ANALIZË E VEPRËS PENALE TË KRIMIT KIBERNETIK SIPAS STANDARDEVE NDËRKOMBËTARE

GLEDIS PEZA

Temë e dorëzuar në përmbushje të kërkesave për titullin Master i Shkencave në Drejtësi

Universiteti “EPOKA”

2023

APPROVAL PAGE

Student Name & Surname:	Gledis Peza
Faculty:	Faculty of Law and Social Sciences
Department :	Department of Law
Thesis Title :	Analizë e veprës penale të krimit kibernetik sipas standardeve ndërkombëtare. An analysis of the criminal offense of cyber crime according to international standards.
Date of Defense:	04.07.2023

I certify that this final work satisfies all the legal requirements as a Master Thesis for the degree of Master of Science in Law.

Dr. Niuton MULLETI
Acting Head of Department

This is to certify that I have read this final work and that in my opinion it is fully adequate,in scope and quality, as a Master Thesis for the degree of Master of Science in Law.

Dr. Alba GËRDECI
Supervisor

Examination Committee Members

Title / Name & Surname	Affiliation	Signature
1- Dr. Alba GËRDECI	EPOKA University	
2- Dr. Eglantina FARRUKU	EPOKA University	
3- Dr. Mirgen PRENÇE	EPOKA University	

ANALIZË E VEPRËS PENALE TË KRIMIT KIBERNETIK SIPAS STANDARDEVE NDËRKOMBËTARE

ABSTRAKT

Zhvillimi teknologjik dhe lindja e internetit në veçanti, kanë çuar në krijimin e një kanali të ri komunikimi, i cili ende konsiderohet si revolucioni i shekullit. Ky zhvillim jo vetëm përfaqëson aftësinë për të dërguar, ose marrë informacion midis njerëzve, të ndodhur në distancë dhe në vende të ndryshme të botës por, së bashku me përdorimin e sistemeve kompjuterike, përbën mjet për kryerjen e veprave penale. Disa lloje të krimit tradicional, si vjedhja e informacionit, mashtrimi, spiunazhi, pedofilia dhe terrorizmi, tani mund të kryhen edhe përmes sistemeve të reja digjitale. Ky punim analizon historikun, përkufizimin, legjislacionin ndërkombëtar dhe vendas mbi krimin kibernetik, duke u fokusuar veçanërisht në rolin e Konventës së Budapestit dhe NATO-s në luftën kundër aktiviteteve kriminale kibernetike. Disa shtete të prekura nga këto sulme, shohin të nevojshme, përveç aplikimit të konventave ndërkombëtare edhe nevojën e ndërhyrjes së NATO-s, si organizatë e sigurisë për të shqyrtuar, krijuar politika për mbrojtjen kolektive kibernetike, si dhe për mundësinë e aktivizimit të nenit 5 të Kartës së NATO-s. Gjithashtu, në këtë punim do analizohet dhe sulmi kibernetik që pësojë Republika e Shqipërisë më 15 korrik 2022. Në fund të këtij punimi, do të trajtohen sfidat që lidhen me adresimin dhe parandalimin e krimit kibernetik, duke theksuar kompleksitetin dhe natyrën në zhvillim të këtij kërcënimi global. Gjetjet evidentojnë nevojën emergjente për bashkëpunim dhe për masa më të forta për të luftuar krimin kibernetik në mënyrë efektive në nivel kombëtar dhe ndërkombëtar.

Fjalët kyçe: Interneti, krimi kibernetik, kërcënim, siguri.

AN ANALYSIS OF THE CRIMINAL OFFENSE OF CYBER CRIME ACCORDING TO INTERNATIONAL STANDARDS

ABSTRACT

Technological advancements, especially the advent of the internet, have lead in a new era of communication, often referred as the revolution of the century. This progress not only enables the exchange of information between individuals across vast distances and different countries but also provides a platform for committing criminal offenses when combined with computer systems. Traditional crimes such as theft, fraud, espionage, pedophilia, and terrorism have found new avenues within digital systems. This paper examines the history, definition, and international legislation surrounding cybercrime, with a specific emphasis on the Budapest Convention and the role of NATO in combating these criminal activities. On this regarde certain states affected by cyber attacks recognize the necessity, in addition to international conventions, for NATO's intervention as a regulatory body for security. This includes the formulation of collective cyber defense policies and the invocation of Article 5 of the NATO treaty. Additionally, this paper will analyze the cyber attack in the Republic of Albania that occurred on July 15, 2022. Finally, the challenges related to addressing and preventing cybercrime will be examined, emphasizing the complexity and evolving nature of this global threat. The findings shed light on the urgent need for enhanced cooperation and robust measures to effectively combat cybercrime at both national and international levels.

Keywords: Internet, cybercrime, threat, security.

FALËNDERIMET

Dëshiroj që këtë hapësirë të punimit tim t'ia kushtoj njerëzve që kanë kontribuar, me mbështetjen e tyre të palodhshme, në realizimin e kësaj teme.

Së pari, falënderoj Dr. Alba Gërdeci, për durimin e saj të pamasë, për këshillat dhe për njohuritë e transmetuara gjatë gjithë procesit të hartimit të punimit. Të kesh mundësinë për të punuar me të ndër vite ishte intelektualisht shpërblyese dhe përmbushëse. E falënderoj për sugjerimet dhe ekspertizën e saj të detajuar.

Falënderimet e mia të veçanta shkojnë për familjen time. Falënderoj prindërit e mi Rudi dhe Shpresa për dashurinë, inkurajimin dhe mbështetjen e tyre të pakushtëzuar gjatë gjithë këtij udhëtimi sfidues. Besimi i tyre tek unë ka qenë një burim i vazhdueshëm motivimi dhe unë jam vërtet me fat që i kam në jetën time. Gjithashtu, dua te falënderoj dhe motrën time Julia e cila më ka qëndruar pranë në momentet e vështira, duke më duruar dhe mbështetur. Nuk do të ndalem kurrë së ju falënderuari që më mundësuat të arrij deri këtu.

Falënderoj Delonin, i cili ka qenë gjithmonë pranë meje duke më mbështetur dhe inkurajuar.

Gjithashtu, dua të falënderoj shoqen time Enxhi Tafani, e cila ndau me mua gëzimet dhe vështirësitë e këtyre pesë viteve të kaluara së bashku.

Shumë faleminderit të gjithëve!

DEKLARATA

Deklaroj se kjo Tezë Masteri, e titulluar Analizë e veprës penale të krimit kibernetik sipas standardeve ndërkombëtare, bazohet në punën time origjinale, përveç citimeve të cilat janë pasqyruar siç duhet. Gjithashtu, deklaroj se kjo tezë nuk është dorëzuar më parë, apo njëkohësisht për dhënien e asnjë diplome, në Universitetin Epoka ose në ndonjë universitet apo institucion tjetër.

Firma:

Gledis Peza

Datë:

TABELA E PËRMBAJTJES

LISTA E FIGURAVE

LISTA E SHKURTIMEVE

AKSHI	Agjencia Kombëtare e Shoqërisë së Informacionit.
BE	Bashkimi Evropian.
CDMB	Bordi i Menaxhimit të Mbrojtjes Kibernetike.
CCDCEO	Qendra e Ekselencës e Mbrojtjes Kibernetike Kooperative.
CSIRT	Ekipi i Reagimit ndaj Incidenteve të Sigurisë Kompjuterike.
DART	Ekipi i Zbulimit dhe Reagimit të Microsoft.
EC3	Qendra Evropiane e Krimit Kibernetik.
ENISA	Agjencia e Bashkimit Evropian për Sigurinë Kibernetike.
FBI	Byroja Federale e Hetimeve.
FEMA	Agjencia Federale e Menaxhimit të Emergjencave.
GJNP	Gjykata Ndërkombëtare Penale.
IOCTA	Vlerësimi i Kërcënimeve të Krimit të Organizuar në Internet
NATO	Organizata e Traktatit të Atlantikut Verior.
OCSE	Organizata për Bashkëpunim dhe Zhvillim Ekonomik.
OKB	Organizata e Kombeve të Bashkuara.

