët që marrin pjesë në krime kibernetike sot nuk drejtohen nga egoja apo përvoja, në vend të kësaj ata duan të përdorin njohurit e tyre për të fituar para në mënyrë të paligjshme, meqenëse e kanë të lehtë këtë mënyrë pa qenë e nevojshme të bëjnë një punë të ndershme, ata e përdorin fuqin e tyre për të mashtruar dhe manipuluar njerëzit.

Krimi në internet është rezultat i rritjes së pandërprerë të teknologjisë kompjuterike. Në të gjitha sferat e jetës, fuqia e teknologjisë kompjuterike ka mundësuar që krimi kibernetik të përhapet globalisht. Për shkak të rrezikut të lartë dhe karakterit global, krimi kibernetik kryhet në kategori dhe lloje të ndryshme në hapësirën kibernetike.

Krimet kibernetike ndahen në tre kategori kryesore: krime kundër individëve, kundër pasurive apo pronës si dhe krimet kundër qeverisë. Në varësi të kategorive, llojet e metodave të përdorura dhe nivelet e kompleksitetit ndryshojnë[40].

Krimet kibernetike kundër individëve – kjo kategori e krimit kibernetik kryhet në forma të ndryshme duke i shkaktuar dëm financiar një individi i cili është viktimë e sulmit apo edhe dëm psiqik e cila përfshin një person që ndan infromacion në internet me qëllim të keq ose të paligjshëm, kjo mund të përfshijë biseda kibernetike, shpërndarjen e pornografisë dhe trafikimin etj.

Krimet kibernetike kundër pasurisë apo pronës – këto krime janë analoge me një shembull në jetën reale të një krimineli që mban informacionin e bankës ose kartës së kreditit në mënyrë të paligjshme. Hakeri vjedh detajet bankare të një individi për të marr qasje në të holla, për të bërë transaksione në internet ose për të kryer mashtrime për ti bërë njerëzit të japin të dhënat e tyre. Ata gjithashtu mund të përdorin softuer të infektuar apo me qëllim të keq për të fituar akses në informacione të ndryshme në faqet e internetit.

[40] Types of Cybercrime – Panda Security, Burim nga interneti: https://www.pandasecurity.com/en/mediacenter/panda-security/types-of-cybercrime/ (qasja e fundit 09.12.2020)

Krimet kibernetike kundër qeverisë – këto krime janë më pak të zakonshme por janë krime të rënda. Një vepër kundër shtetit shpesh quhet terrorizëm kibernetik. Krimi kibernetik kundër qeverisë do të thotë hakimi i faqeve të internetit të qeverisë, faqet e internetit të ushtrisë ose përhapjen e propagandës. Këta shkelës janë zakonisht terroristë nga kombet ose qeveritë e shteteve tjera[41].

Në botën e sotme, teknologjia e lartë gjindet kudo dhe nuk është për tu habitur që ajo gjithashtu ka hyrë në fushën kriminale. Kompjuterët gjithnjë e më shumë po bëhen arma e zgjedhur për një garë të re kriminelësh. Mirëpo krimet e reja kompjuterike inkurajojnë mënyra krijuese për ta kundërshtuar apo luftuar atë, duke çuar në një shumëllojshmëri të gjerë të teknologjive dhe strategjive të sofistukuara të sigurisë kompjuterike, si dhe rritjen e shpejtë të ligjeve dhe legjislacionit në lidhje me krimet kompjuterike.

Ekzistojnë ndarje të ndryshme të kategorive të krimeve kibernetike, mirëpo Konventa e Budapestit mbi krimin kibernetik në kapitullin e dytë të saj i paraqet këto kategori apo shkelje lidhur me kompjuterin të cilat janë:

a) Falsifikimi i lidhur me kompjuterin;
b) Mashtrimi në lidhje me kompjuterin;
c) Shkeljet në lidhje me pornografinë e fëmijëve;
d) Kundërvajtjet në lidhje me shkeljet e të drejtës së autorit dhe të drejtat e lidhura me to[42].

Një ndarje tjetër e cila është cilësuar si një nga më të rëndësishmet nga shumë autorë tjerë është ajo e autorit David Wall i cili krimet apo shkeljet kibernetike i ndanë në disa kategori:

1) **Shkelja kibernetike** – Kalimi i kufijve në pronën e njerëzve të tjerë dhe shkaktimi i dëmit psh. pirateria, viruset;

[41] Po aty;
[42] Konventa e Krimit Kibernetik: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (qasja e fundit 09.12.2020)

2) **Mashtrimet dhe vjedhjet kibernetike** – Vjedhja e parave, pronave apo mashtrimi i kartave të kreditit dhe shkeljet e pronës intelektuale;
3) **Pornografia kibernetike** – Aktivitete që shkelin ligjet në lidhje me turpin dhe moralin;
4) **Dhuna kibernetike** – Shkaktimi i dëmit psikologjik ose nxitja fizike e dëmit kundër të tjerëve, duke shkelur kështu ligjet që kanë të bëjnë me mbrojtjen e personit, p.sh gjuha e urrejtjes dhe përndjekja[43].

Në vazhdim autori Majid Yar i cili poashtu ka prezentuar të njejtën ndarje më lartë të autorit David Wall, ai më tej thekson se përveç këtyre mund të shtohet edhe kategoria "krimet kundër shtetit" që paraqesin çdo veprim që shkel legjislacionin që mbron reputacionin e kombit dhe infrastukturën e tij (p.sh. terrorizmi, spiunazhi dhe zbulimi i sekreteve zyrtare)[44].

Në vijim, autorja Marije T. Britz në librin e saj *Computer Forensics and Cybercrime*, i ka përfshirë në mënyrë më ekzakte dhe të gjithanshme kategoritë e krimeve kompjuterike ku poashtu sqaron se cilat lloje krimesh bëjnë pjesë tek secila kategori të cilat disa prej atyre llojeve janë më të përhapura në botën bashkëkohore të cilat janë:

- "Ndërhyrja në përdorimin e ligjshëm të kompjuterëve – ku bëjnë pjesë: sulmet DDoS (sulmet e shpërndara për mohimin e ofrimit të shërbimit), viruset, hakingu, terrorizmi kibernetik etj.
- Vjedhja e infromacionit dhe shkelja e të drejtës së kopjimit – spiunazhi industrial, vjedhja e identitetit, mashtrimi i identitetit etj.
- Shpërndarja e materialeve kontrabanduese ose fyese – pornografia e fëmijëve, lojërat e fatit në internet, materiale raciste etj.
- Komunikimet kërcënuese – zhvatje, përndejkja kibernetike, ngacmimi në internet etj.
- Mashtrimi – mashtrimi në ankand, mashtrimi me karta krediti, phishing (peshkimi), vjedhja e shërbimeve, manipulimi i aksioneve etj.

[43] Wall, David, "Crime and the Internet", London, 2001, fq. 3-7
[44] Yar, Majid, "Cybercrime and society", SAGE Publications, 2006, fq.11

- Krime ndihmëse – pastrim parash, komplot etj[45].”

Siç shihet më lart kemi një ndarje që përfshin pothuajse të gjitha llojet e krimeve kibernetike më të përhapura në botën bashkëkohore për të cilat do të shpjeog në vazhdim veç e veç se çka janë dhe si kryhen.

2.1.1 DDoS (Distributed Denial of Service) - Sulmet e shpërndara për mohimin e ofrimit të shërbimit)

Mohimi i shërbimit është një përpjekje për të shmanug përdorimin e sukseshëm të një shërbimi zakonisht në një faqe interneti nga konsumatorët e ndryshëm. Pra kur një faqe interneti mbingarkohet dhe nuk mund tu përgjigjet përpjekeve të lidhjeve sepse mbingarkohen nga sulmuesit me lidhje falso. Zakonisht, kërkesat për vërtetim bombardohen në një server rrjeti ku sulmi i mbingarkon burimet e synuara të kompjuterit, duke i detyruar ata të refuzojnë hyrjen e serverit në kompjuterët tjerë duke bërë kërkesa legjitime. Sulmet e shpërndara për mohimin e ofrimit të shërbimit ndodhin ndërsa një sulmues përpiqet të fitoj kontroll mbi disa kompjuterë dhe më pas fillon një sulm kundër një objekti ose synimi të veçantë duke përdour këta kompjuterë për sulme të shpërndara. Këto sulme nuk shkelin në mënyrë të qartë të dhëna ose përpiqen të vjedhin informacione personale, por ato padyshim që mund të shkaktojn dëm të konsiderueshëm ekonomik[46].

Mund të jetë shumë e vështirë për të hetuar sulmet e mohimit të shërbimit sepse ato kryhen më shpesh nga kompjutera të palëve të tretë që nuk dyshojnë. Për të dërguar një program të mohimit të shërbimit në pajisje të ndryshme, sulmuesi përdor një program apo virus i quajtur kalë Trojan. Pastaj, secili prej këtyre programeve fillon të nis një sulm të mohimit të shërbimit ndaj cakut të paracaktuar në një datë dhe kohë të caktuar. Mijëra kompjutera shpesh sulmojnë kompjuterin e synuar dhe ka shumë gjasa që askush nga pronarët e atyre sistemeve kompjuterike të mos kenë të bëjnë me sulmin ose majde janë apo jo të vetëdijshëm se ata janë pjesmarrës në atë sulm[47].

[45] Britz, T. Marjie, “Computer Forensics and Cyber Crime an Introduction”, Pearson, 2013, fq.76
[46] Maras, M. H. “Computer Forenscis: Cybercriminals, Laws, and Evidence”, Jones & Barlett Learning, 2014, fq.29
[47] Easttom, C. & Taylor, J. “Computer Crime, Investigation, and the Law”, Course Technology, 2011, fq.24

2.1.2 Hakingu (hacking)

Hakingu është një shkelje penale e kundërligjshme kundër sistemeve kompjuterike për qëllim të prishjes, manipulimit dhe përgjimit të sistemeve të informacionit. Ky akt karakterizohet nga ndërhyrje të paautorizuara në sistemet e huaja kompjuterike, duke nënkuptuar ndërhyrje të dhunshme në objektet e huaja në kontekstin klasik[48]. Ekzistojnë dy mënyra për ta bërë këtë punë në praktikë, e para prej të cilave është sigurimi i infromacionit të duhur me metoda dhe strategji të ndryshme për ndërhyrje efektive në sistemet kompjuterike, të tilla si sistemet operative, bazat e të dhënave etj. Lloji i dytë është ndërtuar sipas konceptit të "provoni, bëni një gabim, hiqni gabimin" me të cilin sulmuesi përpiqet të ndërhyjë në parametrat mbrojtës për depërtimin në një sistem të caktuar informacioni[49].

Aktivitetet e hakingut mund të bien në secilën kategori, këto qasje kryhen nga motive të ndryshme dhe kanë kompleksitete të veçanta. Hakimet si aktivitete më konvencionale kriminale kanë vetëm disa karakteristika që mund të ndryshojnë në mënyrë dramatike. Mund të ketë individë të caktuar haker në nivel më të ulët amaterë të cilët krenohen veçanërisht kur kryejn disa hyrje të lehta të palejuara nëpër struktura të ndryshme sa për gëzimin e tyre të plotë. Operacionet e tyre mund të variojnë nga kërkimi nëpër kompjuter të fqinjëve të tyre deri në eksplorimin e gropave të bazave të të dhënave sekrete qeveritare. Është vështirë të përcaktohet por disa vlerësime kanë treguar se vetë në SHBA sasia e ndërhyrjeve kompjuterike është në miliona, ndërsa të tjerë tregojnë se kostoja për publikun tejkalon disa miliardë dollarë[50].

Hakingu është një fenomen global i cili nuk është i kufizuar por përfshin të gjitha vendet e botës. Pothuajse çdo vend në të cilin është në dispozicion teknologjia kompjuterika gjenden hakera. Këta njerëz shfaqin ngjashmëri befasuese, pavarësisht nga origjina e tyre kombëtare.

[48] Vula, Veton, "Kriminaliteti Kompjuterik", Prishtinë, 2010, fq.102
[49] Po aty, fq.102
[50] Britz, T. Marjie, "Computer Forensics and Cyber Crime an Introduction", Pearson, 2013, fq.61

2.1.3 Viruset kompjuterike (computer viruses)

Një virus kompjuterik është një program i vetë-replikuar që përhapet në programet e zakonshme në një sistem kompjuterik, duke shtuar kopje të vetvetes dhe që ka qëllime të dëmshme. Ndonjëherë disa disqe rezervë pishen apo shkatrrohen edhe para se të identifikohet virusi. Viruset poashtu mund të gjenden apo zbulohen më shpesh nëpër disqe me softuer të hakuar apo të infektuar[51]. Viruset kompjuterike kanë kërcënuar përdoruesit që kanë lënë pas dore të instalojnë sigurinë e duhur që nga krijimi i parë i teknologjisë kompjuterike. Numri i viruseve kompjuterike është rritur ndjeshëm që nga ajo kohë. Numri i sulmeve të virusit jo vetëm që është rritur por edhe metodat dhe rolet e viruseve kanë ndryshuar. Viruset kompjuterike historikisht janë transmetuar përmes pajisjeve të ruajtjes siç janë disketat, megjithëse shumica e viruseve tani shpërndahen përmes internetit si bashkëngjitje në e-mail ose dokumente të shkarkuara nga përdoruesit. Këto strategji të sukseshme moderne kanë përshpejtuar ndjeshëm infeksionin e viruseve dhe kanë rritur në mënyrë dramatike numrin e sistemeve kompjuterike të infektuara[52].

Zhvillimi dhe shpërndarja e viruseve ndodh kur një program i infektuar përhapet nga një sistem në sistemin tjetër i cili shkakton dëme të ndryshme në çdo pajisje. Ka disa lloje të viruseve: **virus polimorf** i cili krijon kopje të vetes të ndryshme por funksionuese, **virus i fshehtë** është ai që fsheh ndryshimet nëpër dokumente kur është aktiv, **virus si një infektue i shpejt** që infekton programet dhe nuk lejon askes në to, **virus si një infektues i ngadaltë** që mund të infektojë dokumentet vetëm kur ato gjenerohen ose ndryshohen[53]. Katër nga arsyet që individët ndërtojnë viruse dhe u vendosin emra të ndryshëm janë: është një mënyrë për të tërhequr vëmendjen, marrin ndjenjë kënaqësie nga zhvillimi i diçkaje që prek një numër të madh individësh, kanë përfitim ekonomik, si pasojë e virusit të tyre krijuesit mund të entuziazmohen për çdo dëm që shkaktojnë etj[54].

---

[51] Bainbridge, David, "An Introduction to Computer Law", Longman, New York, 2004, fq.399

[52] ITU – International Telecommunication Union, "Understanding Cybercrime: Phenomena, Challenges and Legal Response", United Nations PUBN, 2012, fq.20

[53] EC-Council, "Computer Forenscis: Investigating Network Intrusions and Cyber Crime", Cengage Learning, 2009, kapitulli 6, fq.6-3

[54] Po aty;

Autorët e viruseve bëjnë marrëveshje me haker të ndryshën në ditët e sotme, duke i kthyer viruset nga hobi në një biznes. Këta individë janë në biznesin e hakimit të kompjuterëve për të vjedhur të dhëna të ndryshme që i keqpërdorin për përfitimet e tyre. Biznese apo komani të ndryshme krijojnë programe antivirus që përpiqen ti shmaning ose ndalojë sulmet e pajisjeve nga virusët e ndryshëm, prandaj njerëzit duhet mos i neglizhojnë dhe ti përdorin sa më shumë për sigurinë e tyre.

2.1.4 Terrorizmi kibernetik (cyberterrorsim)

Me termin terrorizëm kibernetik nënkuptojmë përdorimin e sistemeve kompjuterike të lidhur me internet ndërmjet tyre thjesht për të kryer apo lëshuar sulme terroriste që në realitet dikush ose ndonjë grup i përdorin këto teknika kompjuterike për fillimin e një sulmi ushtarak ose terrorist kundër çdo objektivi. Sipas FBI-së (byros federale për hetime) "terrorizmi kibernetik është sulm i paramenduar, i motivuar politikisht kundër informacionit, sistemeve kompjuterike, programeve kompjuterike dhe të dhënave të cilat rezultojnë në dhunë kundër shënjestrave jo-luftarake nga grupe nënkombëtare ose agjentë klandestinë"[55].

Terrorizmi kibernetik përfshin përdorimin e kompjuterëve dhe teknologjive shoqëruese për të detyruar një popullatë civile dhe për të manipuluar politikën e qeverisë së synuar ose përndryshe të ndikoj në sjelljen e saj për të shkaktuar dëm. Sulmet e tyre tentojnë të shkaktojnë reagime të veçanta në qeveri dhe shoqëri. Terrorizmi kibernetik nuk njeh kufij fizikë, gjeografikë sepse interneti u siguron autorëve autorizimin e hyrjes për individët, organizatat dhe bizneset në të gjithë globin. Shkalla e këtyre rreziqeve sfidon konceptimet tradicionale të sovranitetit të kombeve sovrane, duke e bërë shënjestrimin e krimit kibernetik dhe terrorizmit kibernetik veçanërisht të vështirë për autoritetet botërore[56].