HYRJA

Krimi kibernetik është bërë një çështje që kërkon një trajtim urgjent në epokën e stome digjitale. Me zhvillimin e teknologjisë dhe përdorimin masiv të internetit, autorët e veprave penale me natyrë kibernetike kanë gjetur mënyra të reja për të shfrytëzuar dobësitë në rrjetet kompjuterike, duke përdorur pajisje të teknologjisë së lartë për të kryer aktivitete të paligjshme. Krimi kibernetik mund të marrë shumë forma, duke përfshirë hakerimin,vjedhjen e identitetit, mashtrimin në internet, shpërndarjen e malware dhe viruseve. Kjo vepër penale ka ndikim të rëndësishëm dhe të gjerë, duke prekur individë, entitete private dhe qeveritë. Pasojat e krimit kibernetik, mund të rezultojnë në humbje financiare, dëmtim të reputacionit dhe madje edhe dëm fizik në disa raste. Natyra vazhdimisht në zhvillim e krimit kibernetik dhe anonimiteti i autorëve të këtyre veprave penale e bëjnë sfidues parandalimin dhe luftimin e tij. Prandaj, ky punim kërkimor synon të ofrojë një pasqyrë gjithëpërfshirëse të asaj çfarë është krimi kibernetik, ndikimi i tij, strategjitë e parandalimit,sfidat në luftimin e tij dhe drejtimet e ardhshme për kërkime. Krim kibernetik konsiderohen krimet kompjuterike që janë në shkelje të normave penale. Ato përkufizohen si aktivitete të paligjshme që kryhen duke përdorur pajisje ose rrjete kompjuterike, me synim përfitimin e një avantazhi të paligjshëm ose dëmtimin e një individ apo organizate. Ligjet që rregullojnë krimin kibernetik ndryshojnë nga vendi në vend, por shumica e vendeve kanë krijuar ligje specifike për të trajtuar këto krime dhe për të garantuar mbrojtjen e qytetarëve dhe entiteteve të tyre. Përveç kësaj, shumë vende punojnë së bashku për të identifikuar dhe ndjekur penalisht autorët e këtyre veprave penale përmes marrëveshjeve ndërkombëtare të bashkëpunimit gjyqësor.

Krimi kibernetik klasifikohet si transnacional sepse përfshin kalimin e kufijve ndërkombëtarë nëpërmjet internetit dhe rrjeteve kompjuterike. Kjo natyrë e krimit kibernetik vështirëson gjetjen, gjurmimin e autorëve dhe goditjen e tyre. Autorët e këtyre veprave penale shpesh punojnë nga vende të ndryshme anembanë globit, ndërsa përdorin mjete dhe strategji inovative për të fshehur identitetin e tyre. Krimet kibernetike, gjithashtu mund të kryhen nga individë ose grupe të vogla që kanë akses në internet dhe disa aftësi teknike, duke e klasifikuar këtë si një vepër penale që mund të kryhet si nga

organizata kriminale, por edhe vetëm nga një individ. Për shkak se autorët e krimeve kibernetike mund të vijnë nga kudo në botë, është edhe më e vështirë njohja dhe ndjekja penale e tyre, duke e bërë më sfiduese zbatimin e ligjit. Mos harmonizimi i kuadrit ligjor ndërkombëtar është një problem tjetër qësfidon dhe vështirëson luftën ndaj këtij krimi. Përveç kësaj, krimi kibernetik ka avancuar me hakerat që përdorin mjete dhe metoda të fundit për të sulmuar njerëzit, entitetet private dhe qeveritë, veprime këto që kanë rezultuar në humbje të konsiderueshme parash, vjedhje identiteti dhe madje edhe shkelje të sigurisë kombëtare. Bashkëpunimi ndërkombëtar dhe bashkëpunimi midis organizatave të zbatimit të ligjit, qeverive dhe sektorit të biznesit është tejet i nevojshëm për të luftuar krimin kibernetik. Gjithashtu, është tejet e rëndësishme të parandalohet që autorët e këtyre veprave penale të përfitojnë nga boshllëqet ligjore, apo dobësitë e ligjit. Rëndësia e çështjes së krimit kibernetik po rritet globalisht, pasi ai po përbën një kërcënim të rëndësishëm për sigurinë, ekonominë, privatësinë dhe të drejtat e njerëzve.

Objekti i këtij punimi është analiza e llojeve të krimit kibernetik të lindur ndër vite, brenda të cilit planifikohet të analizohen përgjigjet rregullatore ndaj këtij krimi, si nga këndvështrimi i legjislacionit të brendshëm, ashtu edhe nga ai i bashkëpunimit ndërkombëtar. Ky punim analizon veprën penale të krimit kibernetik, duke eksploruar historikun, përkufizimin, legjislacionin ndërkombëtar dhe vendas, duke ofruar një pasqyrë gjithëpërfshirëse të evolucionit të krimit kibernetik dhe duke theksuar se si përparimet teknologjike, veçanërisht zhvillimi i internetit, kanë krijuar rrugë të reja për aktivitete kriminale.

Ky punim është i organizuar në pjesën hyrëse, 4 kapituj dhe në pjesën “përfundime”, si pjesa përmbyllëse e këtij punimi, e cila për shkak të natyrës së krimit nuk do të jap konkluzione, por disa reflektime të arritura mes analizës së legjislacionit ndërkombëtar dhe atij vendas.

Kapitulli i parë do të trajtojë çështjen e krimit kibernetik përmes një përkufizimi më specifik, jo të unifikuar, që na lejon të kuptojmë ndryshimet, kriteret dhe klasifikimet e përdorura nga doktrina dhe jurisprudenca. Gjithashtu, në këtë kapitull do të gjurmohet historia e krimit kibernetik, duke shqyrtuar origjinën e tij dhe faktorët që kanë kontribuar nërritjen e kësaj vepre penale. Në këtë pjesë del në pah dhe fuqia transformuese e internetit, i cili ka lehtësuar komunikimin dhe lidhjen përtej kufijve, por gjithashtu ka ofruar mundësi për kryerjen e aktiviteteve kriminale në shkallë globale. Përcaktimi i

krimit kibernetik është një aspekt tjetër thelbësor, pasi vetëm duke idenfikuar qartë format e kësaj vepre penale mund të zhvillojmë mënyra efektive, strategji dhe politika për të luftuar këtë kërcënim gjithnjë në zhvillim.

Kapitulli i dytë do të trajtojë bashkëpunimin ndërkombëtar me fokus Evropën, duke qenë se sfera e veprimit të krimeve kibernetike prek në shumicën e rasteve disa shtete në të njëjtën kohë. Duke u përqendruar në aktet më të rëndësishme për evoluimin dhe krijimin e mjeteve mbrojtëse nga institucionet evropiane, një rol qendror në këtë kapitull i rezervohet Konventës së Këshillit të Evropës për Krimin Kibernetik, si akti i parë që parashikon një sërë rregullash kontraktuale, të cilat Shtetet Anëtare duhet t'i respektojnë. Një pjesë të konsiderueshme në këtë kapitull do të zërë trajtimi i rolit të NATO-s si organizatë për çështjete sigurisë, si dhe juridiksioni i mundshëm i GJNP-s për të ndjekur penalisht individët përgjegjës për sulmet kibernetike.

Kapitulli i tretë, do të paraqes një analizë të legjislacionit të Republikës së Shqipërisë në raport me krimet kompjuterike "krimi kibernetik" duke sjell dhe një statistikë të këtyre krimeve ndër vite. Një pjesë e konsiderueshme e punimit do ti kushtohet krimit kibernetik në Republikën e Shqipërisë duke eksploruar natyrën e krimit kibernetik brenda vendit dhe duke hedhur dritë mbi sfidat specifike me të cilat përballet Shqipëria në adresimin dhe parandalimin e kërcënimeve kibernetike. Në këtë kapitull do analizohet sulmi kibernetik qëndodhi më 15 korrik 2022, në raport me ndikimet, pasojat dhe mësimet e nxjerra nga incidenti.

Në kapitullin e katërt do të trajtohet çështja nëse sulmet kibernetike kryhen vetëm nga individë apo dhe strukturat shtetërore mbështesin apo favorizojnë në mënyrë pasive akte të tilla. Parë në këtë kontekst, pjesë e këtij kapitulli do të jetë edhe trajtimi i sfidave që lidhen me luftën e krimit kibernetik, çështjet komplekse juridiksionale që lindin në hapësirën kibernetike, nevojën për bashkëpunim ndërkombëtar dhe shkëmbim informacioni, si dhe domosdoshmërinë e masave proaktive, politikave të forta dhe kërkimit të vazhdueshëm përtë adresuar sfidat gjithnjë në zhvillim të paraqitura nga aktivitetet kriminale kibernetike.

METODOLOGJIA DHE PYETJET KËRKIMORE

Në këtë punim kërkimor, kam përdorur një qasje metodologjike të përzier për të pasuruar analizën mbi krimin kibernetik, duke përfshirë metodat sasiore dhe cilësore. Nëpërmjet përdorimit të kësaj metodologjie, synohet të ofrohet një kuptim gjithëpërfshirës i

fenomenit.

Analiza sasiore luajti një rol vendimtar në studimin tim, pasi më lejoi të bashkoja të dhëna statistikore mbi prevalencën, llojet dhe modelet e krimit kibernetik në Republikën e Shqipërisë. Kam mbledhur të dhënat përkatëse nga burime të besueshme siç janë raportet e Prokurorisë së Përgjithshme mbi gjendjen e kriminalitetit në Republikën e Shqipërisë. Duke përdorur statistikat, arrita të identifikoja tendencat, të nënvizoja gjetje të rëndësishme dhe të përcaktoja sasinë e shtrirjes së krimit kibernetik në vend. Megjithatë, duke qenë se krimi kibernetik është një çështje komplekse dhe e shumanëshme nuk mund të kuptohet dhe analizohet plotësisht vetëm përmes numrave. Prandaj, analizën sasiore e kam plotësuar me metoda cilësore, veçanërisht përmes përfshirjes së rasteve nga praktika.

Bazuar në llojin e metodologjisë së zgjedhur në punimin tim mbi krimin kibernetik pyetjet kërkimore që udhëhoqën studimin tim janë:

1. Çfarë është, kur është identifikuar dhe si vepron krimi kibernetik?

2. Çfarë parashikon legjislacioni ndërkombëtar për krimin kibernetik dhe cilat janë aktet ndëkombëtare që e njohin këtë vepër penale?

3. Çfarë parashikon Traktai i Atlantikut të Veriut për mbrojtjen kolektive dhe a mund të flasim për mbrojtje kolevtive ndaj krimit kibernetik?

4. A ka iniciativa ndërkombëtare për ta përfshir krimin kibernetik si krim ndërkombëtar?

5. Si u trajtua sulmi kiberneti që pësoj Republika e Shqipërisë?

6. Cilat janë sfidat dhe zgjidhjet e mundshme mbi krimin kibernetik?

KAPITULLI I

KRIMI KIBERNETIK DHE RËNDËSIA E STUDIMIT TË TIJ

1.1 Historiku i krimit kibernetik

Në të kaluarën, asnjë jurist nuk mund të imagjinonte ekzistencën dhe rëndësinë e një "krimi kompjuterik" ose "krimi kibernetik", pasi ai është produkt i epokës digjitale. Ligji duhet të përballet dhe të përshtatet me realitetin, pjesë e të cilit në ditët e sotëm është dhe përballja me këtë lloj të sofistikuar vepre penale, “krimi kibernetik”. Për herë të parë është dëgjuar të flitet për krimin kibernetik në Francë, në vitin 1834, kur ende nuk ishte folur për internetin. Autorët e kësaj vepre penale vodhën informacionin e tregut financiar duke hyrë në sistemin telegrafik francez (Standage, 2017). Që nga ai moment, krimi kibernetik është rritur në mënyrë eksponenciale, i shënuar nga një evolucion intrigues i taktikave dhe procedurave, të cilat i vënë në zbatim për përfitime keqdashëse.

Vitet 90-të shënuan një epokë revolucionare për teknologjitë e komunikimit me ndikim të rëndësishëm për njerëzimin. Me vënien në përdorim të internetit, njerëzit ishin në gjendje të komunikonin me njëri-tjetrin në distanca të mëdha dhe rrjete të ndryshme komunikimi, pavarësisht se ku ndodheshin. Ky nivel i paprecedentë i komunikimit në distancë solli përparime të jashtëzakonshme në mënyrën se si njerëzit ndërvepruan me njëri-tjetrin, si dhenë mënyrën se si bizneset kryenin operacionet e tyre. Megjithatë, këto përparime patën një kosto, rreziku nga krimi kibernetik. Krimi kibernetik u shfaq si një kërcënim i fuqishëm, duke shfrytëzuar dobësitë e këtyre teknologjive të reja. Autorët e krimit kibernetik përfituan nga fakti se masat e sigurisë dhe kontrollet nuk ishin ende një prioritet gjatë fazave të hershme të zhvillimit të komunikimit në distancë. Termi “siguri kibernetike” nuk ishte krijuar ende dhe si rrjedhojë as për krimin kibenetik nuk flitej. Pavarësisht ndikimeve pozitive të këtyre përparimeve teknologjike, një anë e errët filloi të shfaqej. Një ekonomi e nëndheshme filloi të rritej, me autorët e krimit kibernetik që përdornin mënyra të reja për të fituar akses të paautorizuar në sisteme dhe për të manipuluar të dhënat në internet.

Rritja e shkallës së krimit kibernetik ishte një tregues alarmant se sulmuesit tani kishin mundësi të reja për t'i shfrytëzuar, duke përdorur teknologjitë më të fundit në dispozicion.

Gjatë viteve 90-të ka pasur disa raste krimesh të dukshme kibernetike, siç kanë qenë sulmet ndaj korporatave të mëdha, agjencive qeveritare dhe institucioneve financiare. Mendimi i parë që vjen në mendje kur diskutohet krimi kibernetik është se ky lloj krimi konsiston në një temë që është relativisht e re dhe si rezultat pak e njohur. Nevoja për një legjislacion *ad-hoc* në botë u shfaq në fund të viteve 1980, kur filloi transferimi në rrjetet telematike i pjesësdërrmuese të aktiviteteve të punës dhe jetës sociale, si dhe zhvillimi i tregtisë elektronike dhe komunikimit nëpërmjet internetit (Kumar, 2022, p.1362).

Krimi kibernetik ka një histori të gjatë dhe komplekse, e cila me avancimin e teknologjisë ka mundësuar gjithashtu avancimin e metodave dhe teknikave të përdorura për realizimin ekësaj vepre penale. Në fakt, si "krimi tradicional", ashtu edhe "krimi kibernetik" ndjekin metodat e tyre të pasurimit të paligjshëm në tregjet globale dhe në internet duke përfituar nga globalizimi. Siç dhe është specifikuar në Vlerësimin e Kërcënimeve të Krimit të Organizuar në Internet (IOCTA), krimi kibernetik duhet të konsiderohet një evolucion dhe jo një revolucion (IOCTA, 2021, p. 8). Vitet e fundit në fakt kanë dëshmuar faktin se rrethanat e jashtëzakonshme si pandemia por dhe lufta, përshpejtojnë këtë evolucion. Metodat e veprimit të autorëve të këtyre veprave po bëhen gjithnjë e më sistematike dhe të pamëshirshme. Karakteristika thelbësore e krimit kibernetik është pikërisht mungesa e kufijve gjeografikë dhe fizikë, karakteristikë kjo e cila e dallon këtë vepër penale nga krimet tradicionale. Kjo veçori i bën viktimat e këtij krimi më vulnerabël sepse nuk janë në gjendje të reagojnë për shkak të mungesës së informimit të tyre për të perceptuar sulmin. Nga ana tjetër, disponueshmëria e softuerit të përhapur gjerësisht në internet dhe fakti që krimi kibernetik nuk kërkon ndonjë aftësi të veçantë teknike inkurajon autorët e këtyre veprave penale. Disa nga arsyet thelbësore pse çështja e krimeve kibernetike konsiderohet kaq e rëndësishme janë:

- **Cënimi i sigurisë kombëtare:** krimet kibernetike përbëjnë një rrezik për sigurinë e vendit, pasi ato mund të përdoren për të sulmuar sistemet kompjuterike qeveritare dhe ushtarake.
- **Cënimi i të dhënave personale**: përdorimi i teknologjisë për të ruajtur dhe kontrolluar të dhënat personale po rritet, duke i ekspozuar ato ndaj rrezikut të shkeljeve të privatësisë përmes sulmeve kibernetike. Mbrojta e këtyre të dhënave

bëhet një çështje gjithnjë e më e rëndësishme

- **Cënimi i ekonomisë:** krimet kibernetike mund të kenë pasoja të rëndësishme në ekonominë globale, duke rezultuar në humbje financiare për bizneset, individët dhe qeveritë.
- **Transnacionaliteti:** krimet kibernetike kryhen shpesh përtej kufijve kombëtarë dhesi pasojë është e vështirë zbulimi dhe ndjekja e tyre.

Janë këta elementë që bëjnë të domosdoshëm ndëshkimin e krimit kibernetik, si në planin kombëtarë, ashtu edhe në atë ndërkombëtarë, duke nxjerrë në pah nevojën për të pasur fillimisht një përkufizim për krimin kibernetik, e më tej unifikimin ndërkombëtarisht të këtijpërkufizimi.