Për të përshkruar terrorizmin kibernetik, ekzistojnë dy pikëpamje; të bazuara në efekte dhe të bazuara në internet. Terrorizmi kibernetik ndodh në një situatë të bazuar në efekt, kur

[55] Easttom, C. & Taylor, J. "Computer Crime, Investigation, and the Law", Course Technology, 2011, fq.210
[56] Maras, M. H. "Computer Forenscis: Cybercriminals, Laws, and Evidence", Jones & Barlett Learning, 2014, kpt.7 fq.2

sulmet kompjuterike çojnë në një situatë ku krijohet frikë që është e ngjashme me një sulm konvencional terrorist. Sulmet bëhen për të shkaktuar dëm serioz ekonomik në situata të bazuara në internet. Katër zona janë përfshirë në qëllimin e një sulmi kibernetik të cilat janë: humbja e reputacionit, humbja e disponueshmërisë, humbja e privatësisë dhe dëmtimi fizik[57].

2.1.5 Vjedhja e identitetit (identity theft)

Meqenëse termi vjedhje e identitetit përfshin një numër aktivitetesh kriminale që përfshijnë vjedhje ose keqpërdorim të informacionit personal, nuk ka një koncept të njohur gjerësisht të vjedhjes së identitetit. Vjedhja e identitetit rrallë është një vepër penale e vetme, por konsiston në kryerjen e një game të gjerë të veprave të tjera, shumë prej të cilave janë krime të njohura nga ne. Në shtetet e bashkuara të Amerikës, ligji federal i tanishëm vjedhjen e identitetit e konsideron si krim federal kur dikush

> "me vetëdije transferon, përpunon ose përdor, pa autorizim të ligjshëm, një mjet identifikimi të një personi tjetër me qëllim për të kryer, ose për të ndihmuar dhe mbështetur çdo veprimtari të paligjshme që përbën shkelje të ligjit federal, ose që përbën një krim sipas ndonjë ligji të zbatueshëm shtetëror ose vendor"[58].

Vjedhja e identitetit më së shumëti është bërë e mundur me ekzistencën e sistemeve të pagesave elektronike. Shitësit janë në gjendje tu ofrojnë mallra dhe shërbime të huajve në ekonominë globale në këmbim të pagesës online që mbështetet në të dhëna që lidhin blerësin me një llogari të veçantë në internet. Vjedhja e identitetit përfshin marrjen e informacionit të mjaftueshëm për një individ tjetër i cili i keqpërdor ato duke blerë mallra nëpërmjet tarifës së llogarisë së një personi tjetër, ku d.m.th se vjedhja e identitetit përdoret më së shumëti për përfitime financiare[59].

[57] C. Subramanian, "CYBER SECURITY", International Journal of Recent Scientific Research, Vol. 3, Issue 3, 2012, fq.197
[58] Finklea M. Kristina, "Identity Theft: Trends and Issues", CRS Report of Congress, New York, 2010, fq.2
[59] Anderson, B. K, Dubrin, E. Salinger A. M, "Identity Theft", Journal of Economic Perspectives, Vol.22, 2008, fq.171

Ekzistojnë tre faza apo kategori të vjedhjes së identitetit, këto faza janë: E para është përvetësimi i identitetit nga vjedhja, ku mund të bëjnë hakime kompjuterike, mashtrime, përgjime të postës etj. E dyta është përdorimi i identitetit për përfitime financiare ose për ti shpëtuar arrestimit ose për të fshehur identitetin e dikujt nga autoritetet e ligjit[60]. Krimet në këtë pikë mund të përfshijnë blerjen e llogarive, hapjen e llogarive të reja, përdorimin e kartave bankare, blerja e dokumentave shtesë të identitetit të tilla si patentë shoferi, pasaporta, viza etj. Faza e tretë është identifikimi, megjithëse zbulohen lehtësisht disa keqpërdorime të tilla, vjedhja apo mashtrimi "klasik" i identitetit kërkon një periudh të gjatë zbulimi zakonisht nga 6 muaj deri në disa vjet, provat tregojnë se sasia e dëmit të pësuar tek viktima është e ndërlidhur me kohën që duhet për ta zbuluar atë, ku tek të cilat kërkohet një hulumtim i rëndësishëm[61].

2.1.6 Pornografia e fëmijëve (child pornography)

Sipas departamentit të drejtësis në SHBA, pornografia e fëmijëve është një formë e abuzimit seksual të fëmijëve. Pornografia e fëmijëve përshkruhet nga ligji federal si çdo përfaqësim vizual i veprimtarisë së qartë seksuale që përfshin një të mitur (person më pak se 18 vjet). Shpesh të referuara si video të shfrytëzimit seksual të fëmijëve janë imazhe të pornografisë së fëmijëve[62]. Organizata ndërkombëtare e policisë kriminale (interpol) për veprat kundër të miturëve definon pornografinë e fëmijëve si: "... pasojë e shfrytëzimit ose abuzimit seksual të kryer ndaj një fëmije. Mund të përkufizohet si çdo mjet për të përshkruar ose promovuar abuzimin seksual të një fëmije, përfshirë shtypjen ose audion, përqendruar në veprime seksuale ose organet gjenitale të fëmijëve[63]."

Bazuar në rritjen e viktimizimit seksual, një studim përshkrues identifikoi disa nivele serioziteti dhe përfshiu krejt qëllimisht foto që bien apo nuk bien nën përcaktimin ligjor të pornografisë së fëmijëve, këto nivele janë: fotot treguese (imazhe jo-erotike/seksuale), fotot nudiste (të zhveshura ose gjysmëtë zhveshura), fotot erotike (fotografi të fshehta që tregojnë

[60] Newman, R. G, & McNally, M. M, "Identity Theft Literature Review", NCJRS report, 2005, fq. 5(v)
[61] Po aty;
[62] Definimi i pornografisë së fëmijëve nga departamenti I drejtësis në SHBA: https://www.justice.gov/criminal-ceos/child-pornography#: (qasja e fundit 27.12.2020)
[63] Taylor, M, & Qualye, E, & Holland, G, "Child pornography – an internet crime" Brunner-Routledge, 2004, fq.95

imazhe të fshehta), foto pozuese (pozim i qëllimshëm që sugjeron seksualitetin), pozat pornografike (paraqitje e qëllimshme seksuale ose provokuese), pozimi seksual i qartë (në zonat gjenitale), sjellja e qartë seksuale, imazhe pornografike të lidhura me dhunën, etj[64].

2.1.7 Ngacmimi në internet (cyberbullying)

Në aplikimin e teknologjisë së re, ngacmimi në internet është ngacmim real. Mund të zhvillohet në media sociale, në platforma për dërgimin e mesazheve, platforma për lojëra si dhe nga telefonat celularë. Është një veprimtari e përsëritur, që synon të trembë, bezdisë ose të poshtërojë ata që janë në shënjestër. Shembuj janë: përhapja e gënjeshtrave për fotografitë kompromentuese të dikujt ose ndarja e tyre në rrjetet sociale, dërgimi i mesazheve të dëmshme përmes platformave të mesazheve ose kërcënimeve, të imitojnë të tjerët dhe të dërgojnë mesazhe të ulëta në emër të tyre dhe të tjerëve. Ngacmimi ballë për ballë dhe ngacmimi në internet mund të ndodhin gjithashtu krah për krah. Sidoqoftë, ngacmimi në internet lë një gjurmë digjitale, një rekord që mund të dal i vlefshëm dhe të sigurojë prova për të ndihmuar parandalimin e dhunës[65].

Ngacmimi në internet ndodh brenda një grupi ose kulture më të gjerë i cili është pothuajse i ngjashëm me ngacmimin në jetën reale. Ndonjëherë, përpara tërë klasës ose shkollës së tyre nxënësit viktimizohen. Ashtu si me ngacmimin në jetën reale, ngacmimi në internet ka efekte të ngjashme negative për viktimën, duke përfshirë depresionin, dhunën, frikën, ankthin social, abuzimin e substancave narkotike si dhe deri te vetëvrasja. Poashtu mund të paraqiten edhe sëmundjet fizike të tilla si dhimbje stomaku, çrregullime të gjumit, dhimbje koke, lodhje dhe oreks të dobët janë simptoma që shpesh hasen nga shumë viktima, kurse disa nga viktimat gjithashtu mund të vuajnë nga efektet anësore në performancën në shkollë dhe në punë. Meqenëse autori i krimit mund të jetë anonim dhe krejt i panjohur për viktimën, ngacmimi në internet është më i ndërlikuar[66].

[64] Po aty;
[65] UNICEF – What is cyberbullying? https://www.unicef.org/end-violence/how-to-stop-cyberbullying (qasja e fundit 04.01.2021)
[66] Kremling, J. & Parker, A.M.S. "Cyberspace, Cybersecurity, and Cybercrime" SAGE Publications, 2017, fq.161

2.1.8 Fishingu (phishing)

Phishing ndodh kur njerëzit mashtrojnë të tjerët duke u paraqitur si kompani ekzistuese të ligjshme në mënyrë që të vjedhin informacionin personal të dobishëm të përdoruesve, të tilla si të dhënat e llogarisë dhe informacionin e kartës së kreditit. Kriminelët kibernetikë zakonisht përdorin një email legjitim të ngjashëm me pamjen nga një bankë që i kërkon viktimës të hapë një lidhje për të kontrolluar detajet e tij/saj. Ai ose ajo drejtohet në atë faqe interneti të rrejshme dhe informacionet që i jep shkojn drejtëpërdrejt tek phisheri pasi viktima fut informacionin personal dhe klikon butonin dërgo, kështu në këtë mënyrë ndodhë mashtrimi i tillë dhe kriminelët me të dhënat e vjedhura mund ti përdorin apo keqpërdorin në dobi të tyre[67].

Aktet e phisherëve përbëhen nga disa faza, të cilat janë: faza e parë është ***planifikimi*** – mashtruesi vendos se cilin biznes apo cilat persona do të shënjestrojë dhe mendon se si do të shkoj apo arrij në adresat e postës elektronike e atyre klientëve, faza e dytë është ***përgatitja*** – mashtruesit përcaktojnë cilat teknika do të përdoren për mbledhjen e të dhënave, faza e tretë është ***sulmi*** – mashtruesit dërgojnë mesazhet e rreme përmes kësaj veprimtarie që duket se vijnë nga dërguesit aktual dhe të vërtetë, faza e katërt ***mbledhja e të dhënave*** – mashtruesit mbledhin të dhënat që mbarten në faqen e internetit nga viktima, faza e pestë ***vjedhja e identitetit të klientit*** – mashtruesit përdorin të dhënat personale të viktimës për të bërë transaksione në mënyrë elektronike ose për të përdorur mashtrime në mënyra të tjera[68].

[67] Maras, M.H., "Computer Forensics: Cybercriminals, Laws, and Evidence", Jones & Barlett Learning, 2014, fq.41
[68] Vula, Veton, "Kriminaliteti Kompjuterik", Prishtinë, 2010, fq.80

2.2 Kryerësit e krimeve kompjuterike

Në kontekstin e përgjithshëm dhe të ngushtë, kryerësit e krimeve kompjuterike gjithashtu referohen pa dallim si "hakera". Në aspektin fenomenologjik, studimet zbulojn se nxënësit, praktikantët ose studentët që shpesh kanë fituar aftësitë e tyre të teknologjisë së informacionit me mjete autodidaktike janë hakera tipikë. Shumica e hakerave e kalojnë kohën e tyre të lirë veçanërisht me kompjuterë dhe punojnë shumë vetë pa qenë "socialisht të dukshëm" në këtë proces. Ata preferojnë të mbajnë ndërveprime joformale që rrjedhin qartë nga takime të çastit sesa nga përfshirje solide në sistemet dhe grupet shoqërore[69]. Për shkak të shfaqjes dhe disponueshmërisë së gatshme të grupeve të mjeteve malware të cilat janë softuerë specifikisht të dizajnuarë dhe të gatshëm për të shkaktuar dëme ose hyrje të paautorizuara nëpër sisteme, kriminelët e krimit kibernetik nuk kanë më nevojë për aftësi ose teknika të komplikuara. Megjithëse disa autorë të këtyre krimeve mund të kenë përfunduar trajnim të avancuar, kurse shumë kryerës tjerë të njohurë nuk kanë ndonjë arsimim të specializuar (veçanërisht në fushën e shkencës kompjuterike). Është vlerësuar se më shumë se 80% e akteve të krimit kibernetik vijnë nga një lloj veprimi i organizuar, me tregje të zeza të krimit kibernetik, infeksionimit të kompjuterëve, shitjes së të dhënave dhe informacionit financiar etj. Krimi kibernetik gjithashtu mund të zbatohet nga një shkallë e lartë e organizimit dhe mund ti jepet hua bandave të vogla kriminale, rrjeteve ad hoc ose krimeve të organizuara[70].

Pas krimeve në internet ka një larmi motivimesh. Theksi kryesor është në përfitimin financiar ose mund të jetë një formë proteste ose dëmtimi kriminal, mirëpo ka edhe arsye tjera si p.sh arsyeja e abuzimit të fëmijëve nuk është domosdoshmërisht për përfitim, kurioziteti apo sfida intelektuale, dashakeqësia e përgjitshme, hakmarrja, marrja e një njoheje ose ndikimi në

[69] Bässmann, Jörg, "Perpetrators in the field of cyber-crime", Bunderskriminalamt, 2015, fq.2 (II)
[70] Verleysen, Cindy, "Cybercrime: A theoretical overview of the growing digital threat", EUCPN Secretariat (eds.), EUCPN Theoretical Paper Series, European Crime Prevention Network, Brussels, 2015, fq.15

komunitetet në internet apo edhe thjesht mërzija janë arsye tjera për krim kibernetik[71]. Natyra demografike e shkelësve të ligjit pasqyron krimin tradicional në atë që shumica janë meshkuj të rinj, megjthëse profili i moshës po tregon se njerëzit më të moshuar kanë të bëjnë më shumë në lidhje me krimet e pornografisë së fëmijëve.

Në bazë të zyrës së kombeve të bashkuara për drogën dhe krimin sondazhe të ndryshme tregojnë se autorët e krimit kibernetik janë më shpesh midis moshës 18 dhe 30 vjeç. Sidoqoftë, kryerësit e përgjitshëm të këtij krimi mund të jenë më të rinjë se kriminelët e krimeve të zakonshme, ku shumica e kriminelëve kibernetik janë meshkuj. Varësisht se çfarë lloji krimi kibernetik kryejnë moshat janë të ndryshme, të marrim shembull profili i individëve që prodhojnë, shpërndajnë ose posedojnë pornografi fëmijësh është i ndryshëm ku kryhet nga meshkuj të moshave prej 15 deri 73 vjeç ku mosha mesatare është 41 vjeç[72]. Kryerësit e krimeve kompjuterike në përgjithësi janë të papunë kanë karakteristika të ndryshme duke përfshirë impulsivitetin, shkallën e lartë të agresionit, gënjeshtrat, emocionet e ngopura me pasuri, egozimin, problemet në sjelle si dhe të tjera.

2.3 Faktorët që ndikojnë në kryerjen e krimeve kompjuterike

2.3.1 Faktorët objektiv

Poashtu si tek llojet tjera të shkeljeve edhe krimi kibernetik ndikohet nga një larmi variablash unikë kriminogjenë objektivë. Së pari duhet të ndiqen variablat objektivë në specifikat e vetë teknologjisë së informacionit si dhe ritmi i rritjes së saj. Karakteristikat që e dallojnë këtë lloj krimi nga format e tjera janë:

1. Krimi kompjuterik është një krim i kryer nga shoqëritë moderne të zhvilluara, që tregon se është i lidhur ngushtë me shkallën e rritjes socio-ekonomike të arritur. Sa më e madhe të jetë shkalla e zhvillimit, aq më të përparuara janë strategjitë e performancës, ndërsa aq më të shumtë dhe më të aftë janë shkelësit;

[71] Po aty;
[72] United Nations Office on Drugs and Crimes, "Comprehensive Study on Cybercrime", Vienna, 2013, fq.41-42

2. Krimi kibernetik është krimi në shoqëritë urbane që bazohen në përdorimin e teknologjisë së informacionit në jetën e përditshme dhe në të njëjtën kohë janë të varur nga to;
3. Krimi në internet, si për nga përhapja e tij, ashtu edhe për nga pasojat e tij, është një krim global. Ky krim nuk njeh kufij, pasi mund të kryhet dhe të shkaktojë dëme nga katër anët e botës, nga çdo vend ku ndodhen korniza kompjuterike;
4. Ky krim si karakteristik të rëndësishme ka se është krim i njerëzve të arsimuar, pasi që për realizimin e tij kërkohet një shkallë e lartë e dijes dhe aq më e madhe është, më vështirë është identifikimi dhe parandalimi i autorit të krimit;
5. Krimi kompjuterik është një ndërthurje e dobësive komplekse, veçanërisht ato njerëzore dhe teknologjike që shmangin apo pamundësojnë luftimin e tij;
6. Është e vështirë për të luftuar dhe shmanugr krimin kibernetik, sepse edhe përdorimi i teknologjive më të përparuara nuk garanton ndonjë siguri efikase[73].