1.2 Përkufizimi i krimit kibernetik

Me zhvillimin e teknologjisë dhe zhvillimin e taktikave dhe strategjive të përdoruara nga autorët e veprave penale me natyrë kibernetike, ndryshon edhe kuptimi i krimit kibernetik. Deri më sot, pavarësisht se është shfaqur në burimet evropiane dhe ndërkombëtare, krimi kibernetik, nuk përbëhet nga një kategori e përcaktuar ligjërisht (De Vivo, 2012, pp. 25-27). Me kalimin e kohës, nga njëra anë, ka lindur nevoja për të ndëshkuar vepra penale të reja, të kryera përmes teknologjisë dhe internetit, por nga ana tjetër ende nuk ka një përkufizim të unifikuar dhe të pranuar nga shtetet. Përcaktimi i një përkufizimi universal për krimin kibernetik është tejet i vështirë, pasi ky term përfshin brenda vetes një sërë veprash penale të natyrave të ndryshme,por që të gjitha bashkohen nga një emërues i përbashkët që është përdorimi i një kompjuteri ose pajisje kompjuterike (Simoncelli, 2014, pp. 4-7). Krimin kibernetik, në kuptimin e gjerë mund ta përkufizojmë si të gjitha ato vepra penale që kryhen me përdorimin e teknologjive kompjuterike, ose informatike. Hakerimi, vjedhja e identitetit, phishing, sulmet e malware dhe mashtrimi në internet janë vetëm disa shembuj të shumë mënyrave të ndryshme që mund të shfaqet krimi kibernetik. Të gjitha veprimet kriminale që përfshin një kompjuter, rrjet ose pajisje tjetër digjitale në përgjithësi quhen krim kibernetik. Autorët e këtyre veprave përdorin një sërë strategjish dhe taktikash për të marrë akses të paautorizuar në sistemet ose rrjetet kompjuterike, për të vjedhur të dhëna konfidenciale, ose për të penguar biznesin e rregullt. Ata gjithashtu mund të përdorin teknologjinë për të ndihmuar në krime të tjera

si trafikimi inarkotikëve, ose pastrimi i parave.

Autorë dhe organizata të ndryshme kanë paraqitur përkufizime të krimeve kompjuterike, duke ofruar këndvështrime dhe specifika të ndryshme për këtë çështje. Disa autorë nuk besojnë në dallimin e krimeve kibernetike nga krimet tradicionale, kjo sepse sipas tyre edhe pse këto krime kryhen me mjete të ndryshme, ato sjellin të njëjtat vepra penale. Në të vërtetë, Kodet Penale të shumë shteteve ashtu si edhe Kodi Penal i Republikës së Shqipërisë nuk i ndajnë krimet kompjuterike si një kategori më vete. **Agjencia Federale e Menaxhimit të Emergjencave** (FEMA) e përkufizon krimin kibernetik si:

"Sulme dhe kërcënime për sulm ndaj kompjuterëve, rrjeteve dhe të dhënavetë ruajtura në to në mënyrë të paligjshme"(FEMA, n.d).

Duhet thënë gjithashtu se një nga keqkuptimet me të përhapura mbi këtë vepër penale është se mendohet që çdo hap duhet të përfshijë një mjet kompjuterik ose internet. Në fakt, në vijim do të trajtojmë faktin se një vepër penale do të quhet krim kompjuterik dhe nëse ky objekt do të përdoret si mjet qoftë dhe vetëm në njërën nga fazat e kryerjes së veprës (Yue Ba, 2021, pp. 6-7).

Një përkufizim tjetër është dhëne nga **Manuali i Talinit** (Schmitt, 2013), një studimi i rëndësishëm jo detyrues mbi zbatueshmërinë e ligjit ndërkombëtar në luftën kibernetike, sipas të cilit krimikibernetik i referohet çdo akti të paligjshëm që kryhet duke përdorur ose drejtuar kundër sistemeve ose rrjeteve kompjuterike, ashtu edhe ato akte në të cilat kompjuterët ose rrjetet kompjuterike shërbejnë si mjet për të lehtësuar aktivitetet "tradicionale kriminale".

Pavarësisht nga fakti se nuk ka ende një përkufizim universal të krimeve kibernetike, tani ekziston një marrëveshje e gjithë pranuar, e cila përfshin një klasifikim me tre faza, siç është përmbledhur nga Departamenti Amerikan i Drejtësisë:

1. Krimet e kryera me pajisje kompjuterike, të cilat kanë si target një viktimë, një kompjuter ose rrjet kompjuterik, për shembull, malware, sulme DoS dhe hakerime (Clough, n.d., p. 10).
2. Krimet ekzistuese ku kompjuteri është një pajisje që përdoret për të kryer krimin, për shembull, pornografia e fëmijëve, ndjekja dhe mashtrim (Clough, n.d., p. 10).
3. Krimet në të cilat përdorimi i kompjuterit është një detaj i rastësishëm, i cili

mundtë ofrojë prova të krimit, për shembull, adresat e gjetura në kompjuterin e një të dyshuari për vrasje, ose regjistrimet telefonike të bisedave ndërmjet dhunuesit dhe viktimës para kryerjes së vrasjes. Në këto raste, kompjuteri nuk është pjesë aktive në kryerjen e veprës penale, por shërben më shumë si një provë (Clough, n.d., p. 10).

Për sa i përket legjislacionit për të sanksionuar krimin kibernetik është tejet i rëndësishme për disa arsye. Së pari, ligjet kundër krimit kibernetik ofrojnë një bazë ligjore për shtetet qëtë punojnë së bashku për të hetuar dhe ndjekur penalisht autorët e krimeve kibernetike, për të shkëmbyer informacione, përvoja dhe për të zhvilluar strategji për parandalimin e sulmeve kibernetike në të ardhmen. Së dyti, pasja e ligjeve për të sanksionuar krimin kibernetik ndihmon në ndërtimin e besimit në ekonominë digjitale. Ligjet kundër krimit kibernetik kanënjë ndikim pozitiv në formimin e një mjedisi më të sigurt në internet, i cili mbështet inovacionin dhe rritjen ekonomike.

1.3 Karakteristikat e krimit kibernetik

Veprat penale të këtij lloji mund të kenë forma dhe karakteristika të ndryshme, por në përgjithësi ato mund të identifikohen nëpërmjet karakteristikave të mëposhtme:

- **Përdorimi i teknologjisë**: Krimet kibernetike ndodhin përmes përdorimit të teknologjisë së informacionit, si interneti, kompjuterët, telefonat, serverat dhe teknologjitë e tjera të lidhura me to. Këto teknologji janë gjithnjë e më të lehta për t'u përdorur në ditët e sotme, duke siguruar një nivel të lartë disponueshmërie dhe aksesibiliteti, jo vetëm për përdoruesit e zakonshëm por dhe për personat të cilët synojnë të kryejnë vepra penale nëpërmjet tyre.
- **Anonimiteti:** Konfidencialiteti në botën digjitale dhe kibernetike favorizon autorëte veprave penale. Ata mund të fshehin identitetin e tyre në internet përmes përdorimittë serverave proxy, e-mailave të falsifikuar ose adresave IP dhe e-mail anonime. Anonimiteti gjithashtu mund të ruhet përmes përdorimit të enkriptimit, i cili është lehtësisht i arritshëm, dhe gjurmët e provave digjitale mund të largohen përmes softuerëve të gatshëm në treg.
- **Mungesa e kufijve gjeografikë:** Paradigma e drejtësisë penale ka qenë tradicionalisht vendore, duke u limituar në juridiksionin territorial ku ka ndodhur vepra penale. Rrjetet e reja kompjuterike e kanë sfiduar këtë paradigmë. Krimet

kibernetike mund të kryhen nga kudo në botë dhe mund të prekin viktima kudo në botë, pasi interneti dhe teknologjitë e informacionit nuk njohin kufij gjeografikë.

- **Vështirësi në identifikimin e autorëve:** Rreziku i perceptuar për t'u kapur dhe ndjekur penalisht është një element i rëndësishëm që mund të ketë efekte në sjelljen kriminale. Në këtë drejtim, teknologjia digjitale paraqet një sërë vështirësish për zbatimin e ligjit. Përveç vëllimit të madh të përdoruesve, natyra e komunikimeve me anë të pajisjeve kompjuterike moderne e bën mbikëqyrjen jashtëzakonisht të vështirë. Ashtu si në mjedisin offline, nuk është as praktike dhe as e dëshirueshme që policia të jetë kudo, roli i "kujdestarit" duhet të ndahet me të tjerët në të gjithë komunitetin. Për shkak të natyrës globale dhe virtuale të krimeve kibernetike, shpesh është e vështirë të identifikohen autorët e krimeve të tilla dhe të vihen para drejtësisë.
- **Potenciali për dëme të konsiderueshme:** Krimet kibernetike mund të shkaktojnë dëme të konsiderueshëm për viktimat, si humbja e të dhënave, privatësia e kompromet uar, vjedhja e identitetit, humbja e parave dhe dëme të tjera ekonomike, dëmtimi i imazhit dhe reputacionit të kompanive dhe organizatave, e të tjera.
- **Evolucioni i vazhdueshëm:** Krimi kibernetik po evoluon vazhdimisht dhe autorët e këtyre veprave po zhvillojnë vazhdimisht metoda dhe teknika të reja për të kryer sulmet e tyre.

Përsa i përket formave të krimit kibernetik ato janë të ndryshme dhe gjithnjë në zhvillim, duke paraqitur sfida unike për profesionistët e zbatimit të ligjit dhe të sigurisë kibernetike. Një nga format më të zakonshme të krimit kibernetik është **hyrja e paautorizuar kompjuterike**, e cila përfshin marrjen e aksesit të paautorizuar në një sistem kompjuterik ose rrjet. Në ditët e para të informatikës, kjo vepër penale shpesh kryhej nga individë të cilët ishin të motivuar nga kurioziteti ose dëshira përtë shtyrë kufijtë e teknologjisë. Megjithatë, ndërsa sistemet kompjuterike janë bërë më komplekse dhe të sofistikuara, hyrja e paautorizuar kompjuterike ka evoluar në një aktivitet kriminal shumë më serioz dhe më të organizuar. Sot, autorët e kësaj vepre penale mund të përdorin një sërë teknikash, të tilla si inxhinieri sociale, thyerja e fjalëkalimit dhe malware, për të fituar akses në informacione të ndjeshme.

Një formë tjetër e zakonshme e krimit kibernetik është **malware,** i cili i referohet çdo lloj

softueri keqdashës që është krijuar, për të dëmtuar ose prishur një sistem ose rrjet kompjuterik. Malware mund të marrë shumë forma, si viruse dhe mund të përhapet në mënyra të ndryshme, duke përfshirë bashkëngjitjet e postës elektronike, faqet e internetit me qëllim të keq dhe shkarkimet e software-ve të infektuar. Malware, gjithashtu mund të aplikohet për të vjedhur informacione të ndjeshme, për të shkaktuar prishje të sistemit, ndërprerje, ose për të fituar akses të paautorizuar në rrjet.

Phishing, është një formë tjetër e zakonshme e krimit kibernetik, që përfshin mashtrimin e njerëzve për të zbuluar informacionin e tyre personal, si emrat e përdoruesve, fjalëkalimet dhe numrat e kartave të kreditit. Sulmet e phishing shpesh kryhen përmes postës elektronike, mediave sociale ose kanaleve të tjera digjitale dhe ato mund të jenë shumë bindëse, duke përdorur teknika të sofistikuara për të krijuar faqe interneti të rreme dhe emaile që duken të ligjshme. Pasi autori i këtij krimi të ketë marrë informacionin personal të viktimës, ai mund ta përdorë atë për një sërë qëllimesh si vjedhja e identitetit, mashtrimi me karta krediti ose lloje të tjera krimesh financiare.

Vjedhja e identitetit është një lloj tjetër i krimit kibernetik, i cili përfshin vjedhjen e informacionit personal të dikujt, si emrin, adresën apo të dhëna të tjera personale, dhe përdorimin e tij për të realizuar mashtrime ose krime të tjera. Vjedhja e identitetit mund të kryhet përmes një sërë mjetesh, të tilla si phishing, hakerim ose lloje të tjera taktikash inxhinierike sociale. Pasi autori i kësaj vepre të ketë marrë informacionin personal të viktimës, ai mund ta përdorë atë për të hapur llogari bankare, për të aplikuar për karta krediti ose për të kryer lloje të tjera mashtrimesh financiare.

Ngacmimi në rrjet është një tjetër lloj krimi kibernetik që është bërë gjithnjë e më i përhapur vitet e fundit. Ngacmimi kibernetik përfshin përdorimin e teknologjive digjitale, të tilla si mediat sociale, postën elektronik ose aplikacionet e mesazheve, për të ngacmuar, frikësuar ose kërcënuar dikë. Ngacmimi kibernetik mund të jetë veçanërisht tinëzar, pasi mund të kryhet në mënyrë anonime dhe mund të jetë i komplikuar për t'u gjurmuar. Ky lloj krimi kibernetik mund të sjellë pasoja serioze për viktimën, duke përfshirë traumën emocionale, depresionin dhe madje edhe vetëvrasjen.

KAPITULLI II

BASHKËPUNIMI NDËRKOMBËTAR NË LUFTËN KUNDËR KRIMIT KIBERNETIK

2.1 Krimi kibernetik në legjislacionin dhe praktikën ndërkombëtare

Krimi kibernetik është bërë një çështje kryesore në Bashkimin Evropian (BE) për shkak të ndikimit të tij negativ në aspekte të ndryshme të shoqërisë. Një nga arsyet pse krimi kibernetik është i rëndësishëm në BE është ndikimi i tij në ekonomi. Krimi kibernetik i kushton BE-së miliarda euro çdo vit, gjë që mund të ketë pasoja të rëndësishme për bizneset që operojnë brenda saj (Conti, 2014, pp. 44-45). Për të adresuar këtë çështje, BE-ja ka zbatuar një sërë masash si krijimi i Strategjisë së Sigurisë Kibernetike (European Commission, 2020), e cila synon të rrisë aftësitë e BE-së për sigurinë kibernetike, të rrisë ndërgjegjësimin për kërcënimet kibernetike dhe të promovojë bashkëpunimin midis shteteve anëtare, prezantimi i Direktivës për krimin kibernetik (Directive 2013/40/EU, 2013), e cila ka ofruar një kornizë për agjencitë e zbatimit të ligjit për të hetuar dhe ndjekur penalisht autorët e veprave penale me natyrë kibernetike. Për më tepër, BE-ja ka krijuar agjenci të specializuara si **Agjencia e Bashkimit Evropian për Sigurinë Kibernetike** (ENISA) dhe **Qendra Evropiane të Krimit Kibernetik** (EC3) për të rritur aftësitë e saj dhe për të parandaluar dhe luftuar krimin kibernetik. Këto agjenci punojnë së bashku me agjencitë e zbatimit të ligjit, bizneset dhe palët e tjera të interesuara për të zhvilluar strategji dhe iniciativa për të adresuar krimin kibernetik. Objekti i EC3 mbulon të gjitha ato krime që kryhen kundër të drejtave dhe privatësisë në internet, veçanërisht krimet kibernetike që lidhen me grupet e organizuara kriminale ose organizata të tjera. Si pasojë e dëmeve të shumta që i kanë shkaktuar njerëzimit, vendet dhe organizatat ndërkombëtare janë gjetur në pozitën e nevojës për të rregulluar krimet kompjuterike. Ndërsa është e vërtetë që disa vende po bëjnë përpjekje për t'i shmangur ato, sot ende nuk ka një kriter të unifikuar se si duhet të veprohet në rastet e sulmit kibenetik, kështu që është tejet e nevojshme që puna të vazhdojë për të unifikuar kriteret duke bërë të mundur një legjislacion koherent ndërkombëtar dhe duke angazhuar vendet.

Natyra e krimit kibernetik është transnacionale, pra do të thotë se është thelbësore të ketë dispozita që janë në përputhje në shtete të ndryshme. Në Evropë, takimi i parë i Këshillit

të Evropës i fokusuar në sektorin e Drejtësisë dhe Çështjeve të Brendshme, veçanërisht në krimet që lidhen me përdorimin e teknologjisë së informacionit, u mbajt në Tampere në vitin1999. Ishte gjatë kësaj kohe që u njoh rëndësia ndërkombëtare e krimit kibernetik e cila çoinë miratimin e Konventës së Budapestit nga Këshilli i Evropës më 23 nëntor 2001 (Council of Europe, Convention on Cybercrime, 2001). Kjo konventë konsiderohet si marrëveshja e parë ndërkombëtare për krimet e kryera nëpërmjet internetit ose rrjeteve elektronike. Këshilli Evropian miratoi gjithashtu Direktivën 2005/222/JHA (Council Framework Decision, 2005) të cilën e zhvillon dhe e zëvendëson Direktiva 2013/40/BE (Council Framework Decision, 2013) mbi sulmet kundër sistemve kompjuterike. Bashkimi Evropian po forcon vazhdimisht rregullat e tij për sigurinë kibernetike për të luftuar kërcënimin në rritje dhe për të përfituar nga mundësitë e epokës së re digjitale, duke pranuar mungesën e bashkëpunimit ndërkombëtarë në këtë fushë. Edhe OKB-ja nga ana tjetër pranon gjithashtu se ka disa probleme që pengojnë bashkëpunimin ndërkombëtar në këtë fushë. Këto përfshijnë mungesën e marrëveshjeve globale se cilat lloje sjelljesh duhet të përbëjnë krimet kompjuterike, përkufizimet ligjore të sjelljeve të tilla kriminale dhe ligje të specializuara kombëtare procedurale për hetimin e krimeve kompjuterike. Përveç kësaj, shumë krime të kryera nëpërmjet përdorimit të kompjuterëve kanë një natyrë transnacionale dhe mungojnë traktatet e ekstradimit, marrëveshjet e ndihmës reciproke, apo mekanizma të sinkronizuar për të mundësuar bashkëpunimin ndërkombëtar (A/RES/74/247, 2019).