Në ditët e sotme kriminelët kibernetik shpesh zgjedhin një mënyrë të shpejtë për të fituar para të mëdha, si faktorë tjerë janë hyrja e lehtë në sistemet kompjuterike, ruajtja e të dhënave në një hapësirë të vogël, neglizhenca, humbja e provave, evolucioni i krimit kibernetik dhe të tjera.

2.3.2 Faktorët subjektiv

Ekzistojnë edhe faktorë kriminogjenë në kuptimin e ngushtë, përveç faktorëve kriminogjenë në kuptimin e gjerë që i përshtaten kësaj veprimtarie kriminale dhe inkurajojnë formimin, përhapjen dhe intensitetin e saj në nivel global, të cilët prekin kryersit e mundshëm të situatës specifike. Sipas autorit Petrovic kjo kategori faktorësh përfshin: Motivet, Gatishmërin dhe Mundësinë[74].

Për të kryer një ose më shumë veprime të veçanta kriminale, është e rëndësishme që në një moment të caktuar kohor, të përmbushen tre parakushte nga kryersi në të njëjtën kohë të cilat janë:

[73] Vula, Veton, "Kriminaliteti Kompjuterik", Prishtinë, 2010, fq.143

[74] Petrovic, S., "Kompjuterski Kriminal", Beograd, 2000, fq.108

- Motivi, për shkak të të cilit kryersi potencial do të ndërmerr veprimin;
- Gatishmëria e kryersit që për këtë të pranoi rrezikun e caktuar;
- Mundësia që veprimi kriminal të kryhet[75].

Motivet janë zakonisht të ndryshme ku mund të marrim parasysh si vijojnë: motivet financiare, vetitë, problemet mentale, konkurenca ekonomike, arsyet emocionale, motivet ideologjike, qëndrimi personal, kodi etik, motivet politike, etj.

Një pasojë e pandershmërisë së tij është gatishmëria e personit për të marrë pjesë në veprimtari të paligjshme. Kjo vlen për personalitetin e tij, gjë që është praktikisht e pamundur të provohet. Megjithëse sistemet nuk ofrojnë siguri të plotë, rreziku i kryerjes së një krimi të tillë mbetet në një farë mase, i cili ndryshon në varësi të mjedisit në të cilët përdoren aplikimet informatike[76].

KAPITULLI I TRETË

3. Hetimi dhe zbulimi i kriminalitetit kompjuterik

3.1 Metodika e hetimit dhe zbulimit të kriminalitetit kompjuterik

Në mënyrë që të identifikohen autorët e krimit digjital dhe qëllimet e tyre të vërteta, një hetim i krimit kibernetik është procesi i hetimit, analizimit dhe rikuperimit të të dhënave digjitale kriminalistike kritike nga rrjetet e përfshira në sulm, ku mund të jenë në internet ose në një rrjet lokal. Mekanizmi me të cilin policia apo hetuesit monitorojnë të dyshuarit duke përdorur kompjuterë njihet si hetim kibernetik. Kjo teknikë mund të përdoret për të ndjekur penalisht krimet kompjuterike ose për të monitoruar historinë kriminale duke përdorur forenzikën apo ekspertizën kompjuterike. Analiza kriminalistike është një studim

[75] Po aty, fq 109-110
[76] Armstrong, Illnea, "Real Risk or Shadow? The Threat of Cyberterrorsim", Article online: https://www.scmagazine.com/home/security-news/features/real-risk-or-shadow-the-threat-of-cyberterrorism/ (qasja e fundit 12.01.2021)

gjithëpërfshirës i problemeve të krimit dhe zbatimit të ligjit, si dhe çështjeve të tjera të studimit duke përfshirë faktorët socio-demografik, hapësinor dhe kohor, që ndihmojnë policinë apo hetuesit të ndëshkojë, të zbusë, të zbuloj dhe të parandalojë krimin[77].

Studimi nënkupton hetimin, vëzhgimin nga afër ose kërkimin e informacionit, kërkimet shkencore ligjore janë pra një hetim i përqendruar dhe sistematik i problemeve të krimit dhe çrregullimeve dhe çështjeve të tjera që lidhen me ruajtjen e rendit. Studimet kriminalistike nuk janë trilluese, ato përdorin procedura për mledhjen e të dhënave të shkencave shoqërore, metodave analitike dhe teknikave statistikore[78].

Ndryshe nga krimi klasik, ku provat materiale që mbajnë gjurmët e autorit dhe viktimës janë prova e pakundërshtueshme dhe në të vërtetë provat materiale sigurojnë rëndësinë e krimit të kryer nga autori, dmth lidh kryerësin dhe viktimën që ishin në vendin specifik ku ka ndodhur krimi në një kohë të caktuar. Për shembull: në rastin e një vrasje me armë zjarri, të gjitha gjurmët e gishtërinjëve të autorit mbesin aty apo gjenden nga eksperetiza daktiloskopike. Por nuk është e mundur të sigurohen prova të tilla të drejtpërdrejta ose përfundimtare në krimin kibernetik ose gjurmët e vijave papilare në kompjuter sepse nuk është e thënë që një krim i veçantë është kryer me atë apo në atë kompjuterë, me rëndësi është evidentimi i të dhënave elektronike digjitale, kodi për hyrjen në sistemin kompjuterik dhe arsyet për kryerjen e një krimi të veçantë kompjuterik[79].

Dallimi kryesor midis të dhënave në letër dhe atyre digjitale është niveli i njohurive të nevojshme për të rishikuar të dhënat dhe provat apo faktet digjitale, sasia e të dhënave të mbajtura dhe lehtësia me të cilën të dhënat digjitale mund të prishen ose humbin. Të dhënat në formë elektronike janë një burim alternativ i provave që mund të përdoren për të provuar një shkelje që ka ndodhur në botën virtuale apo në atë fizike. Këto janë pak më të vështira për

[77] Vula, Veton, "Kriminaliteti Kompjuterik" Prishtinë, 2010, fq.54
[78] Boba, Rachel, "Криминалистичко истражување – мапирање на криминалот", Nampress, 2001, fq.3
[79] Nikoloska, Svetlana, "Методика на истражување компјутерски криминалитет" Shkup, 2013, fq.78

tu hetuar dhe paraqesin probleme të reja për hetuesit në drejtim të përpunimit të të dhënave ose fakteve dhe provave të tilla dhe zbulimin apo kapjen e kryerësve të këtyre krimeve[80].

3.1.1 Roli i hetuesve të krimeve kibernetike

Një hetues ose detektiv i specializuar në krimin kibernetik njihet si hetues i krimit kibernetik. Këta hetues kërkohen shumë si në sektorin privat ashtu edhe në atë publik sepse ata kanë ekspertizën për të zgjedhur krimet e sotme komplekse në internet[81]. Qëllimi kryesor i një hetuesi të krimit kibernetik është të mbledh informacione nga rrjetet digjitale që mund të përdoren në hetimin e veprimtarisë së paligjshme të bazuar në internet ose hapësirë kibernetike. Shumë krime në botën e sotme përfshijnë më së shumëti përdorimin e internetit. Një hetues i krimit kibernetik mund të ndihmojë në mbledhjen e informacionit dhe të dhënave për të ndihmuar në hetimin dhe zbulimin e këtyre krimeve kibernetike.

Në fushën digjitale, hetuesit e aftë kanë një kuriozitet natyror të shoqëruar me dëshirën për të zbuluar provat, për të përcaktuar fakte dhe për të dhënë përgjigje për pyetjet teknike që lindin gjatë një hetimi. Për të përcaktuar sekuencat e ngjarjeve, përdoren arsyetimet deduktive dhe induktive. Për të miratuar ose hedhur poshtë teoritë e çështjeve, përdoren metodat tradicionale të zbatimit të ligjit të tilla si monitorimi, pyetja, kërkimi dhe kapja si dhe proceset e strukturuara të proceseve ligjore[82].

Cdo minutë të çdo dite, kriminelët kibernetik kërcënojnë rrjetet e sektorit privat dhe atë publik. Universitetet sulmohen për zhvillimin dhe rritjen e tyre, ndërsa kompanitë ndëshkohen për sekretet tregtare dhe informacione të tjera të rëndësishme. Vjedhësit e identitetit synojnë qytetarët dhe kidnapuesit në internet synojnë fëmijët. Për ndjekjen penale efektive të këtyre krimeve, aftësia për të ruajtur dhe tërhequr prova digjiitale është thelbësore. Sulmet kibernetike nga hakerat, të huajt dhe terroristët hetohen nga prokurori i krimit kibernetik.

[80] Bernik, Igor, "Cybercrime and Cyberwarfare", John Wiley & Sons, Inc., 2014, fq.38
[81] Cameron S. D. Brown, "Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice", *International Journal of Cyber Criminology, Vol 9 Issue 1*, Australia, K. Jaishankar, 2015, fq.64 (qasja e fundit 03.03.2021: http://www.cybercrimejournal.com/Brown2015vol9issue1.pdf)
[82] Po aty;

Sulmet kibernetike po bëhen gjithnjë e më të shpeshta, më të rrezikshme dhe më të sofistikuara, poashtu njejt me këto edhe sfidat e hetuesve të krimit kibernetik rriten[83].

3.1.2 Roli i policisë në hetimin e krimeve kibernetike

Poashtu edhe policia ka një rolë të rëndësishëm në hetimin dhe zbulimin e krimeve kibernetike. Zyrtari policor së pari duhet të vlerësojë elementet themelore të krimit dhe nëse ligjet nën juridiksionin e tyre mbështesin ndjekjen penale, sepse për shkak të shumë inovacioneve të reja në përdorim, e drejta dhe ligjet shtetërore ndoshta nuk kan arritur ti përcaktojnë ato krime[84]. Ekzistenca globale e internetit është një aspekt tjetër për t'u marrë parasysh kur hetohen krimet kibernetike, ku për të marrë më shumë njohuri për krime të veçanta kibernetike dhe për të patur suskes në hetimin dhe zbulimin e tyre është gjithashtu i dobishëm bashkëpunimi dhe koordinimi i institucioneve d.m.th bashkëpunimi i policisë me prokurorin, etj. Teknikat normale të hetimit janë poashtu të rëndësishme, gjithmonë vlejnë pyetjet kush, çfarë, ku, pse dhe si, pastaj vazhdonë kryhet hetimi fillestar, identifikimi dhe mbledhja e evidencave të mundshme, sigurohet marrja e pajisjeve dhe ndjekja e detyrave tjera me ligj, si dhe analizimi i rezultateve.

Qasjet e vendosura për të luftuar krimin në botën reale shpesh dështojnë në hapësirën kibernetike ose janë të pazbatueshme për përdorimin e paligjshëm të teknologjisë së informacionit dhe komunikimit. Krijimi i një qasjeje për të luftuar aspektet të ndryshme të krimit kibernetik shkon paralelisht me sfidat e veçanta me të cilat përballen organet hetimore dhe policia të cilat duhet të merren parasysh gjatë hartimit të strategjive për të luftuar krimin në botën virtuale të cilat janë: numri i madhë i përdoruesve të internetit, disponueshmëria e mjeteve dhe informacionit, vështirësit në gjurmimin e shkelësve, mungesa e mekanizmave të kontrollit, mungesa e kufijve në hapësirën kibernetike dhe komponenti ndërkombëtar i krimit

[83] CYBERSECURITY GUIDE, literaturë nga interneti: https://cybersecurityguide.org/careers/cyber-crime-investigator/(qasja e fundit 03.03.2021)
[84] Wall, S. D., "Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace", Police Practice & Research: An International Journal, 8(2), 2007, 183-205

në internet[85]. Të gjitha këto shqetësime vënë në pikëpytje rolin që ka policia për qëllimet në luftimin e krimit kibernetik. Jo vetëm që është vështirë të hetohen krimet në hapësirën kibernetike, por policimi i hapësirës kibernetike në përgjithësi është shpesh i vështirë, për shkak të dukshmërisë së ulët të krimeve të tilla dhe mungesës së raportimit që mund të ndodhi për një larmi arsyesh, nga subjektet tregtare, kompanitë financiare, duke refuzuar të raportojnë për shkak të shqetësmeve të reputacionit dhe reklamimit negativ, si dhe për mungesën e njohurive apo burimeve të tilla që ai krim mund të raportohet[86].

Për gjitha këto arsye është jashtëzakonisht e vështirë për njësit policore të fillojnë hetimet dhe për të patur sukses, mirëpo është e rëndësishme që të gjithë zyrtarët e policisë të kenë një kuptim të plotë të sigurisë kibernetike, ku ata do të jenë në gjendje të zgjerojnë ekspertizën e tyre në këtë fushë gjithnjë e më të rëndësishme, duke rritur sigurinë e tyre profesionale dhe personale.

3.1.3 Roli i prokurorëve në hetimin e krimeve kibernetike

Ndërkombëtarisht si prokurorët e shtetit dhe në përgjithësi gjithnjë e më shumë merren me problemet e krimit kibernetik si dhe sfidat e ndryshme që ato paraqesin. Prokurorët domosdoshmërisht marrin përgjegjësin për ndjekjen penale të krimeve kibernetike që nuk janë shumë të dëmshme, përkundrazi atyre krimeve më të rrezikshme që duhet hetuar dhe zbuluar në nivel shtetëror, ku të cilat këto krime i vlerësojnë në bazë të kritereve të ndryshme dhe niveleve të rrezikshmëris. Megjithatë në mënyrë efektive ka dhe duhet të ketë një bashkëpunim dhe marrëveshje të ndërsjellt midis prokurorëve në nivele të ndryshme që të arrihet suksesi i duhur në zbulimin e këtyre krimeve të paligjshme[87]. Roli i një prokurori mund të jetë edhe si këshillues ligjor përveç atij të hetuesit, ku shpeshherë prokurorët përfshihen personalisht në çështje që rrezikojnë procesin si dhe imunitetin e tyre. Një nga funksionet kryesore të një prokurori është të sigurojë udhëzime në lidhje me ligjin gjatë një hetimi, përveç kësaj ata

[85] Tropina, T. "Cyber-policing: the role of the police in fighting cybercrime", (Eds.) *European Police Science and Research Bulletin – Special Conference Issue Nr.2,* Germany, 2009, fq.288
[86] Po aty; fq.289
[87] Susan W. Brenner & Joseph J. Schwerha IV, "Transnational Evidence Gathering and Local Prosecution of International Cybercrime", 20J. Marshall J. Computer & Info., 2002, fq.371

veprojnë si një urë lidhëse e mungesës së informacionit të gjykatësve në lidhje me kryerjen e një krimi kibernetik, domethënë është puna e prokurorit që tua sqaroj se si është përdorur teknologjia për të kryer atë krim[88].

Me fjalë të tjera një prokuror, mbikëqyr, kryen ose ndihmon në hetimin e një krimi kibernetik, ose jep këshilla për ekzistencën e një shkaku të mundshëm të atij krimi dhe kryersit të saj dhe pastaj në zbulimin e evidencave dhe provave bën kallëzimin penal, domethënë kryen funksione të shoqëruara normalisht me një hetim policor. Përsëri, rolet e secilit lloj të hetuesit gjithmonë duhet të mbeten të përcaktuara dhe kufijtë nuk duhet të kalohen kurrë, gjithashtu secili sektor duhet të kuptojë problemet dhe sfidat e tjetrit që të shmangin konfuzionin dhe keqkuptimet.

3.2 Mjetet dhe teknikat e hetimit dhe zbulimit

Ekspertët kriminalistikë të hetimit të të dhënave kanë nevojë për një sërë mjetesh të specializuara si dhe zbatimin e teknikave shumë specifike. Hetuesit mund të përdorin një mjet ose një tjetër në varësi të llojit të sistemit kompjuterik dhe llojit të provës digjitale. Megjithëse krimi kibernetik po rritet me shpejtësi në nivele të paimagjinueshme gjatë dy dekadave të fundit, poashtu edhe forenzika kompjuterike nuk është kufizuar në këtë lloj krimi. Sepse të gjitha të dhënat apo evidencat nuk largohen kurrë nga fusha digjitale ku shumica e informacionit gjenerohet dhe konsumohet digjitalisht ku në përdorimin e mjeteve dhe teknikave efikase shkojnë deri te marrja e provave nëpërmjet çështjeve dhe metodave të ndryshme. Në fakt, shumë lloje të provave janë në dispozicion vetëm në formë digjitale, ku në hetimet kriminalistike, marrja e provave digjitale kërkon përdorimin e mjeteve të specializuara.

Edhe pse disa nga mekanizmat konvencionalë të hetimit dhe zbulimit të krimit kibernetik të prezantuara nga ekspertët e forenzikës nuk i pengon apo zvogëlon këto krime, sasia e krimeve kibernetike është duke u rritur me shpejtësi. Kjo sepse viktimat ose shënjestrat e krimit kibernetik ndryshojnë bazuar në motivin e krimit dhe kriminelët kibernetik përsosin taktikat e tyre dhe përdorin teknologji të re për të kryer krimet dhe përmbushjen e objektivave

[88] R, Anthony. & O, Kevin. & S, Jim. & H, R. Jon. & J, R. Benjamin. & R, Thomas. "Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcment, and Prosecutors", Syngress Publishing, 2007, fq.82

të tyre. Prandaj (IEEE – Institute of Electrical and Electronics Engineers)[89] instituti i inxhinierëve elektrikë dhe elektronikë në studimin e tyre për rishikimin gjithëpërfshirës të teknikave të zbulimit të krimit kibernetik ato kanë vendosur disa teknika identifikimi ku kategoritë kryesore të këtyre proceseve janë: teknika statistikore, të mësuarit makinerik, zbulimi i njohurive nga të dhënat, rrjetet nervore, teknikat e vizionit kompjuterik, teknikat biometrike, kriptografike si dhe forenzika kompjuterike apo mjetet kriminalistike apo forenzike tek të cilat do të fokusohem dhe zgjerohem më shumë në vazhdim[90].

3.2.1 Forenzika kompjuterike

Forenzika kompjuterike është degë e forenzikës digjitale dhe është e specializuar në identifikimin e provave në pajisjet kompjuterike, siç janë disqet fikse dhe lëvizëse, memorien e punës etj. Fokusi i hetimit është në marrjen e të dhënave të humbura nga disqet dhe RAM memoritë, si dhe skanimin e ngjarjeve nga aktivitetet e regjistrave, postat elektronike dhe burime të tjera, për të gjetur, ruajtur, marrë, interpretuar dhe paraqitur fakte dhe mendime në lidhje me përmbajtjen digjitale.

Forenzika ligjore kompjuterike është një disiplinë që përfshin aspekte të ligjit dhe shkencës kompjuterike për të kapur dhe interpretuar të dhëna nga aplikacionet kompjuterike, rrjetet, sistemet e rrjeteve pa tel dhe pajisjet e ruajtjes së të dhënave në një mënyrë që është e ligjshme dhe e pranueshme në një gjykatë. Ku sipas FBI-së apo byrosë federale për investigim shkenca e forenzikës kompjuterike u zhvillua për të përmbushur nevojat unike dhe të shprehura të zbatimit të ligjit në mënyrë që të lejojë përdorimin më të madh të kësaj forme të re të provave elektronike. Ato e definojnë forenzikën kompjuterike si praktikë të mbledhjes, ruajtjes, nxjerrjes dhe shfaqjes së provave që janë mbledhur në mënyrë elektronike dhe të ruajtura në mediat kompjuterike[91].

[89] W. A. Al-Khater, S. Al-Maadeed, A. A. Ahmed, A. S. Sadiq and M. K. Khan, "Comprehensive Review of Cybercrime Detection Techniques," in IEEE Access, vol. 8, 2020
[90] Po aty;
[91] Definimi i forenzikës kompjuterike nga FBI - https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/oct2000/computer.htm (qasja e fundit 21.03.2021)

Forenzika kërkon analizën e të gjitha mediave të ruajtjes së të dhënave në mënyrë që të identifikojë dhe ekzaminojë dokumentet ose informacione të tjera të rëndësishme për çdo operacion kriminal. Meqenëse përveç kompjuterëve, gjithnjë e më shumë teknologji digjitale, të tilla si kamera digjitale, telefona celularë dhe telefonat inteligjentë janë në dispozicion, parimi i forenzikës kompjuterike është evoluar në forenzikën digjitale.

Përfshihen metoda dhe standarde të marrjes së të dhënave, por ka protokolle dhe procedura shtesë për të vendosur një gjurmë ligjore në ekzaminim apo shqyrtim. Provat e forenzikës kompjuterike zakonisht mbahen në të njëjtat standarde dhe procedura si shumica e provave vizuale. Forenzika kompjuterike apo digjitale përdoret në një sërë gjykimesh të profilit të lartë dhe po fiton shpejt pranimin si një mjet i besueshëm si në sistemin ligjor të SH.B.A.-së dhe Evropës.

3.2.2 Modelet hetuese të forenzikës kompjuterike

Aktivitetet e paligjshme si kryerja e krimeve kompjuterike-kibernetike janë në rritje të cilat përdorin përmbajtjen digjitale si medium dhe kërkohet një qasje sistematike për tu marrë me to. Që nga prezantimi i një modeli të zyrtarizuar në vitin 1984 e deri më sotë, janë zhvilluar një numër i madh i metodave moderne të hetimit forenzik kompjuterik ku nga të gjitha këto procese është identifikuar një model i përgjithshëm i cili quhet **Modeli (GCFIM)** – Generic Computer Forensic Investigation Model apo Modeli Gjenerik i Hetimit Kriminalistik Kompjuterik.

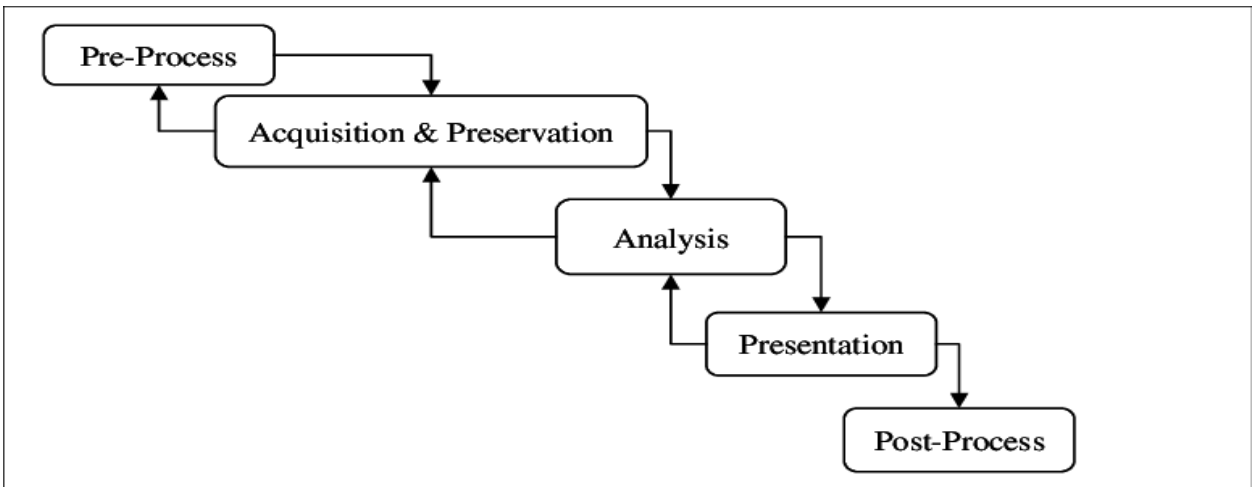


Fig 1: Modeli Gjenerik i Hetimit Kriminalistik Kompjuterik

Në bazë të autorëve Yunus Yusoff dhe Rosian Ismail në punimin e tyre "Common Phases of Computer Forensics Investigation Models"[92], ky model përbëhet nga disa faza të cilat janë:

Para-procesi: Aktivitetet e kryera gjatë këtij procesi kanë të bëjnë me të gjitha detyrat që duhet të kryhen para hetimit përfundimtar dhe mbledhjes zyrtare të të dhënave. Marrja e lejes së duhur nga autoriteti përkatës, si dhe planifikimi dhe vendosja e pajisjeve që do të përdoren, etj.
Përvetësimi & Ruajtja: Identifikimi, mbledhja, transportimi, mirëmbajtja dhe ruajtja e të dhënave janë të gjitha detyrat që duhet të kryhen gjatë këtij procesi. Në përgjithësi gjatë kësaj faze të gjitha të dhënat e zbatueshme mblidhen, ruhen dhe vihen në dispozicion për procesin tjetër.
Analiza: Këtu fillojnë dhe mbarojnë procedurat elektronike të analizës kriminalistike, ka më shumë faza në grupin e saj, duke sugjeruar që shumica e modeleve të analizuara bazohen në procesin e hulumtimit. Forma të ndryshme të hetimit kryhet në provat e mbledhura në mënyrë që të përcaktohet shkaku i krimit dhe i dyshuari.

Prezentimi: Rezultatet e fazës së hulumtimit raportohen dhe i paraqiten autoriteteve. Ky proces është kritik pasi që çështja jo vetëm që duhet të formulohet në një mënyrë që kapet lehtë nga grupi në të cilin paraqitet, por gjithashtu duhet të mbështetet nga prova të mjaftueshme dhe të përshtatshme. Performanca kryesore e kësaj faze është ose dëshmia ose refuzimi i veprimeve të dyshuara e të paligjshme.

Post-Procesi: Ky proces ka të bëjë me përfundimin e duhur të hetimit. Kur kërkohet dokumentacioni digjital dhe i prekshëm duhet ti kthehet pronarit të ligjshëm dhe të ruhet në një vend të sigurt. Duhet të bëhet një analizë e procesit penal në mënyrë që të përfitojmë nga përvoja dhe të rriten hetimet në të ardhmen.

[92] Yusoff, Y., Ismail, R., & Hassan, Z. "Common phases of computer forensics investigation models", International Journal of Computer Science & Information Technology, 2011, 3(3), 17-31.

3.2.3 Mjetet e nevojshme të forenzikës kompjuterike

Aplikimi i forenzikës kompjuterike përdoret në çdo situatë kur është e qartë se ka informacion në lidhje me çështjen në ndonjë kompjuter dhe se provat nuk mund të merren diku tjetër pa përdorimin e teknikave të forenzikës kompjuterike të aplikuara nga specialistët në këtë fushë[93]. Kjo ka për qëllim të ruajë faktet dhe të zvogëlojë rrezikun e përfshirjes apo përdorimit të tyre në pcoedurë ligjore. Forenzika kompjuterike jo vetëm që mund të ketë punën e ekspozimit të të dhënave ose të fshehura apo të fshira, por aftësia e ekspertit për të punuar me këtë formë të ekspertizës gjithashtu mund të përqendrohet në vlerësimin e nivelit dhe vlerës së këtyre provave dhe interpretimin profesional të gjetjeve që ai ka arritur dhe mbrojtja e tyre me argumente para gjykatës. Hetuesit mund të përdorin softuer dhe metoda elektronike të forenzikës për të marrë informacione në lidhje me përdoruesit e kompjuterit, për të rikuperuar dokumentet që mungojnë, për të rivendosur objektet dhe për të provuar të mbledhin sa më shumë prova të jetë e mundur[94]. Për të qenë të pranueshme në gjykatë, rezultat e përdorimit të ndonjë prej këtyre teknikave duhet të trajtohen nga ekspertët e trajnuar të forenzikës së të dhënave kompjuterike. Një teknikë kriminalistike forenzike ofron gjetje që janë të dobishme, të përsëritshme dhe të verifikueshme. Mjetet e forenzikës harduerike dhe softuerike përbëjnë dy kategori kryesore të këtyre mjeteve.

Fig 2:Mjet Mobil i Forenzikës Kompjuterike

[93] Vula, Veton, "Kriminaliteti Kompjuterik" Prishtinë, 2010, fq.58
[94] Po aty;

3.2.3.1 Mjetet harduerike të forenzikës kompjuterike

Përfitimet dhe aftësitë e këtyre mjeteve qëndrojnë në teknika që zëvendësojnë softuerin për procedurat dhe përdorimin e mjeteve të vogla dhe janë të lehta për tu përdorur. Mjetet e veçanta të harduerit të cilat përmbajnë ndonjë veçori përtej standardeve, të tilla si kabllot e avancuara, bllokuesit e shkrimit, arkivuesit e provave si dhe shumë mjete tjera që mundsojnë funksionimin e mjeteve softuerike, janë gjithashtu më të thjeshta dhe më të sigurta gjatë hetimeve teknike[95]. Sistemet e ruajtjes së të dhënave me kapacitet të lartë janë një pjesë tjetër e rëndësishme e pajisjeve të tilla si: disqet magnetike, hard disqet, flash disqet, usb etj.

Këto mjete harduerike kanë edhe disa avantazhe të cilat janë: përfshijnë rritjen e përfunduar të hetimeve, të cilat kursejnë hapësirë dhe kohë ndërsa thjeshton ende procesin e gjetjes, ka transportueshmërin e rritur të të dhënave, përvetësimin më të shpejtë të të dhënave digjitale duke përdorur mjetet harduerike në krahasim me ato softuerike[96].

Për të kryer hetime dhe studime, duhet një stacion pune i forenzikës kompjuterike, i cili është një kompjuter apo mjet tjetër i konfiguruar posaçërisht për atë punë, dmth mjet që është i pajisur me hapësira shtesë, porte, softuer dhe mjete harduerike forenzike. Stacionet e punës më pak efikase përdoren për operacione rutinë, ndërsa stacionet e punës më të mëdha me shumë qëllime përdoren për analiza intensive.

Ekzistojnë tre lloje të ndryshme të stacioneve të forenzikës kompjuterike, varësisht nga vendi i kryerjes së hetimeve mund të jenë:

- Një platformë me shumë hyrje dhe disa lloje të pajisjeve ndihmëse të cilat referohen si një stacion pune i palëvizshëm; (pajisje e kompletuar e tavolinës, kompjuter desktop);

[95] Philip, A. & Cowen, D. & Davis, C., "Hacking Exposed Computer Forensics, Second Edition: Computer Forensics Secrets & Solutions", McGraw Hill Professional, 2009, fq.53-54

[96] GlobalSpec – Forensic Hardware Tools, Marrë nga: https://www.globalspec.com/reference/31783/203279/part-2-forensic-hardware-tools (qasja e fundit 22.03.2021)

- Stacion pune i lëvizshëm – mjete mobile si p.sh një laptop me pjesë shtes për teren me pothuajse të njëjtin numër portesh dhe pajisjesh periferike si stacionet e punës të palëvizshme;
- Stacion pune i lehtë – kompjuter desktop me një grup të personalizuar të pajisjeve periferike, ku ky stacion përmban edhe mjete të ndryshme si: qeset e provave, bateritë e dorës, kabllot, kaçavidat, kamerat, darët, dorëzat si dhe formular për ecurinë e ruajtjes së provave, etj[97].

3.2.3.2 Mjetet softuerike të forenzikës kompjuterike

Llojet e mjeteve softuerike të përdorura në forenzikën kompjuterike përcaktohen normalisht nga lloji i hetimit. Nëse kërkimi është për rikuperimin e të dhënave, përdoren mjetet e riparimit të të dhënave, secili mjet softuerik ka zgjidhjen, funksionin dhe performancën e vet. Mjetet e riparimit të të dhënave, veglat e ndarjes, veglat e klonimit të diskut, mjetet tjera të riparimit, mjetet e testimit, testi i shpejtësisë së sistemit, mjetet e diskut të rrjetit, mjetet e informacionit të sistemit dhe të tjera janë të gjitha shembuj të mjeteve softuerike të forenzikës kompjuterike[98].

Për të klasifikuar dhe marrë prova kompjuterike, ekzaminuesit e kompjuterëve përdorin një larmi teknikash. Puna kriminalistike forenzike mund të kryhet duke përdorur një larmi metodash dhe mjetesh softuerike, ka disa lloje të mjeteve softuerike të forenzikës kompjuterike nga të cilat disa janë softuer komercial ndërsa të tjerët pa pagesë apo falas të cilët janë[99]:

- EnCase;
- Paraben's P2 Examination Process;
- Forensic Toolkit (FTK);

[97] Paranjpe, P. *Computer Forensic Workstation*, Marrë nga: http://prateek-paranjpe.blogspot.com/p/computer-forensics.html (qasja e fundit 12.04.2021)
[98] Hasan, R., & Raghav, A., & Mahmood, S., "Overview on Computer Forensics Tools", UKACC International Conference on Control, Cardiff, 2012, fq.402
[99] Computer (Digital) Forensic Software Tools, Marrë nga: https://www.guru99.com/computer-forensics-tools.html (qasja e fundit 13.04.2021)

- ProDiscover;
- Autopsy;
- Digital Forensics Framework (DFF) etj.

EnCase – është mbikëqyrja, siguria kibernetike, analitika e sigurisë dhe produkti i zbulimit elektronik që është pjesë e një pakete mjetesh të automatizuara hetimesh. EnCase përdoret për të marrë të dhëna nga disqet kompjuterike të sekuestruara, poashtu i mundëson hetuesit apo prokurorit të mbledhë të dhëna të tilla si shënime, imazhe, histori interneti dhe informacione të regjistrave në sisteme të ndryshme operative duke bërë një rishikim të thellë të dokumentave të përdoruesit.

Forensic Toolkit (FTK) – Pakoja e mjeteve forenzike është një softuer apo program kompjuterik i forenzikës i cili skanon hard diskun e kompjuterik që hetohet për të gjetur pjesë të ndryshme të materialit që kërkohet, për shembull, mund të gjejë email që mungojnë, të gjejë vargje tekstesh të fshira për tu përdorur në fjalkalimet e thyera etj. FTK u mundëson ekspertëve të forenzikës të kenë qasje të shpejt në të gjitha dokumentet e nevojshme të cilat hetohen dhe të cilat i gjenerojnn ato menjëherë brenda një kërkese.

Digital Forensics Framework (DFF) – Korniza digjitale forenzike është softuer elektronik me burim të hapur ku profesionistët dhe jo-ekspertët e përdorin atë për të mbledhur, ruajtur dhe zbuluar informacione digjitale pa rrezikuar proceset ose shënimet e hetimit.