2.1.1 Konventa e Budapestit

Konventa e Këshillit Evropian (Council of Europe, 2001) e njohur ndryshe si Konventa e Budapestit është një mjet vendimtar shumëpalësh në betejën kundër krimit kibernetik, pasi përcakton një standard të së drejtës penale të bazuar në parime dhe rregulla procedurale që kërkojnë arkivimin e përkohshëm të të dhënave që mund të përdoren si prova në ndjekjet penale. Edhe pse Konventa e Budapestit për Krimet Kibernetike e vitit 2001 konsiderohet si burimi më i plotë i informacionit mbi këtë temë dhe një ndryshim i madh në peizazhin evropian të krimit kibernetik, pasi ishte marrëveshja e parë për të rregulluar këtë lloj të ri krimi, është thelbësore të theksohet se përpjekjet për të rregulluar shkeljet e bazuara në kompjuter filluan shumë më herët. Në vitin 1976, Këshilli i Evropës mbajti një konferencë në Strasburg mbi kriminologjinë dhe krimet ekonomike, gjatë së

cilës u diskutuan në mënyrë të përgjithshme krimet e lidhura me kompjuterin. Më pas në vitin 1986 u shfaqën edhe Rekomandimet e OCSE-së (Schjolberg, 2008, p. 4), të cilat u krijuan për të luftuar krimet dhe abuzimet e bëra nëpërmjet përdorimit të teknologjisë së informacionit dhe prezantuan disa koncepte të reja si:

- **Mashtrimin elektronik** i cili përfshinte mashtrimin e dikujt duke përdorur mjete elektronike;
- **Falsifikim kompjuterik**, i cili përfshinte krijimin ose ndryshimin e të dhënave kompjuterike me qëllim kryerjen e mashtrimit;
- **Dëmtimi i software-ve**, i cili përfshin ndryshimin, fshirjen ose shkatërrimin e paautorizuar të software-ve të kërkuar për funksionimin e sistemeve kompjuterike;
- **Shkelje të të drejtave ekskluzive mbi programet dhe procesorët**, i cili përfshin kopjimi ose shpërndarjen e paautorizuar e software-ve.

Alexander Seger, Kreu i Divizionit të Krimeve Kibernetike, theksoi se konventa mbetet instrumenti ndërkombëtar më efikas, sinonim i vizionit të një interneti falas, informacioni qëmund të rrjedhë lirshëm, të konsultohet në mënyrë të sigurt dhe të pavarur për të kontestuarpërdorimin e paligjshëm (Arena, 2021, pp. 3-25).

Konventa është një bazë ligjore për bashkëpunimin ndërkombëtar dhe po zhvillohet vazhdimisht falë mundësisë që palët të shtojnë shënime udhëzuese dhe protokolle. Konventa duhet parë si një përpjekje e vërtetë "ndërkombëtare", jo ekskluzivisht evropiane, karakteristikë kjo që e bën këtë konventë akoma me prestigjoze. Aktualisht 68 shtete kanë nënshkruar Konventën, nga të cilat 65 e kanë ratifikuar atë. Prej tyre janë 47 vende janë anëtarë të Këshillit të Evropës, ndër to edhe Shqipëria (Council of Europe, 2001). Në terma të përgjithshëm, Konventa e Budapestit parashikon si objektiva kyçe kriminalizimin e sjelljeve kriminale, mjetet e së drejtës procedurale, për kryerjen e hetimeve për të luftuar krimin kibernetik dhe gjithashtu për të mundësuar një bashkëpunim efikas ndërkombëtar. Objektivi kryesor i Konventës përkrimin kibernetik, i cili paraqitet qartë në preambulën e kësaj konvente qëndron në nevojën për të futur një objektiv minimal për mbrojtjen e aseteve ligjore të prekura nga krimet kibernetike dhe një nivel të përbashkët minimal thelbësor të strategjive për të luftuar këto vepra (Council of Europe, 2001). Konventa është e përbërë nga 48 nene dhe është e organizuar në katër kapituj, ku secili i shërben një qëllimi të caktuar.

Ndryshimet dhe risitë më të rëndësishme të paraqitura nga Konventa për krimin kompjuterik gjenden në seksionin që ka të bëjë me ndihmën e ndërsjelltë. Kjo konventë në nenin 35 parashikon krijimin e një "task force", i cili operon 24 orë në ditë, shtatë ditë në javë, i njohur si "Rrjeti 24/7" (Council of Europe, 2001, Art.36). Rrjeti ndërkombëtar për kontrollin e krimit kompjuterik lindi nga nevoja për të mbajtur kontakte të vazhdueshme me shtetet për t'i ofruar ndihmë të menjëhershme hetimeve, si ditën ashtu edhe natën. Funksioni kryesor i këtij rrjeti është përmirësimi i mënyrave tradicionale të marrjes së ndihmës.

Një tjetër risi që ka sjellë Konventa e Budapestit është përfshirja e disa veprave të reja të krimit kibernetik. Konventa është amenduar disa herë për të përfshirë vepra të reja, siç janë veprat që lidhen me pornografinë e fëmijëve dhe vjedhjen e identitetit. Përfshirja e këtyre veprave të reja ka ndihmuar në ofrimin e një kuadri ligjor më gjithëpërfshirës për krimin kibernetik dhe ka lejuar vendet të trajtojnë kërcënimet kibernetike të reja dhe në zhvillim. Një tjetër zhvillim i ri që ka trajtuar Konventa e Budapestit është çështja e juridiksionit në hapësirën kibernetike. Konventa pranon se krimi kibernetik është një çështje globale që kërkon bashkëpunim dhe koordinim ndërkombëtar. Megjithatë, përcaktimi i juridiksionit në hapësirën kibernetike mund të jetë sfidues dhe Konventa ka zhvilluar udhëzime për të adresuar këtë çështje. Konventa parashikon gjithashtu asistencën reciproke juridike midis vendeve, e cila ka ndihmuar në lehtësimin e mbledhjes së provave elektronike dhe ndjekjen penale të shkelësve të krimit kibernetik përtej kufijve (Conti, 2014, p.44). Për më tepër, Konventa e Budapestit ka njohur gjithashtu rëndësinë e mbrojtjes së të drejtave dhe privatësisë individuale në luftën kundër krimit kibernetik. Konventa parashikon masa për mbrojtjen e të drejtave të individëve, siç është kërkesa për autorizim ligjor për përgjimin e komunikimeve dhe mbrojtjen e të dhënave personale. Përveç kësaj, Konventa e Budapestit ka njohur rëndësinë e partneritetit publik-privat në adresimin e krimit kibernetik. Konventa promovon bashkëpunimin ndërmjet agjencive të zbatimit të ligjit, qeverive dhe sektorit privat për të luftuar krimin kibernetik, duke pranuar se sektori privat ka një pasuri të ekspertizës dhe burimeve që mund të përdorenpër të trajtuar në mënyrë efektive krimin kibernetik.

Një protokoll shtesë iu shtua Konventës më 28 janar 2003 dhe hyri në fuqi më 1 mars 2006. Protokolli synon të zgjerojë më tej dispozitat e Konventës për krimin kibernetik duke kriminalizuar aktet e natyrës raciste dhe ksenofobike të kryera përmes sistemeve kompjuterike (Council of Europe, 2003). Kjo është në përputhje me parimet e të drejtave

të njeriut, të cilat mbështesin se të gjitha qeniet njerëzore janë të barabarta dhe se aktet raciste dhe ksenofobike përbëjnë shkelje të këtyre të drejtave. Protokolli i dytë shtesë i Konventës për krimin kibernetik, i cili u miratua më 12 maj 2022, trajton nevojën për bashkëpunim të zgjeruar dhe zbulimin e provave elektronike (Council of Europe, 2022). Ky protokoll krijon një kornizë ligjore për zbulimin e informacionit të regjistrimit të emrit të domenit dhe lehtëson bashkëpunimin e drejtpërdrejtë me ofruesit e shërbimeve për të marrë në mënyrë efektive informacionin. Ai përfshin gjithashtu dispozita për aksesin në informacionin dhe të dhënat, sigurimin e bashkëpunimit të menjëhershëm në situata emergjente, sigurimin e mjeteve të ndihmës reciproke dhe mbrojtjen e të dhënave personale.

2.1.2 Direktiva për sigurinë e rrjeteve dhe sistemeve të informacionit

Direktiva NIS (Direktiva për sigurinë e rrjeteve dhe sistemeve të informacionit) është një direktivë e Bashkimit Evropian që synon të rrisë nivelin e sigurisë kibernetike nëpër shtetet anëtare të BE-së (Directive EU, 2016). Kjo direktivë përcakton kërkesat e sigurisë për operatorët e shërbimeve dhe ofruesit e shërbimeve digjitale dhe u kërkon vendeve të BE-së të krijojnë strategji kombëtare të sigurisë së rrjetit dhe informacionit, të caktojnë autoritetet kompetente dhe të bashkëpunojnë për incidentet ndërkufitare të sigurisë kibernetike. Direktiva u miratua fillimisht në vitin 2016 dhe u zëvendësua me Direktivën (BE) 2022/2555, e cila synon forcimin dhe qëndrueshmërinë e Evropës ndaj sigurisë kibernetike.