Përdorimi i mjeteve më të njohura të forenzikës kompjuterike është një pjesë e madhe e suksesit të hetuesve specialist në këtë fushë. Në mënyrë tipike, këto programe janë të paketuara si mjete komplet në një vend me një larmi të gjerë karakteristikash për përfundimin e projekteve nga fillimi në fund. Këto karakteristika përfshijnë aftësinë për nxjerrjen dhe procedimin e të dhënave, kryerjen e kërkimeve, gjenerimin e raporteve etj.

3.2.4 Provat kompjuterike dhe karakteristikat e tyre

Provat kompjuterike janë çdo material provues i mbledhur ose shpërndarë në forma të ndryshme në kompjuter ose në internet që një palë në një çështje gjyqësore mund ti përdorë si

fakte dhe informacione gjatë gjykimit, ku të cilat mund të jenë si prova fizike apo prova digjitale-elektronike.

Provat fizike kanë formën e sendeve të prekshme, të tilla si letra, fotografi, objekte dhe gjurmë të tjera të identifikueshme fizikisht, të cilat mund të gjenden shpejt dhe të mblidhen si prova[100]. Provat digjitale-elektronike, ndryshojn pak nga provat e zakonshme për sa i përket vlefshmërisë provuese, përfshirë faktin që ato nuk janë lehtë të disponueshme. Ato shpesh gjenden në vendet ku vetëm ata me trajnim të specializuar mund ti gjejnë dhe ti mbledhin apo mbrojnë ato, duke u dhënë atyre vlerë ligjore para gjykatave. Një nga avantazhet e të dhënave digjitale është potenciali për ti pasur ato në një numër të pafund kopjesh, secila prej të cilave është origjinale[101].

Përfaqësimi digjital nënkupton që kjo është një njësi elektronike ose magnetike me të dhëna të ruajtura në memorje, disk të ngurtë, kartë flash ose mjete tjera ruajtëse. Në këtë drejtim është e rëndësishme të njihen karakteristikat dhe tiparet e provave digjitale që të kuptohen më mirë ato. Karakteristikat janë:

- Numri potencialisht i madh i inkriminimeve
- Identifikimi i ndërhyrjeve
- Numri potencialisht i madh i provave
- Nënshtrimi kontaminimit
- Lehtësia e humbjes së provave[102].

Sipas mendimit tim, provat kompjuterike në bazë të karakteristikave të lartëpërmendura e bëjnë kujdesin ndaj tyre më kompleks, gjë që kërkon ekspertizë teknike dhe kualifikimet e duhura për të trajtuar klasifikimin dhe ruajtjen e tyre. Kur bëhet fjala për ndërhyrje në regjistrat elektronikë, duhet të merret parasysh se të dhënat dhe faktet e kompjuterit janë gjithashtu shumë të ndjeshme të cilat mund të prishen dhe dëmtohen me

[100] Doracak për krimin kompjuterik: https://www.osce.org/sq/skopje/121225 (qasja e fundit më 16.04.2021)
[101] Po aty;
[102] Mohay, G. & Anderson, A. & Collie, B. & D. Mckemmish. R. "Computer and Intrusion forensics", Attrech, Boston, 2003, fq.44

lehtësi dhe ndikon tek ato faktori kohë. Ato mund të shqyrtohen dhe analizohen vetëm nga profesionistë të trajnuar posaçërisht në atë drejtim për të patur rezultate më të suksesshme.

3.3 Hetimi i krimeve dhe sulmeve në internet

Çdo vepër ose veprim kriminal i kryer në internet ose duke përdorur internetin referohet si krim në internet. Krimi në internet është një vepër penale që është zhvilluar ose është bërë e mundur me shpikjen e teknologjisë ose një krim konvencional që është ndryshuar nga përdorimi i teknologjisë. Fjala "krim kibernetik" shpesh përdoret për t'iu referuar një game të gjerë krimesh në internet përfshirë ndërhyrjet në rrjet, hakingun si dhe të tjera[103].

Për të përcaktuar autorët e sulmit në kompjuter dhe motivet e tyre të vërteta, një hetim i krimit kibernetik është një metodë e hetimit, rishikimit dhe marrjes së provave digjitale nga rrjetet e përfshira në sulm, të kryera në internet ose rrjet lokal. Ekspertët e krimit kompjuterik duhet të jenë profesionistë të shkencave kompjuterike ti njohin të gjitha aspektet, duhet të

jenë mjaftë inteligjent për të kuptuar se si funksionojnë këto elemente që të marrin një kuptim të plotë të asaj se çka ka ndodhur, pse ka ndodhur dhe kush e ka kryer krimin kibernetik[104].

Në internet, ekzekutuesi ose kryersi kryen veprime të paligjshme në dëm të viktimave të ndryshme që mund të jenë individë, persona fizik apo juridik në një numër formash, disa nga format e ndryshme më të shpeshta të krimeve në internet janë: phishing (peshkimi), vjedhja e identitetit, mashtrimi me karta kreditit, shkarkimi i paligjshëm, pornografia e fëmijëve, kiber terrorizmi, krijimi dhe distribuimi i viruseve dhe të tjera, të cilat janë shtjelluar më gjerësisht në kapitullinë e parë të këtij punimi.

3.3.1 Hapat dhe qëllimet e hetimit të krimeve në internet

Masat apo hapat e marra në hetimin dhe zbulimin e krimeve në internet në bazë Këshillit ndërkombëtar të konsultentëve të tregtisë elektronike apo EC-Council[105] janë si vijojnë:

[103] Shipley, T.G., Bowker, A., "Investigating Internet Crimes: An Introduction to Solving Crimes in Cybersoace", Newnes, 2013, fq.2
[104] Borges, E. *Cyber Crime Investigation Tools and Techniques Explained,* Marrë nga: https://securitytrails.com/blog/cyber-crime-investigation# (qasja e fundit 23.04.2021)

- ***Marrja e urdhërit për kërkim, për të marrë sendet personale të viktimës*** - në kërkesën për urdhër kërkim duhet të thuhet qartë se policia do të ekzaminojë kompjuterin dhe pajisjet e rrjetit në vend, kompjuterët që janë përdorur në këtë rast sekuestrohen, ku së bashku me ato edhe pajisjet e përdorur nga viktima, ruterin, kamerë, si dhe pajisje tjera;
- ***Intervist me viktimën*** - viktima duhet të intervistohet nga hetuesi në lidhje me incidentin, ku i parashtrohen disa pyetje të cilat janë: çfarë incidenti ka ndodhur, si u fut hakeri në rrjet, cili ishte qëllimi i sulmit, cilat janë humbjet nga ky incident;
- ***Kopjimi i të dhënave në formë binare*** - duke përdorur një mjet forenzik, hetuesit duhet të krijojnë kopje rezervë të rrjedhës të të dhënave binare të pajisjeve të prekura;
- ***Përcaktimi apo njohja e konfigurimit të kryerësit*** - përfshinë kontrollimin e çdo regjistri, të dhënat e pajisjes, postën elektronike dhe regjistrat të serverit në Web;
- ***Marrja e provave***;
- ***Kontrollimi i fakteve, provave dhe marrja e një vendimi bazuar në to***;
- ***Krijimi i raportit***.

Kriminalistika apo forenzika e internetit është përdorimi i mjeteve shkencore dhe të ligjshme për të hetuar krimet e internetit, me një theks në gjithçka, nga një pajisje e vetme në të gjithë internetit. Ekspertët në këtë drejtim përdorin një përzierje të metodave të sofistikuara llogaritëse dhe të inteligjencës njerëzore për të zbuluar të dhëna rreth individëve dhe pajisjeve të përfshira në krimin kibernetik[106]. Forenzika kompjuterike ka të bëjë me sende të prekshme, ndërsa kriminalistika apo forenzika në internet ka të bëjë me shkaqe të efektshme dhe të përkohshme, ku sipas EC-Council[107], qëllimet e hetimit të krimeve në internet janë:

- ❖ Sigurimi që të gjitha regjistrat dhe provat përkatëse janë ruajtur;
- ❖ Të kuptoj se si sulmuesi u fut në pajisjen kompjuterike;
- ❖ Për të kuptuar pse sulmuesi zgjodhi kompjuterin si një objektiv;
- ❖ Mbledhja e sa më shumë informacioneve për ndërhyrjen;

[105] EC-Council, "Computer Forensics: Investigating Network Intrusions and Cyber Crime", Cengage Learning, 2009, kapitulli 6, fq 6-4
[106] Po aty;
[107] Po aty;

- ❖ Të mblidhen prova që mund të ndihmojnë në ngushtimin e listës së të dyshuarve;
- ❖ Të sigurohen gjurmët e dëmtimit të ndërhyrjes;
- ❖ Mbledhja e sa më shumë provave për të përcaktuar nëse organe më të rëndësishme mund të përfshihen.

Poashtu, subjektet dhe organizatat private, përfshirë autoritetet e zbatimit të ligjit, kryejnë hetime në përgjigje të një krimi kibernetik të zbuluar ose të konfirmuar. Qëllimi kryesor është që të hetohet dhe zbulohet sa më shumë rreth incidentit dhe të paraqesin një kallëzim penal, një çështje kundër të dyshuarve për krim në internet dhe të arrihen rezultate sa më të suksesshme.

3.3.2 Sigurimi dhe vlerësimi i vendit nga ku është kryer krimi kibernetik

Mbrojtja dhe sigurimi i vendit është ndoshta një nga çështjet më të rëndësishme dhe ndonjëher e nënvlerësuar, në ndjekjen penale të suksesshme të të dyshuarve. Në ndryshim nga skenat tipike të krimit, të cilat shpesh zbulohen dhe ruhen nga policia, shumica e skenave të krimit në lidhje me kompjuterin kanë një përgatitje më të përparuar. Si rezultat, procedurat e sigurimit në vendin e ngjarjes shpesh përshtaten me karakteristikat specifike të çështjes dhe vendosen para mbërritjes. Hetuesit gjithashtu mund të vlerësojnë llojin e tyre të provës së bazuar në karakteristikat e çështjes. Si rezultat, është e rëndësishme ti kushtohet vëmendje kësaj faze të hetimit[108].

Të paktën, veprime të shumta duhet të ndodhin njëkohësisht pas mbërritjes në vendin e ngjarjes për të pasur rezultate të suksesshme. Specifikat e çështjes vendosin protokollet e duhura dhe identifikojnë çështjet e mundshme. Kështu që sipas autores Marije T. Britz, aktivitetet minimale që duhet të kryhen janë[109]:

1) Personat e rrezikshëm ose kërcënimet e sigurisë duhet të identifikohen dhe menaxhohen sa më shpejt që të jetë e mundur;

[108] Britz, T. Marije, "Computer Forensics and Cyber Crime an Introduction", Pearson, 2013, fq.315
[109] Po aty;

2) Çdo pajisje kompjuterike duhet të sigurohet;
3) I gjithë personeli duhet të tërhiqet nga afërsia e provave;
4) Është thelbësore të verifikohen lidhjet e rrjetit dhe të merren masat e përshtatshme, si p.sh të bllokohen lidhjet e rrjetit menjëher, duke ndaluar shkatërrimin e provave nga distanca;
5) Të gjithë kriminelët kibernetik duhet të izolohen dhe të merren në një vend të caktuar sa më shpejt të jetë e mundur.
6) Një polic duhet të caktohet që të ruaj të gjitha pajisjet, kjo është e nevojshme për tu siguruar që mos ndërhyhet në asnjë mënyrë, qoftë në distancë ose në mënyrë tjetër.

3.3.3 Dokumentimi dhe mbledhja e provave në internet

Shumë njerëz nuk janë të vetëdijshëm se përgjimi i një rrjeti është i lehtë dhe se serverat në internet ruajnë një sasi të madhe të të dhënave për aktivitetet e njerëzve. Ndonjë nga këto informacione është kalimtarë, zgjat vetëm disa sekonda, minuta ose ditë në kompjuter, ndërsa llojet tjera të të dhënave digjitale mund të rikuperohen vite më vonë. Këto të dhëna digjitale mund të zbulojnë detaje rreth mendimeve dhe dëshirave private të një personi, modelet e aktivitetit dhe vendndodhjen në një kohë të caktuar, të gjitha këto mund të jenë shumë të dobishme në një hetim[110].

Dokumentimi dhe mbledhja e provave në internet është një detyrim ligjor. Karakteristika themelore e mbledhjes së provave në internet është grumbullimi i tyre, i cili përfshin kapjen e të dhënave përkatëse si dhe nëse është e mundur edhe meta të dhënat që qëndrojnë në themel të këtyre të dhënave. Procedura fillon me identifikimin e të dhënave që mblidhen si dhe protokollin, teknikën e mbledhjes dhe vendodhjen. Ekzistojnë dy lloje të proceseve të mbledhje së provave në internet: ato prova të mbledhura nga pajisjet

[110] Casey, E. "Digital Evidence and Computer Crime, Forensic Science, Computers and the Internet", 2nd Edition, Academic Press, 2004, fq.477

kompjuterike nga zyra e hetuesit dhe ato prova të mbledhura në terren në kompjuterin e viktimës ose dëshmitarit[111].

Përpilimi, grumbullimi dhe ruajtja në internet e të dhënave elektronike shpesh kërkon paramendim nga ana e hetuesve për sa i përket procedurës, funksionimit dhe vërtetësisë së të dhënave. Poashtu kërkohet një bashkëpunim më i gjerë hulumtues me organe të zbatimit të ligjit, agjenci dhe kompani të ndryshme, me këshillues teknik dhe ligjor etj.

3.4 Parandalimi dhe luftimi i kriminalitetit kompjuterik

Krimi kompjuterik po bëhet me shpejtësi të madhe një sfidë e vërtetë shoqërore, si dhe një shqetësim i madh për qeverit kombëtare dhe të huaja në epokën moderne, për shkak të karakteristikave të tij unike, rrezikut të lartë shoqëror dhe ritmit të shpejt të rritjes. Juridiksionet në të gjithë botën janë detyruar të shqyrtojnë dhe ndryshojnë procedurat e tyre ligjore vitet e fundit në mënyrë që të përballen me kërcënimet dhe sfidat në rritje të krimit kibernetik[112]. Duke pasur parasysh sfidat e shmangies, identifikimit, sqarimit dhe hetimit të krimeve kibernetike, ekzistojnë tre lloje të sistemeve që mund të reagojnë në mënyrë efektive ndaj këtyre provokimeve në betejën kundër këtij fenomeni: teknologjia mbrojtëse, etika dhe rregullat. Këto sisteme mbrojtëse janë parandaluese dhe shtrënguese. E para dhe më e rëndësishmja, hapat e parandalimit duhet të kenë përparësi mbi masat ndëshkuese në zbatimin e tyre[113]. Për këta dhe faktorë të tjerë, nevoja për masa të përshtatshme për të dekurajuar dhe trajtuar në mënyrë efektive këtë krim në kulturën moderne është e pamohueshme.

3.4.1 Sfidat e luftimit të krimit kompjuterik

Ekzistenca transacionale dhe për këtë arsye shumë juridiksionale e krimit kibernetik, si dhe vështirësitë në parandalimin e këtyre sulmeve, sistemet e papërshtatshme, rregullatoret dhe mjedisi teknologjik që ndryshon gjithnjë, të gjitha paraqesin sfida për hetimin dhe ndjekjen

[111] Shipley, T.G., & Bowker, A., "Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace", Newnes, 2013, fq.100
[112] Petrovic, S., "Kompjuterski Kriminal", Beograd, 2000, fq.355
[113] Denning, E.D., "Crime and Crypto on the Information Superhighway", Georgetown University, 1994, Marrë nga: https://faculty.nps.edu/dedennin/publications/Crime-and-Crypto-on-Information-Superhighway.txt

penale të krimit kibernetik. Policia dhe hetuesit përballen me shumë sfida të përgjithshme në betejën kundër këtij krimi, ku të cilat më të zakonshmet janë këto të deklaruara[114]:

- Rritja e aksesit në hyrjen apo përdorimin e shpejtë të internetit;
- Disponueshmëria në rritje e mjeteve harduerike dhe softuerike;
- Rritja e lehtësisë së fillimit të sulmeve të automatizuara në internet;
- Zhvillimi i shpejtë i teknikave të reja të krimit kibernetik;
- Natyra e shpejtë e sulmeve kibernetike;
- Brishtësia dhe natyra e përkohëshme e të dhënave elektronike;
- Mungesa e kapacitetit hetimor kushtuar hapësirës kibernetike;
- Rritja e shpejtë e numrit të përdoruesve vështirëson proceset e hetimit;
- Natyra anonime e komunikimeve në internet.

Pandemia e përhapur e krimit kibernetik ka rezultuar në disa shtresa të rregullimit dhe mbikëqyrjes globale. Ekspertët e sigurisë janë të përkushtuar për të luftuar krimin në internet me teknologji parandaluese siç janë rrjetet e zbulimit të ndërhyrjeve dhe sektoret e ndryshme sfiduese në zhvillim e teknologjisë.

Mbrojtja e infrastrukturës dhe rrjeteve operative nga kërcënimet është hapi i parë në luftimin e krimit kibernetik. Ndërsa asnjë pajisje nuk mund të jetë plotësisht e sigurt, qëllimi i mbrojtjes është të sigurojë një barrierë mjaft të fortë për të parandaluar shumicën, nëse jo të gjithë sulmuesit. Për çdo formë të pajisjes, përbërësit ose problemet që duhet të zgjidhen për të ndërtuar një mjedis të qëndrueshëm janë zakonisht të njëjtat. Sidoqoftë, detajet se si të zbatohet një strategji sigurie dhe të bëhen përmisime individuale të sgurisë, ndryshojnë nga mjedisi i funksionimit dhe teknologjive të ndryshme[115]. Me rritjen e përdorimit të rrjeteve pa tela (wi-fis) me shpejtësi të lartë e me kosto të ulët, më shumë pajisje shtëpiake dhe biznese janë të prekshme ndaj kërcënimeve afatgjate të internetit si kurrë më parë. Softueret apo programet kundër viruseve, vendosja e fjalëkalimeve të sigurta, bllokimi i ndarjes së

[114] World Bank, United Nations. "Combatting Cybercrime: Tools and Capacity Building for Emerging Economies", Washington, DC. 2017, fq.28

[115] Shinder, D. & Tittel, E. (Eds.), "Scene of the Cybercrime: Computer Forenscis Handbook" Syngress, Elsevier Science, 2002, fq.493

dokumenteve dhe përdorimi i pajisjeve për tu mbrojtur nga qasja e paautorizuar nëpër sisteme kompjuterike janë vetëm disa nga masat e sigurisë që duhet të merren për tu mbrojtur këto lidhje tërë kohën nga sulmet në internet[116].

3.4.1 Korniza juridike ndërkombëtare kundër krimit kompjuterik (Konventa e Budapestit)

Natyra globale e krimit në internet kërkon bashkëpunim ndërkombëtar në ndalimin dhe zbutjen e krimit, që përfshin organizimin e përpjekjeve nga të gjitha vendet dhe vendosjen e normave ndërkombëtare në fushën e sigurisë së pajisjeve kompjuterike. Në fushën e kibernetikës, bashkëpunimi i suksesshëm do të ndikojë në identifikimin dhe shmangien e veprave penale [117].

Është e rëndësishme të dihet se nuk ka siguri totale dhe se çdo sistem informacioni i nënshtrohet rreziqeve aktuale, por shkalla e rrezikkut aktual duhet të mbahet brenda kufijve të arsyeshëm. Për ti bërë të gjitha këto, duhet të kihen parasysh planet sistematike, pa të cilat është e vështirë të përfshihen zgjidhje efikase, të orientuara drejt rezultateve. Zbatimi i politikave më të suksesshme të rekomanduara në praktikë do të shërbejnë si masa mbrojtëse duke ngritur gjithashtu vetëdijen tek njerëzit e të gjitha moshave për të drejtën e përdorimit të pakufizuar të sistemeve kompjuterike dhe të gjitha të drejtat që lidhen me këto sisteme[118].

Shtetet anëtare të Këshillit të Evropës dhe shtetet tjera nënshkruese besojnë se qëllimi është arritja e unitetit midis anëtarëve të tij, duke njohur vlerën e nxitjes së bashkëpunimit me shtetet e tjera përmes nënshkrimit të Konventës së Budapestit apo Konventës së Krimit Kibernetik në mënyrë që të vendoset rregullorja për parandalimin dhe luftimin e krimit kibernetik, për respektimin e të drejtave të njeriut dhe mbrojtjen e të dhënave të tyre personale.

Meqenëse sistemet e informacionit dhe komunikimit përdoren nga komunitetet në të gjithë botën, prokurorët dhe gjykatësi në çdo shtet që ka rafitifkuar Konventën e Krimit

[116] Po aty;
[117] Gercke, M., "National, Regional and International Legal Approaches in the Fight Against Cybercrime", in Journal ofInformation Law and Technology, 2008, Issue 1, fq.7-14
[118] C. Carr (Ed)., "The Book of War", New York: Random House, fq.18-24

Kibernetik duhet të jenë të përgatitur për tu marrë me krimin kibernetik dhe provat elektronike.

Si rezultat, nevojiten masa të veçanta për të përshtatur prokurorët për të hetuar dhe ndjekur penalisht krimin kibernetik dhe përdorimin e provave elektronike përmes përgatitjes dhe krijimit të rrjeteve të specializimit, gjë që do të kërkonte një bashkëpunim më të madh ndërkombëtar.

Sipas mendimit tim kjo ide u shpik për të ndihmuar në këto përpjekje, ku një nga qëllimet e këtij koncepti është të ndihmojë agjensitë e trajnimit të gjyqësorit të vendosin sisteme të trajnimit për luftimin e krimit kibernetik dhe të dhënave elektronike digjitale, që të munden të integrohen në arsimin normal fillestar dhe të vazhdueshëm. Për më tepër, ky parim do të inkurajonte krijimin e rrjeteve për të forcuar vetëdijen e tyre dhe për të siguruar që anëtarët të vazhdojnë të financojnë inciativa trajnimi, për arritje të rezultateve sa më të suksesshme në luftimin dhe parandalimin e kësaj sfide në botën bashkëkohore.

KAPITULLI I KATËRT

4. STUDIM EMPIRIK

4.1 Analiza dhe prezantimi i të dhënave statistikore nga Enti shtetëror statistikor i RMV-së bazuar në kërkime empirike lidhur me veprat penale të krimeve kompjuterike

Enti shtetëror i statistikave është një organ i specializuar dhe autonom që punon brenda administratës shtetërore të RMV-së. Përgjegjësitë kryesore të institucionit përfshijnë mbledhjen, përpilimin dhe shpërndarjen e të dhënave statistikore dhe shkencore mbi trendet demografike, sociale dhe ekonomike, si dhe mbi sektorë të ndryshëm. Të dhënat statistikore janë kritike për procesin e vendimmarrjes së një shoqërie.

Në lidhje me këtë hulumtim shkencor për të fituar rezultate më të besueshme, janë marrë të dhëna nga Enti shtetëror i statistikave, të cilat zbulojn numrin e krimeve të krimit kompjuterik të ndjekur penalisht si dhe në të njëjtën kohë paraqiten edhe dënimet që janë vendosur për këto vepra penale në periudhën kohore nga viti 2012 në 2017-ën.

Tabela e 1-rë, paraqet statistika apo të dhëna për disa nga llojet e veprave penale të krimit kompjuterik të kryera në RMV, të cilat ishin më të përhapura dhe për të cilat kishte më shumë krime të kryera për periudhën e caktuar kohore, ku janë të paraqitura në bazë të neneve të kodit penal të cilat janë: dëmtimi dhe hyrja e paautorizuar në sistemin kompjuterik, përpunimi dhe përdorimi i kartelës së rrejshme pagesore, shkelja e të drejtës së autorit dhe të drejtat e lidhura me to si dhe pirateria e veprës audio-vizuale, poashtu edhe llojet e dënimeve apo sanksioneve të shqiptuara për këto vepra dhe se sa kryerës janë dënuar.

Mundemi të konkludojmë se nga veprat penale në fjalë, si vepër penale më e kryer dhe më e përhapur në të gjitha vitet është dëmtimi dhe hyrja e paautorizuar në sistemin kompjuterik në krahasim me veprat tjera të cilat kanë numër më të ulët të kryerësve. Një rezultat tjetër është se në vitin 2015 janë sanksionuar më shumë kryerës, 55 në tërësi. Bazuar në këtë hulumtim, mund të konkludojmë se forma më e zakonshme e sanksionit në vitet në fjalë është dënimi me kusht, ku janë shqiptuar 83 dënime, ku prej të cilave janë shqiptuar në gjithsej 69 raste të dënimeve me burg, kurse në dënim me të holla 41 raste.

Llojet e krimeve kompjuterike	2012		2013		2014		2015		2016		2017	
	Llojet e dënimeve	Të dënuar	Llojet e dënimeve	Të dënuar	Llojet e dënimeve	Të dënuar	Llojet e dënimeve	Të dënuar	Llojet e dënimeve	Të dënuar	Llojet e dënimeve	Të dënuar
Neni 251 Dëmtimi dhe hyrja e paautorizuar në sistemin kompjuterik	**15 dënime me burgim, 6 dënime me të holla**	21	**7 dënime me burgim, 1 dënim me të holla, 18 dënime me kusht, 1 vërejtje gjyqësore**	27	**4 dënime me burgim, 2 dënime me të holla, 8 dënime me kusht**	14	**7 dënime me burgim, 4 dënime me të holla, 9 dënime me kusht**	20	**1 dënim me burgim, 3 dënime me të holla, 12 dënime me kusht**	16	**3 dënime me burgim, 1 dënim me të holla, 13 dënime me kusht**	17
Neni 274-b Përpunimi dhe përdorimi i kartelës së rrejshme pagesore		0		0		0	**10 dënime me burgim, 9 dënime me të holla, 6 dënime me kusht**	25	**3 dënime me burgim, 1 dënim me kusht**	4	**7 dënime me burgim, 1 dënim me kusht**	8
Neni 157 Shkelja e të drejtës së autorit dhe të drejtat e lidhura me to		0		0	**1 dënim me burgim, 4 dënime me të holla 1 dënim me kusht**	6	**1 dënim me burgim, 5 dënime me kusht**	6	**1 dënim me të holla**	1		0
Neni 157-b Pirateria e veprës audio-vizuale	**9 dënime me burgim, 4 dënime me të holla**	13	**3 dënime me të holla**	3		0	**1 dënim me burgim, 3 dënime me të holla**	4	**1 dënim me kusht**	1		0
TOTAL		**34**		**30**		**20**		**55**		**22**		**25**

Tabela 1: Llojet, dënimet dhe të dënuarit e veprave penale të krimit kompjuterik në RMV – periudha kohore 2012-2017

4.2 Statistika për krimin kibernetik në SHBA

Meqenëse ky hulumtim shkencor është i përfshirë në përgjithësi si studim më i gjerë për hulumtimin dhe zbulimin e krimeve kompjuterike në botën bashkëkohore, poashtu do të paraqes statistika dhe të dhëna të ndryshme për disa lloje të krimeve kompjuterike në SHBA, se sa është numri më i përhapur i këtij lloji kriminaliteti në vendet më të zhvilluara teknologjikisht. Në vazhdim është paraqitur një tabelë që ka të bëjë me numrin e shkeljeve të të dhënave dhe

rekordeve të ekspozuara në SHBA për periudhën kohore 2005-2020-të. Me shkelje të të dhënave nënkuptojmë kur informacionet e vlefshme të klasifikuara private dhe të sigurta, ekspozohen ndaj një përdoruesi të paautorizuar. Shkelja mund të jetë shkatërrimi ose vjedhja e shënimeve të kopjuara, disqeve, USB-ve, laptopëve ose pajisjeve mobile, vjedhja e llogarisë bankare ose numrave të kartave të kreditit, informacioneve personale, fjalëkalimeve etj.

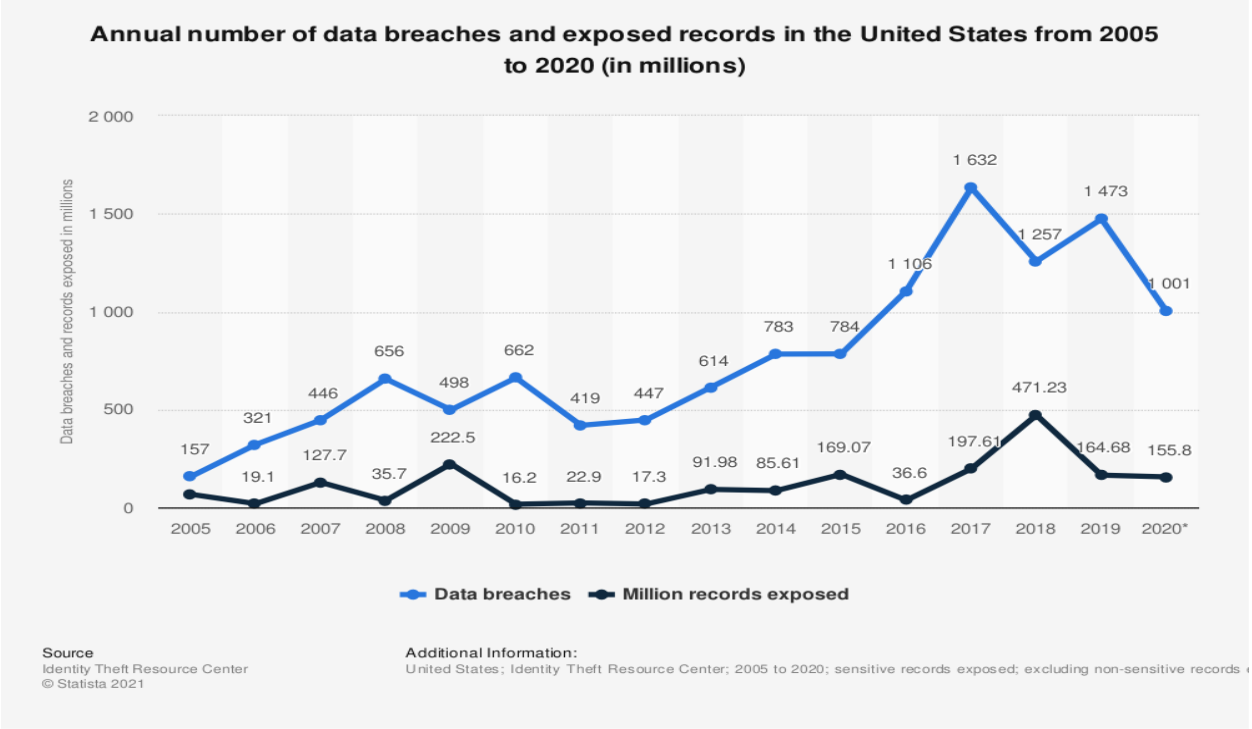


Tabela 2: Numri vjetor i shkeljeve të të dhënave dhe rekordeve të ekspozuara në SHBA nga 2005 në 2020[119]

Tabela e dytë, paraqet të dhëna statistikore në lidhje me shkeljen e të dhënave dhe rekordeve të ekspozuara në milione, të cilat janë të siguruara nga Statista[120] kompani e specializuar në të dhënat e tregut dhe konsumatorit. Në këtë hulumtim mund të konstatojmë se nga viti 2005 deri në vitin 2013 ka pasur numër më të ulët të shkeljeve dhe ekspozimit të të dhënave, ndërsa nga vitit 2014 deri vitin 2020, me zhvillimin e teknologjisë dhe përhapjen më

[119] Të dhëna statistikore nga STATISTA: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (qasja e fundit 21.05.2021)
[120] Po aty;

të shpejtë të internetit, shihet qartë se ka një rritje të dyfishuar të numrit të shkeljeve të të dhënave.

Numri i shkeljeve të të dhënave në Shtetet e Bashkuara në vitin 2020 arriti në 1001 incidente. Ndërkohë, mbi 155.8 milion njerëz u ndikuan nga ekspozimi i të dhënave në të njëjtin vit, i cili përshkruhet si zbulimi i paqëllimtë i informacionit konfidencial për shkak të mbrojtjes joadekuate të informacionit.

Megjithëse numri i shkeljeve të të dhënave është rritur në mënyrë dramatike gjatë dekadave të fundit, nga 662 në 2010 në mbi një mijë deri në vitin 2020, ndërsa numri i ekspozimeve të të dhënave jo. Numri i dokumenteve konfidenciale arriti kulmin në 2009 dhe 2018, me mbi 223 dhe 471 milion rekord të rrjedhura në çdo vit. Edhe pse ndërhyrjet në të dhëna janë rezultat i sulmeve të qëllimshme kibernetike në rrjetin e një kompanie, ekspozimet e të dhënave janë rezultat i neglizhencës njerëzore, siç është mungesa e sigurisë së brendshme kibernetike, e cila ekspozon të dhënat.

Sulmi më i madh i të dhënave deri më sot u zbulua në fund të vitit 2016, kur faqja e internetit Yahoo zbuloi se hakerat kishin hyrë në informacionin e përdoruesit nga të paktën 1 miliard llogari nga viti 2013. Sidoqoftë, i gjithë qëllimi i kësaj shkelje u ekspozua në tetor të vitit 2017, i cili te tabela e mësipërme poashtu është një ndër vitet që ka më së shumëti shkelje tëtë dhënave ku numri arrin deri në 1632 shkelje dhe në po të njëjtin vit 197.61 milion njerëz u ndikuan nga ekspozimi i të dhënave.

4.3 Statistika në Europë (Hollandë)

Krimi në internet po bëhet më sfidues dhe i dhunshëm. Kjo mund të shihet në përvetësimin e teknologjisë së lartë, në sulmet apo shkeljet e të dhënave, mashtrimet seksuale si dhe llojet tjera të krimit në internet. Krimi kibernetik po bëhet një çështje më e madhe në vendet Europiane, ku teknologjia e internetit është e zhvilluar mirë dhe proceset e pagesave pothuajse shumica bëhen në internet. Sidoqoftë, kriminelët në internet janë të interesuar për një fushë më të gjerë të dhënash, jo vetëm për të dhëna financiare. Numri dhe frekuenca e shkarkimit apo vjedhjes së të dhënave po rritet, gjë që çon në një rritje të rasteve të vjedhjeve dhe shantazhimeve. Duke u bazuar në kompaninë e bazës së të dhënave Statista, në Europë vendi i parë në list për nga sulmet kibernetike është Holanda, për të cilën kam paraqitur të dhënat statistikore si dhe analizimin e tyre.