Direktiva (BE) 2022/2555 kërkon që Shtetet Anëtare të miratojnë strategji kombëtare të sigurisë kibernetike dhe të krijojnë Autoritetet Kombëtare Kompetente (Directive (EU) 2022/2555, 2022). Gjithashtu përfshin masa për administrimin e rreziqeve të sigurisë kibernetike dhe detyrimet e raportimit për subjektet që operojnë në sektorë kritikë si kujdesi shëndetësor, si dhe kërkesat e shkëmbimit të informacionit dhe komunikimit për mbikëqyrjen e sigurisë kibernetike. Direktiva NIS 2 kërkon njoftim të menjëhershëm për CSIRT dhe autoritetet përkatëse për çdo incident që mund të ndikojë ndjeshëm në ofrimin e shërbimit.

2.2 Roli i NATO-s në luftën kundër krimit kibernetik

NATO (Organizata e Traktatit të Atlantikut të Veriut) është një aleancë ushtarake ndërqeveritare që u formua në vitin 1949 me nënshkrimin e Traktatit të Uashingtonit. Aktualisht ajo ka 31 vende anëtare dhe objektivi i saj kryesor është të sigurojë mbrojtjen kolektive të anëtarëve të saj kundër kërcënimeve të mundshme. Që nga fillimi i saj, NATO është përballur me sfida të ndryshme për strategjitë e saj të mbrojtjes, veçanërisht pasi natyra e luftës ka evoluar. Me rritjen e sulmeve kibernetike, NATO është përballur me mënyrën se si të formulojë një përgjigje kolektive ndaj kërcënimeve të tilla.

Sipas nenit 5 të Traktatit të Uashingtonit, një sulm i armatosur kundër çdo shteti anëtar konsiderohet një sulm kundër të gjithë anëtarëve dhe secili anëtar pritet të përgjigjet në përputhje me rrethanat (The North Atlantic Treaty, 1949, Article 5). Megjithatë, përkufizimi i një "sulmi të armatosur" është bërë i paqartë me përfshirjen e hapësirës kibernetike në ekuacion. Kjo ka ndezur një debat brenda NATO-s nëse një sulm kibernetik mund të konsiderohet një sulm i armatosur dhe se si vendet anëtare duhet t'i përgjigjen atij. Ndërsa NATO ka njohur kërcënimin e sulmeve kibernetike dhe ka riafirmuar politikën e saj të parandalimit, zbulimit, rimëkëmbjes dhe mbrojtjes në Deklaratën e Samitit të Uellsit, asaj ende i mungon një politikë e njohur publikisht për aktivitetet e hapësirës kibernetike, siç kërkohet sipas nenit 5. Neni 5 nuk përmend në mënyrë eksplicite sulmet kibernetike, por NATO nëpërmjet Sekretarit të Përgjithshëm, Stoltenberg ka pranuar se sulmet kibernetike mund të jenë po aq të rrezikshme sa sulmet fizike dhe ka treguar se një sulm i rëndë kibernetik mund të vër në lëvizje këtë nen (Stoltenberg, 2022).

Gjatë pesëmbëdhjetë viteve të fundit, qasja e NATO-s ndaj çështjeve kibernetike është zhvendosur nga fokusi teknik në atë strategjik. Udhëheqësit e aleancës fillimisht pranuan nevojën për të "forcuar aftësitë dhe mbrojtjen kundër sulmeve kibernetike" në vitin 2002, por vetëm në sulmet kibernetike të vitit 2007 ndaj Estonisë, NATO njohu potencialin e sulmeve kibernetike për t'u përdorur në konfrontimet shtetërore (Maigre, 2022, pp. 2-4). Në vitin 2008, në Samitin e Bukureshtit, NATO miratoi politikën e saj të parë të mbrojtjes kibernetike. Konflikti midis Rusisë dhe Gjeorgjisë më vonë theksojë potencialin që sulmet kibernetike të bëhen një komponent i rëndësishëm i luftës konvencionale (NATO, 2008). Ky evolucion në qasjen e NATO-s ndaj çështjeve

kibernetike pasqyron një njohje në rritje të rëndësisë strategjike të sigurisë kibernetike dhe nevojën për ta trajtuar atë në një kontekst më të gjerë sesa thjesht mbrojtje teknike.

Qendra e Ekselencës për Mbrojtjen Kibernetike të NATO-s (CCDCOE) u bë një Qendër Ekselence në vitin 2008 dhe që atëherë është rritur në një qendër ndërkombëtare për ekspertët e mbrojtjes kibernetike në të gjithë qeverinë, ushtrinë, industrinë dhe akademinë. CCDCOE-ja fokusohet në teknologjinë, strategjinë, operacionet dhe ligjin dhe projektet e tij përfshijnë stërvitjen më të madhe të mbrojtjes kibernetike në botë. Në vitin 2014, NATO krijoi gjithashtu edhe Bordin e Menaxhimit të Mbrojtjes Kibernetike (CDMB) për të mbikëqyrur aktivitetet e saj të mbrojtjes kibernetike, duke përfshirë mbrojtjen e rrjeteve dhe sistemeve të informacionit të NATO-s (North Atlantic Treaty Organisation CCDCOE, n.d.). CDMB-ja punon ngushtë me vendet anëtare të NATO-s dhe partnerë të tjerë për të koordinuar përpjekjet për zbulimin, parandalimin dhe reagimin ndaj sulmeve kibernetike. NATO gjithashtu kryen ushtrime të mbrojtjes kibernetike për të testuar dhe përmirësuar aftësinë e saj për t'iu përgjigjur kërcënimeve kibernetike. Këto ushtrime përfshijnë sulme të simuluara ndaj rrjeteve dhe sistemeve të NATO-s dhe ndihmojnë në identifikimin e dobësive në mbrojtjen kibernetike të NATO-s. Për më tepër, NATO ka zhvilluar një sërë standardesh të mbrojtjes kibernetike, të njohura si Politika e Mbrojtjes Kibernetike e NATO-s, e cila ofron udhëzime për vendet anëtare të NATO-s se si të mbrojnë rrjetet dhe sistemet e tyre nga kërcënimet kibernetike (North Atlantic Treaty Organization, 2021). Përveç kësaj, NATO ka krijua partneritete me organizata të tjera, si Agjencia e Bashkimit Evropian për Sigurinë Kibernetike (ENISA), për të ndarë informacionin dhe për të koordinuar përpjekjet për të luftuar krimin kibernetik (Purser, 2014, pp. 101-104).

Në vitin 2014, NATO njoftoi se kishte përditësuar politikën e saj të mbrojtjes kibernetike për të sqaruar se një sulm kibernetik mund të konsiderohet si një "shkaktues i mundshëm" për Nenin 5. Megjithatë, vendimi për të thirrur nenin 5 në përgjigje të një sulmi kibernetik do të përcaktohet nga një sërë faktorësh, duke përfshirë natyrën dhe ashpërsinë e sulmit, atribuimin e sulmit dhe nivelin e dëmit të shkaktuar. Në praktikë, ka të ngjarë që NATO të shqyrtojë me kujdes situatën dhe të konsultohet me vendet e saj anëtare përpara se të vihet në lëvizje Nenin 5, si një përgjigje ndaj një sulmi kibernetik. Por, mungesa e standardeve të paracaktuara për vlerësimin e sulmeve kibernetike e bën sfiduese për vendet anëtare që të përgjigjen në mënyrë uniforme ndaj kërcënimeve të tilla. Në mungesë të një politike të qartë, vendet anëtare kanë lirinë për t'iu përgjigjur sulmeve

kibernetike siç e shohin të arsyeshme, bazuar në kriteret e tyre të brendshme për t'iu kundërvënë kërcënimeve të tilla. Kjo mund të çojë potencialisht në konflikte midis vendeve anëtare dhe të minojë fuqinë e aleancës. Për të adresuar këtë çështje, NATO duhet të miratojë një standard uniform për vlerësimin dhe reagimin ndaj sulmeve kibernetike për të siguruar një përgjigje kolektive dhe të koordinuar. Pranimi i një standardi të tillë do të parandalonte konfliktet e brendshme dhe do të siguronte qartësi për vendet anëtare se si t'i përgjigjen kërcënimeve të tilla.