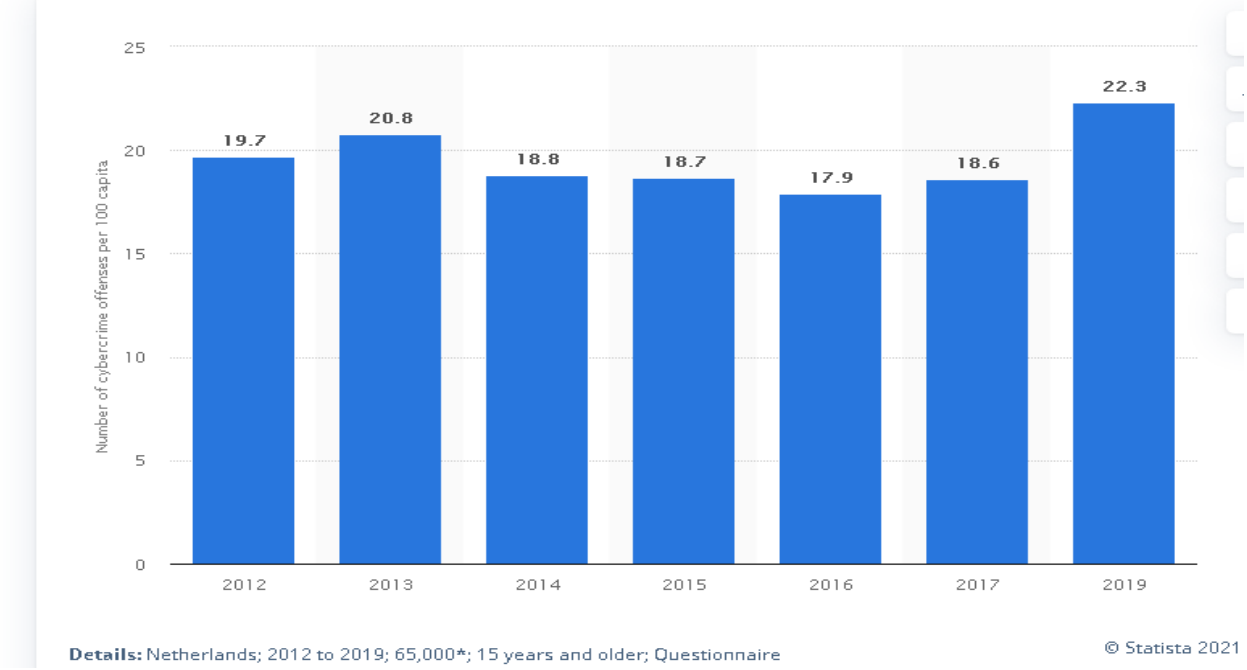


Tabela 3: Numri i veprave penale të krimit kibernetik në Hollandë (për 100 banorë)

periudha kohore 2012-2019[121]

Në tabelën e mësipërme që ka të bëjë me krimin kibernetik në Hollandë, statistikat apo të dhënat janë të marra nga kompania e bazës së të dhënave Statista, nëpërmjet një pyetësori me persona mbi moshën 15 vjet. Është paraqitur numri i personave të viktimizuar (për 100

[121] Të dhëna nga STATISTA: https://www.statista.com/statistics/593495/number-of-cyber-crime-offenses-in-the-netherlands/#statisticContainer (qasja e fundit 25.05.2021)

banorë) nga krime të ndryshme kibernetike gjatë periudhës kohore nga viti 2012 në 2019-tën, ku në vazhdim do të paraqiten konstatime të ndryshme në lidhje me këtë hulumtim.

Duke analizuar tabelën, mund të konstatojm se gjatë gjithë viteve në periudhën kohore 2012-2019, viti 2016 është viti i cili ka numër më të vogël të veprave penale 17 persona të viktimizuar nga 100, dmth më pak persona të atakuar nga ndonjë krim kibernetik, duke parasysh në vitet 2014, 2015, 2017 të cilët kanë nga 18 shkelje apo persona viktima, pastaj viti 2012 me 19 shkelje dhe viti 2013 me 20 shkelje, ndërsa pa ndonjë dallim të madh në numër, ulje apo ngritje drastike, viti 2019 është viti i cili ka numër më të madh të veprave penale ku janë të viktimizuar 22 persona nga 100.

Në bazë të studimit nga autori apo publikuesi i kësaj tabele Joseph Johnson, në vitin 2019, rreth 22 në çdo 100 Hollandezë ishin viktima të krimit kibernetik, ku hakingu ishte krimi kibernetik më i popullarizuar në Hollandë në vitin 2019, me 8 në 100 persona që raportuan se profili i tyre në internet, telefoni ose llogaria e postës elektronike së tyre ishte sulmuar ose keqpërdorur. Sipas tij, në Hollandë kishte shqetësime në lidhje me krimin kibernetik bankar në internet ku përfshiu pyetje në lidhje me këtë aspekt, ku pavarësisht nga fakti se shumica e të anketuarve thanë se ata kurrë nuk kishin qenë viktimë e mashtrimeve bankare në internet ose mashtrimit me kartela pagesore, dmth ishin mestaraisht të shqetësuar për këtë lloj të krimit në internet, në krahasim me të anketuarit tjerë evropian.

Sulmet kibernetika të huaja poashtu janë një shqetësim dhe po shkaktojnë frikë të mëtejshme. Sipas sondazheve të fundit, qytetarët holandezë pajtohen se sulmet kibernetike globale kan qenë një rrezik më i madh në 2018 sesa ishin në 2016. Shërbimi ushtarak holandez informativ dhe i siguris në Tetor 2018 kishte ndaluar një sulm ndërkombëtar të organizatës për ndalimin e armëve kimike në Hagë, kështu duke rritur mundësinë dhe për tu bërë më të vetdijshëm që të identifikojnë sulmet kibernetike nga kombet e tjera.

4.3.1 Rastet e regjistruara të krimit kibernetik në Belgjikë

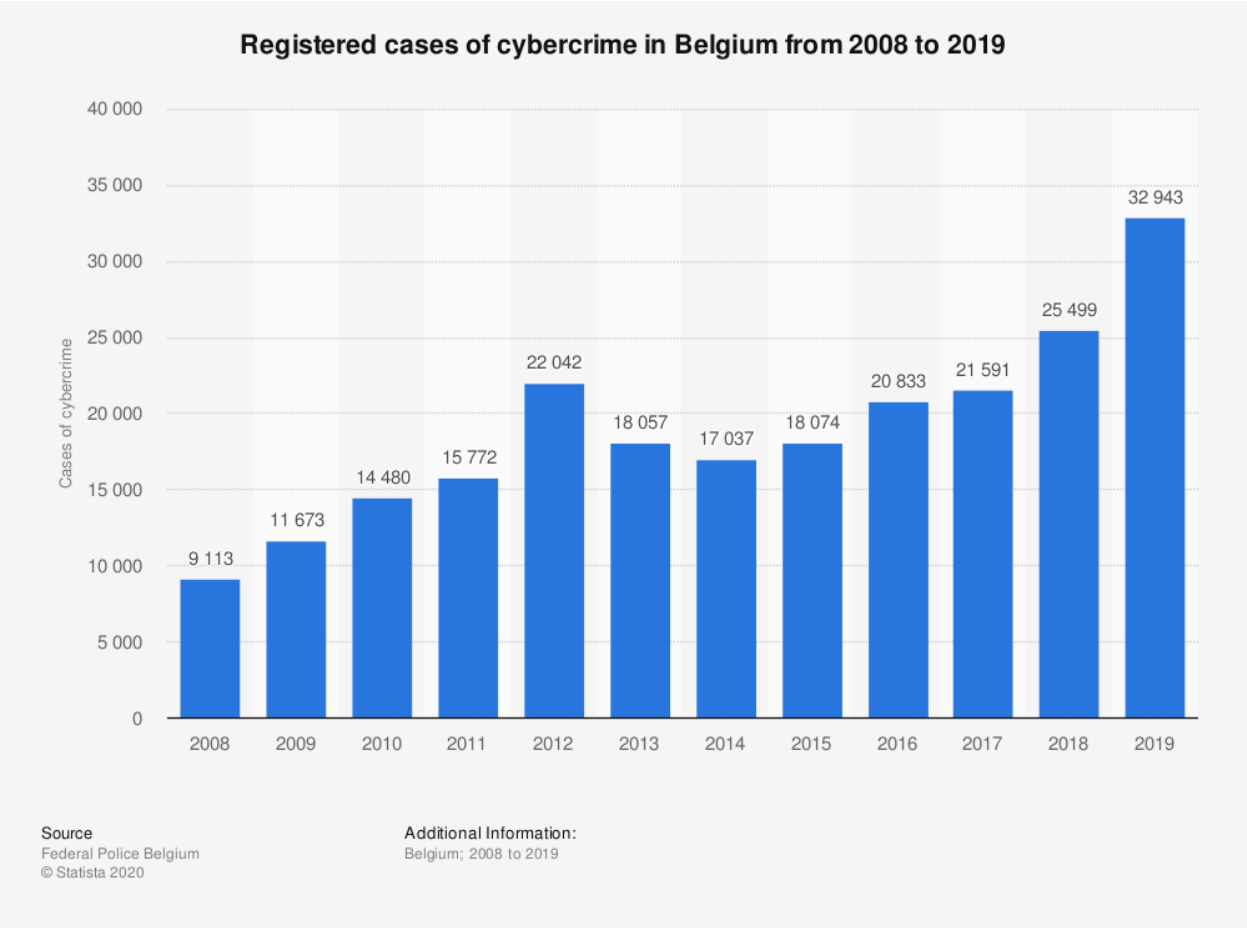


Tabela 4: Rastet e regjistruara të krimit kibernetik në Belgjikë periudha kohore 2008-2019[122]

Tabela e mësipërme paraqet hulumtim të publikuar nga Statista platforma më e madhe globale për gjeneralizimin e të dhënave dhe statistikave, në lidhje me çështjet e paraqitura të krimit kibernetik në Belgjikë për periudhën kohore të caktuar, analizimim e statistikave si dhe konstatime të ndryshme në lidhje me to.

Nga ky hulumtim mund të konstatojmë se krimi kibernetik në Belgjikë të gjitha vitet në intervalin kohor kanë pothuajse disa ndryshime të përafërta në numrin e kryerjes së krimeve,

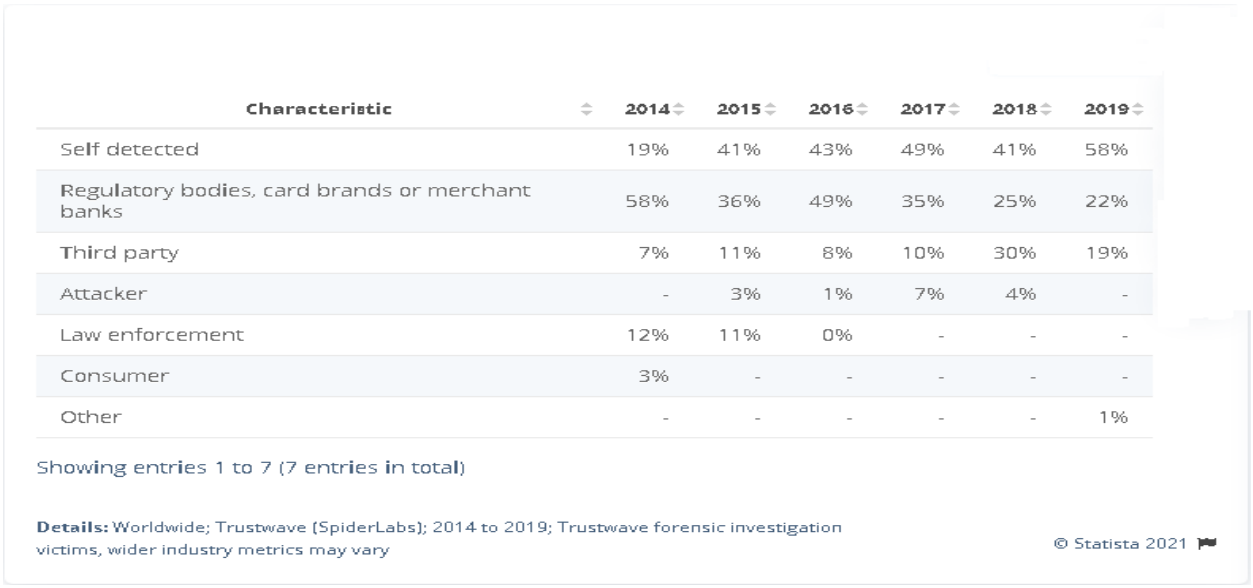
[122] Burim nga STATISTA: https://www.statista.com/statistics/534977/cybercrime-in-belgium/ (qasja e fundit 25.05.2021)

ndërsa vitet që dallojn janë nga viti 2008 ku ka pasur numër më të ulët të rasteve të regjistruara me 9113 raste, duke arritur një rritje në numrin e rasteve të regjistruara në vitin 2012 me 22042 raste, ku në vijim pason viti 2019 ku ka një ngritje drastike të numrit të krimeve kibernetike ku arrin në 32943 raste.

Siç e përmenda se mbi 32 mijë incidente të kriminalitetit kibernetik u regjistruan nga policia federale Belge në vitin 2019. Krime të tilla ndodhin në hapësia dhe fusha të ndryshme kibernetike, rritja e këtyre krimeve është ndihmuar nga demokratizimi i përdorimit të softuerit si dhe globalizimi i aksesit në rrjet.

Në botën e sotme, rrjeti i internetit ka evoluar në një forum të rëndësishëm për konfliktet e armatosure. Në disa shtete përdorimi i teknologjive për të shënjestruar dhe sulmuar kombet tjera është konfirmuar zyrtarisht, ku termi për këtë lloj konflikti ësht luftë kibernetike. Shfrytëzimi i internetit lejon që rrjetet e prekshme të shënjestrohen nga kudo në botë si për shembull, faqet e drejtuara nga qeveria, institucionet, bizneset, organizatat joftimprurëse dhe madje edhe individët mund të sulmohen.

4.3.2 Statistika të zbulimit të sulmeve kibernetike



Characteristic	2014	2015	2016	2017	2018	2019
Self detected	19%	41%	43%	49%	41%	58%
Regulatory bodies, card brands or merchant banks	58%	36%	49%	35%	25%	22%
Third party	7%	11%	8%	10%	30%	19%
Attacker	-	3%	1%	7%	4%	-
Law enforcement	12%	11%	0%	-	-	-
Consumer	3%	-	-	-	-	-
Other	-	-	-	-	-	1%

Showing entries 1 to 7 (7 entries in total)

Details: Worldwide; Trustwave (SpiderLabs); 2014 to 2019; Trustwave forensic investigation victims, wider industry metrics may vary

© Statista 2021

Tabela 5: Zbulimet e sulmeve kibernetike kriminalistike në të gjithë botën nga 2014 në 2019, të organizuara nga teknika e zbulimit[123]

Tabela e pestë, paraqet të dhëna nga viti 2014 në vitin 2019 që tregojnë karakteristikat apo llojet më të përhapura të zbulimit të sulmeve kibernetike. Në rend të parë renditet zbulimi nga vetë viktimat se janë atakuar nga një sulm apo krim kibernetik ku çdo vitë gjatë intervatlit kohor ka një përqindje të lartë të zbulimit nga vet viktimat, ndërsa në vitin 2019 janë zbuluar rreth 58% të rasteve të shkeljeve të të dhënave.

Vendin e dytë e zënë organizatat apo agjencionet publike ose qeveritare si dhe bankat tregtare për zbulimin e sulmeve kibernetike ku poashtu ka një përqindje të lart të zbulimit të rasteve nga këto institucione ku në vitin 2014, 2015, 2016 ka pasur përqindje më të lart përafërsisht te 50-60% të sulmeve të zbuluara, ndërsa në vitet 2017, 2018, 2019 ka një rënie më të ulët të përqindjes së rasteve të zbulimit ku arrin numri deri në 22-25%.

Poashtu edhe pala e tretë dhe zbatuesit e ligjit kanë ndikim apo rol të rëndësishëm në zbulimin e sulmeve kibernetike, ku sigurisht se pas zbulimit të sulmit apo atakimit të krimi kibernetik nga vetë viktima, ndihma që ofrohet për hetim dhe zbulim është nga këto subjekte.

[123] Burim nga STATISTA: https://www.statista.com/statistics/434820/cyber-attack-detection-investigation/ (qasja e fundit 26.05.2021)

PËRFUNDIMET DHE REKOMANDIMET

Si përfundim i këtij punimi, është e pamundur të parashikohet se deri ku do të arrij krimi kibernetik në të ardhmen dhe se si do të trajtohen këto lloje krimesh. Gjërat që kanë ndodhur në të kaluarën nuk na tregojnë se çfarë do të ndodhë në të ardhmen, pasi bota e kompjuterëve përparon çdo ditë. Njerëzi në këtë shoqëri teknologjike gjithnjë në zhvillim mbështeten në një larmi mjetesh teknike për ta bërë jetën e tyre më të lehtë dhe më të shpejtë. Globalizimi ka ndodhur falë internetit, i cili ka lidhur njerëz në të gjithë botën. Jeta e njerëzve është ndikuar në mënyrë drastike nga përdorimi i vazhdueshëm i teknologjisë dhe internetit. Interneti ka aftësinë për të lidhur njerëz, organizata dhe biznese në të gjithë botën me ritme relativisht më të shpejta.

Si përfundim qëndron fakti se krimi kibernetik ka qenë në rritje vitet e fundit dhe janë shkaktuar dëme të mëdha financiara tek individët apo edhe subjektet tjera. Çdo vit llogariten rreth 1.5 milion sulme kibernetike, kriminelët kibernetik vazhdimisht formulojnë procese dhe instrumente apo metoda të reja çdo ditë për të kryer këto krime dhe dëmtojnë rëndë ekonominë në përgjithësi nëpër shtete të botës, ku duhet të ketë përmirësime, avancime dhe të hulumtohen apo shqyrtohen këto fenomene të rrezikshme për ti zbuluar dhe parandaluar ato.

Përderisa krimi kibernetik po zhvillohet me një ritëm shumë të madh, luftimi i efektshëm i këtij krimi mund të garantojë sigurinë e ardhshme financiare në të gjithë botën për njerëzit si dhe shoqatat apo organizatat. Beteja kundër këtij krimi është domethënëse për faktin se do të garantojë ndershmëri dhe mundësin e arritjes që të besojnë se të dhënat e tyre individuale monetare janë të sigurta, poashtu edhe organizatat dhe qeveritë mund të ndihen të sigurta se informacioni i tyre është i sigurt.

Rekomandimi im është që të arrihen njohuri më të qarta rreth rrezikshmërisë së këtij krimi, metoda dhe mjetet më të përsosura që të përdoren për hetimin dhe zbulimin e këtij fenomeni dhe duhet të arrihet në një ndërgjegësim apo realizim nga njerëzit dhe organizatat e

ndryshme që janë viktima të këtyre krimeve që vazhdimisht neglizhojnë të vendosin instrumente themelore të sigurisë në pajisjet, kornizat dhe organizatat e tyre për mbrojtje nga sulmet kibernetike, pavarësisht se a u besojnë apo ndihen të sigurt nga hetuesit dhe zbuluesit e këtyre krimeve.

Drejtësia kundër kriminelëve kibernetik realizohet rrallë, sepse është vështirë që të kapen, të ndiqen penalisht dhe të vendosen para drejtësis. Kjo nënkupton se qeveritë, organizatat dhe njerëzit që merren me luftimin e këtij krimi duhet të luftojnë në mënyrë bashkëpunuese, që të arrihen rezultate sa më të suksesshme.

Sidoqoftë, ne mund ti shmangim krimet e tilla duke iu përmbajtur udhëzimeve të caktuara. Qeveritë gjithashtu duhet të krijojnë sisteme të posaçme anti-kibernetike që përqendrohen vetëm në krimin kibernetik në të gjithë vendin. Pra, në këtë botë me ritëm të shpejt ku interneti është mënyra e vetme për tu lidhur, ne duhet të jemi jashtëzakonisht vigjilentë në lidhje me të dhënat tona personale dhe profesionale për të siguruar që ato të mos kompromentohen kurrë nga kriminelët kibernetikë.

Është e rëndësishme nevoja për strategji organizative dhe procedura autoritare në nivel kombëtar për të luftuar me efektshmëri rreziqet e sigurisës së rrjetit dhe krimit kibernetik si dhe të ndëshkojë këto krime pavarësisht se ku janë kryer. Në shumë vende, duhet ngritur zyra të reja, si dhe të caktohen punë të reja për organizatat ekzistuese për t'u përshtatur me kërkesat për mbrojtjen në internet ose luftën kundër këtij krimi, gjë që do ndikoj në uljen e kësaj vepre të paligjshme.

Për të siguruar që ligjet që kufizojnë aksesin dhe përmbajtjen në internet nuk abuzohen dhe janë në përputhje me ligjin dhe të drejtat e njeriut, kërkohen apo është e nevojshme për masa mbrojtëse. Qartësia në ligj është e nevojshme gjithashtu për të siguruar që ligjet të mos përdoren për të kufizuar ose lejuar qasjen në përmbajtje të paligjshme të internetit në mënyra që shkelin të drejtat e njeriut.

Për shkak të natyrës transacionale të krimit kibernetik dhe ndërvarësisë së sistemeve digjitale dhe pajisjeve të lidhura me internetin brenda dhe jashtë kufijve të vendeve,

informacioni për krimin kibernetik duhet të shpërndahet përtej kufijve. Përtej kësaj, ekziston nevoja për ndarjen e njohurive rreth praktikave më të mira në hetimet e krimit kibernetik. Qasjet e palëve të interesuara për hetimet e krimit kibernetik dhe informacionet në lidhje me hetimet ndryshojnë në varësi të vendit ku ata jetojnë dhe punojnë. Për të siguruar hetime efektive të krimit kibernetik si në shkallë kombëtare dhe ndërkombëtare, është e nevojshme të menaxhohet kjo njohuri si brenda edhe përtej kufijve.

Krimi kibernetik paraqet një kërcënim serioz për proceset digjitale dhe aktivitetet operacionale të të gjitha kompanive dhe organizatave moderne. Edhe kompanitë më të mëdha në botë janë prekur nga kompromentime të mëdha të sigurisë kibernetike kështu që që të ndalohen këto ndërhyrje na duhen sa më shumë punëtorë të aftë për të ndihmuar vendet dhe t'u përgjigjen me forcë shqetësimeve të tyre të përditshme në këtë fushë.

Unë mendoj se të gjitha kompanitë duhet të njohin rreziqet e mundshme dhe kërcënimin serioz të krimit kompjuterik me të cilin përballen çdo ditë dhe se çdo kompani duhet të ketë të paktën një person të aftë dhe të përshtatshëm në përpjekjen për të zvogëluar dhe ndaluar krimin kompjuterik në tërësin e saj. Dhe i njëjti person duhet të marrë pjesë rregullisht në trajnime dhe kurse të reja nëpër botë sepse çdo ditë këto forma të krimit përhapen gjerësisht dhe në forma të reja.

Ndërsa teknologjia përparon, ligji duhet të përshtatet me gjitha zhvillimet e reja për të hetuar dhe zbuluar ata që abuzojnë dhe keqpërdorin teknologjinë e re. Shumë viktima të krimit kibernetik refuzojnë të raportojnë krime të vogla sepse besojnë se shuma e parave që kanë humbur është e parëndësishme dhe ata preferojnë të jenë të lirë sesa të turpërohen, po krimi duhet të raportohet sa më shpejt që të jetë e mundur në mënyrë që të tjerët të mësojn dhe të ndërgjegjësohen nga një shembull i tillë.

Unë shpresoj që qytetarët e kësaj shoqërie bashkëkohore ta marrin seriozisht këtë çështje, krimi kibernetik duhet të ndalet, çdo formë e krimit, qoftë online ose jo, nuk duhet të tolerohet kurrë për mendimin tim. Siguria dhe mirëqenia e qytetarëve duhet të ruhet, gjithkush meriton të drejtën për të jetuar në një mjedis të sigurt, pa marrë parasysh në jetën reale ose në internet.

BIBLIOGRAFIA

Britz T. Marjie, “Computer Forensics and Cyber Crime an Introduction”, Pearson, 2013

Ch, Mohamed. & D, Ashraf. & K. A. Mohammad. & T, Sapna. “Cybercrime, Digital Forencsics and Jurisdiction”, Vol 593, Springer, 2015

Parker, B. Donn, “Computer Crime: Criminal Justice Resource Manual” Washington D.C. 1989

R, Anthony. & O, Kevin. & S, Jim. & H, R. Jon. & J, R. Benjamin. & R, Thomas. “Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcment, and Prosecutors”, Syngress Publishing, 2007

E, Chuck. & T, Jeff. “Computer Crime, Investigation, and the Law”, Course Technology, 2011

C, Glenn. & D, Ronald. & E, Seth. & I, Noel. & M, Carl. & S, Eric. & S, Taru. & S, Tomoko. “Cybercrime: an annotated bibliography of select foreign-language academic literature”, Library of Congress, 2009

Casey, Eoghan. “Digital Evidence and Computer Crime: Forensic science, Computers, and the Internet”, Academic Press, 2011

Latifi, Vesel. “Kriminalistika”, Prishtinë, 2014

Vula, Veton, “Kriminaliteti Kompjuterik” Prishtinë, 2010

Latifi, Vesel. & Demolli, Haki. “Kriminalistika” Prishtinë, 2019

Nuredini, Ahmet, “Challenges in combating the cyber crime”, Vol.5 No.19, Rome-Italy, 2014

ITU – International Telecommunication Union, “Understanding Cybercrime: Phenomena, Challenges and Legal Response”, United Nations PUBN, 2012

Wall, David, “Crime and the Internet”, London, 2001

Yar, Majid, “Cybercrime and society”, SAGE Publications, 2006

Maras, M. H. “Computer Forenscis: Cybercriminals, Laws, and Evidence”, Jones & Barlett Learning, 2014

Easttom, C. & Taylor, J. “Computer Crime, Investigation, and the Law”, Course Technology, 2011

Bainbridge, David, “An Introduction to Computer Law”, Longman, New York, 2004

EC-Council, “Computer Forenscis: Investigating Network Intrusions and Cyber Crime”, Cengage Learning, 2009

C. Subramanian, “CYBER SECURITY”, International Journal of Recent Scientific Research, Vol. 3, Issue 3, 2012

Finklea M. Kristina, “Identity Theft: Trends and Issues”, CRS Report of Congress, New York, 2010

Anderson, B. K, Dubrin, E. Salinger A. M, “Identity Theft”, Journal of Economic Perspectives, Vol.22, 2008

Newman, R. G, & McNally, M. M, “Identity Theft Literature Review”, NCJRS report, 2005

Taylor, M, & Qualye, E, & Holland, G, “Child pornography – an internet crime” Brunner-Routledge, 2004

Kremling, J. & Parker, A.M.S. “Cyberspace, Cybersecurity, and Cybercrime” SAGE Publications, 2017

Bässmann, Jörg, “Perpetrators in the field of cyber-crime”, Bunderskriminalamt, 2015

Verleysen, Cindy, “Cybercrime: A theoretical overview of the growing digital threat”, EUCPN Secretariat (eds.), EUCPN Theoretical Paper Series, European Crime Prevention Network, Brussels, 2015

United Nations Office on Drugs and Crimes, “Comprehensive Study on Cybercrime”, Vienna, 2013

Petrovic, S., “Kompjuterski Kriminal”, Beograd, 2000

Boba, Rachel, “Криминалистичко истражување – мапирање на криминалот”, Nampress, 2001

Nikoloska, Svetlana, “Методика на истражување компјутерски криминалитет” Shkup, 2013

Bernik, Igor, “Cybercrime and Cyberwarfare”, John Wiley & Sons, Inc., 2014

Tropina, T. “Cyber-policing: the role of the police in fighting cybercrime”, (Eds.) European Police Science and Research Bulletin – Special Conference Issue Nr.2, Germany, 2009

Yusoff, Y., Ismail, R., & Hassan, Z. “Common phases of computer forensics investigation models”, International Journal of Computer Science & Information Technology, 2011

Philip, A. & Cowen, D. & Davis, C., “Hacking Exposed Computer Forensics, Second Edition: Computer Forensics Secrets & Solutions”, McGraw Hill Professional, 2009

Hasan, R., & Raghav, A., & Mahmood, S., “Overview on Computer Forensics Tools”, UKACC International Conference on Control, Cardiff, 2012

Shipley, T.G., Bowker, A., “Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace”, Newnes, 2013

Shinder, D. & Tittel, E. (Eds.), “Scene of the Cybercrime: Computer Forenscis Handbook” Syngress, Elsevier Science, 2002

Gercke, M., “National, Regional and International Legal Approaches in the Fight Against Cybercrime”, in Journal oflnformation Law and Technology, 2008

Burime nga interneti:

1. Përkufizimi i kriminalitetit kompjuterik nga Komisioni Europian: https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en (qasja e fundit 17.11.2020);

2. EUROPOL, Definimi i krimit kibernetik, IOCTA 2018:https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018 (qasja e fundit 17.11.2020);

3. Konventa për Krimin Kibernetik, Këshilli i Evropës, Budapest, 2001 https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (qasja e fundit 17.11.2020);

4. Burime nga interneti për hisotrinë e krimit kibernetik: https://www.le-vpn.com/history-cyber-crime-origin-evolution/ (qasja e fundit 23.11.2020);

5.WEBROOT – The Evolution of cybercrime: https://www.webroot.com/blog/2019/04/23/the-evolution-of-cybercrime/ (qasja e fundit 23.11.2020);

6.History of Cybercrime: https://www.floridatechonline.com/blog/information-technology/a-brief-history-of-cyber-crime/ (qasja e fundit 24.11.2020);

7. Role of computers in crime: https://www.geeksforgeeks.org/role-of-computers-in-crime/ (qasja e fundit 25.11.2020);

8. Krimi Kibernetik – Kompjuterët si shënjestër ose mjete kriminale https://law.jrank.org/pages/11983/Cyber-Crime-Computers-targets-or-criminal-tools.html#ixzz6ekk8qWGv (qasja e fundit 25.11.2020);

9. Statistika nga Gazeta e ligjit dhe politikës së sigurisë kombëtare në SHBA, Burim nga interneti: https://www.thirdway.org/report/countering-the-cyber-enforcement-gap-strengthening-global-capacity-on-cybercrime (qasja e fundit 27.11.2020);

10. Europol and Eurojust Public Information, "Common challenges in combating cybercrime", JOINT REPORT, 2019, fq.3, (https://www.eurojust.europa.eu/common-challenges-combating-cybercrime-identified-eurojust-and-europol qasja e fundit 30.11.2020)

11.Viktimat e krimeve kibernetike: https://www.turremgroup.com/1-in-10-people-have-become-a-victim-of-cybercrime/ (qasja e fundit 1.12.2020);

12.DBS – Important steps that all cybercrime vitctims must take, https://www.dbs.com/act/4-important-steps-that-all-cyber-crime-victims-must-take.html (qasja e fundit 2.12.2020);

13. Types of Cybercrime – Panda Security https://www.pandasecurity.com/en/mediacenter/panda-security/types-of-cybercrime/ (qasja e fundit 09.12.2020);

14. Definimi i pornografisë së fëmijëve nga departamenti I drejtësis në SHBA: https://www.justice.gov/criminal-ceos/child-pornography#: (qasja e fundit 27.12.2020);

15. UNICEF – What is cyberbullying? https://www.unicef.org/end-violence/how-to-stop-cyberbullying (qasja e fundit 04.01.2021);

16. Armstrong, Illnea, "Real Risk or Shadow? The Threat of Cyberterrorsim", Article online: https://www.scmagazine.com/home/security-news/features/real-risk-or-shadow-the-threat-of-cyberterrorism/ (qasja e fundit 12.01.2021);

17. CYBERSECURITY GUIDE, Cybercrime investigator: https://cybersecurityguide.org/careers/cyber-crime-investigator/(qasja e fundit 03.03.2021);

18. Definimi i forenzikës kompjuterike nga FBI - https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/oct2000/computer.htm (qasja e fundit 21.03.2021);

19. GlobalSpec – Forensic Hardware Tools https://www.globalspec.com/reference/31783/203279/part-2-forensic-hardware-tools (qasja e fundit 22.03.2021);

20. Paranjpe, P. Computer Forensic Workstation, Marrë nga: http://prateek-paranjpe.blogspot.com/p/computer-forensics.html (qasja e fundit 12.04.2021);

21. Computer (Digital) Forensic Software Tools

https://www.guru99.com/computer-forensics-tools.html (qasja e fundit 13.04.2021);

22. Doracak për krimin kompjuterik: https://www.osce.org/sq/skopje/121225 (qasja e fundit më 16.04.2021);

23. Borges, E - Cyber Crime Investigation Tools and Techniques Explained https://securitytrails.com/blog/cyber-crime-investigation# (qasja e fundit 23.04.2021);

24. Të dhëna statistikore nga STATISTA për SHBA: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (qasja e fundit 21.05.2021);

25. Të dhëna nga STATISTA për Hollandën https://www.statista.com/statistics/593495/number-of-cyber-crime-offenses-in-the-netherlands/#statisticContainer (qasja e fundit 25.05.2021);

26. Burim nga STATISTA për Belgjikën: https://www.statista.com/statistics/534977/cybercrime-in-belgium/ (qasja e fundit 25.05.2021);

27. Burim nga STATISTA për modelet e zbulimit të sulmeve kibernetike: https://www.statista.com/statistics/434820/cyber-attack-detection-investigation/ (qasja e fundit 26.05.2021);