2.3 Krimi kibernetik si krim me natyrë ndërkombëtare

Ndodhitë e fundit kanë treguar se sulmet kibernetike mund të përbëjnë një kërcënim të rëndësishëm për paqen dhe sigurinë ndërkombëtare. Mënyra se si funksionojnë operacionet sulmuese në hapësirën kibernetike krijon sfida unike jo vetëm për shtetin, por dhe për të drejtën ndërkombëtare. Aktualisht është rënë dakord që në fushën e krimeve kibernetike të zbatohet ligji ndërkombëtar duke anashkaluar disi pjesën nëse këto sulme duhet ose jo të konsiderohen krime themelore sipas Ligjit Penal Ndërkombëtar (Chawki, Darwish, Khan, & Tyagi, 2015). Gjykata Ndërkombëtare Penale (GJNP) është një gjykatë e mundësisë së fundit që ndjek penalisht individët për krimet më të rënda që shqetësojnë komunitetin ndërkombëtar. Juridiksioni i GJNP-së është i kufizuar në katër lloje krimesh: gjenocidi, krimet kundër njerëzimit, krimet e luftës dhe krimi i agresionit. Aktualisht, sulmet kibernetike nuk njihen si krime themelor nga kjo gjykatë. Megjithatë, kjo nuk do të thotë domosdoshmërisht se ato nuk mund të ndiqen penalisht nga GJNP. Sulmet kibernetike që rezultojnë në kryerjen e gjenocidit, krimeve kundër njerëzimit ose krimeve të luftës mund të ndiqen penalisht nga GJNP nën juridiksionin e saj ekzistues. Thënë kjo, zhvillimi i luftës kibernetike dhe përdorimi i sulmeve kibernetike për të arritur objektivat politike dhe ushtarake ka ngritur shqetësime për përshtatshmërinë e ligjeve dhe normave ndërkombëtare aktuale në adresimin e këtij lloji të ri kërcënimi.

Disa ekspertë juridik argumentojnë se sulmet kibernetike duhet të konsiderohen një formë agresioni dhe duhet të përfshihen në përkufizimin e krimit të agresionit sipas Statutit të Romës, i cili është traktati që themeloi GJNP-në (De Vito, 2020). Nëse sulmet kibernetike do të përfshiheshin në përkufizimin e krimit të agresionit, kjo do t'i jepte

GJNP-së juridiksionin për të ndjekur penalisht individët përgjegjës për sulme të tilla. Megjithatë, kjo është një çështje komplekse që ngre shumë sfida politike dhe ligjore. Mbetet për t'u parë nëse sulmet kibernetike do të klasifikohen si një krim themelor nga GJNP-ja ose nëse do të zhvillohen korniza të reja ligjore për të adresuar këtë kërcënim në rritje.

Mungesa e një përkufizimi të qartë dhe ezaurues midis "kërcënimi i përdorimit të forcës" apo "përdorimi i forcës" në Kartën e OKB-së sjell si pasojë një vështirësi në interpretim e krimit kibernetik. Për të shmangur këtë paqartësi Asambleja e Përgjithshme e OKB-së më 14 dhjetor 1974 me anë të Rezolutës nr. 3314 përkufizoi termin "forcë" si forcë e armatosur (UN General Assembly, 1974). Ndërkaq, Gjykata Ndërkombëtare e Drejtësisë pohon si opinion këshillues se neni 2(4) i Kartës së Kombeve të Bashkuara zbatohet për çdo përdorim të forcës, pavarësisht nga armët ose mjetet e përdorura. Prandaj, trajtimi i disa sulmeve kibernetike si ekuivalente me përdorimin e forcës së armatosur i mundëson Këshillit të Sigurimit të OKB-së të veprojë sipas Kapitullit VII dhe shteteve të reagojnë në vetëmbrojtje sipas nenit 51 të Kartës së OKB- së (Legality of the Threat or Use of Nuclear Weapons, 1996, p. 226).

2.3.1 Lufta kibernetike, instrumenti i luftrave në të ardhmen

Hapësira kibernetike është shfaqur si një fushë beteje e re në epokën moderne dhe ekziston një shqetësim në rritje se ajo mund të bëhet një instrument kritik lufte në të ardhmen. Hapësira kibernetike zotëron në vetvete dy karakteristika të veçanta: ajo mund të kuptohet si mjet teknologjik përmes të cilit zhvillohen ndërveprimet njerëzore, gjithashtu ajo vepron si një rrugë tranziti për përdoruesit duke mundësuar një lidhje planetare (Taddei, 2015). Në të njëjtën kohë megjithatë, hapësira kibernetike me përhapjen e saj globale nuk është e imunizuar nga krijimi i kërcënimeve ndaj sigurisë kombëtare (Martino, n.d., p. 5). Lufta kibernetike përfshin përdorimin e teknologjisë së informacionit për të nisur sulme ndaj sistemeve kompjuterike, rrjeteve dhe infrastrukturës. Gjithashtu duhet përcaktuar se termi "luftë" edhe në dimensionin kibernetik ka nevojë për elementë dhe qëllime shtrënguese dhe shkatërruese, më saktë, lufta kibernetike do të konsistonte në "një veprim të një shteti të aftë për të depërtuar në sistemet kompjuterike ose rrjetet e një shteti tjetër me qëllim dëmtimin ose shkatërrimin

e tij”.

Rëndësia e hapësirës kibernetike si një instrument lufte qëndron në aftësinë e saj për t'i siguruar një sulmuesi anonimitetin, shpejtësinë dhe mohimin. Sulmet kibernetike mund të nisen nga kudo në botë dhe mund të jetë sfiduese t'i atribuohet një entiteti ose shteti specifik. Kjo e bën atë një opsion tërheqës për aktorët shtetërorë dhe jo shtetërorë që dëshirojnë të përfshihen në veprime agresive pa u mbajtur përgjegjës. Lufta kibernetike mund të konsiderohet si kufiri i ri i luftës. Hapësira kibernetike pranë tokës, ajrit, detit dhe hapësirës së jashtme, domenet tradicionale të luftës, përfaqëson sot “dimensionin e pestë të konfliktit” (Martino, n.d., p. 5).

Potenciali që lufta kibernetike të bëhet një instrument i rëndësishëm lufte në të ardhmen është një shqetësim në rritje për shumë vende. Ndërsa vendet bëhen më të varura nga teknologjia dhe digjitalizimi, ato bëhen më të prekshme ndaj sulmeve kibernetike. Kjo dobësi e bën të rëndësishme për vendet që të zhvillojnë aftësinë për t'u mbrojtur kundër sulmeve kibernetike dhe për të penguar sulmuesit e mundshëm. Përdorimi i hapësirës kibernetike si instrument lufte ngre pyetje të rëndësishme ligjore dhe etike. Kjo paqartësi mund të çojë në një përshkallëzim të rrezikshëm të konfliktit kibernetik dhe ka potencialin të shkaktojë dëme të konsiderueshme për civilët. Hapësira kibernetike nuk duhet të konsiderohet më si e kufizuar në fokusin e saj parësor pra, lehtësimin e disa aktiviteteve të përditshme, por duhet rishqyrtuar pasi ajo është krijuar tashmë në të gjitha aspektet si një "mjedis strategjik" i ri dhe si e tillë duhet të trajtohet nga analistë dhe politik-bërësit.

Një shembull aktual për sa i përket këtij argumenti është dhe sulmi kibernetik që pësojë **Ukraina nga Rusia**. Operacionet kibernetike në dhe kundër Ukrainës kanë qenë një tipar i spikatur i konfliktit të vazhdueshëm midis Ukrainës dhe Rusisë. Që nga fillimi i konfliktit në vitin 2014, të dyja palët janë angazhuar në një sërë operacionesh kibernetike, duke përfshirë spiunazhin, fushatat e dezinformimit dhe sulmet përçarëse në infrastrukturën kritike. Një nga incidentet më të rëndësishme kibernetike në konflikt ishte sulmi *NotPetya* (NotPetya 2017) në 2017, i cili preku mijëra kompjuter në Ukrainë dhe në mbarë botën. Sulmi iu atribua Rusisë dhe shkaktoi dëme të konsiderueshme në infrastrukturën kritike, duke përfshirë bankat, aeroportet dhe rrjetet e energjisë (Sari, 2023, pp. 3-4). Rusia është akuzuar gjithashtu për përdorimin e operacioneve kibernetike për të ndërhyrë në proceset politike të Ukrainës, përfshirë zgjedhjet presidenciale të vitit

2019. Këto operacione kanë përfshirë përhapjen e lajmeve të rreme dhe dezinformatave përmes mediave sociale dhe platformave të tjera online. Që nga shkurti i vitit 2022, në Ukrainë si rrjetet private, ashtu edhe ato publike janë shënjestruar në mënyrë të vazhdueshme (Sari, 2023, p.4). Ndërsa shumë nga këto operacione kanë qenë të lidhura me grupe pro-ruse dhe autoritetet ruse, duhet theksuar se qeveria ruse ka mohuar përfshirjen e saj. Ukraina u është përgjigjur këtyre kërcënimeve kibernetike duke zhvilluar aftësitë e saj të sigurisë kibernetike dhe duke punuar ngushtë me partnerët ndërkombëtarë, përfshirë NATO-n dhe Bashkimin Evropian. Konflikti i vazhdueshëm kibernetik në Ukrainë thekson rëndësinë në rritje të hapësirës kibernetike si një fushë lufte dhe nënvizon nevojën që vendet të zhvillojnë masa të fuqishme të sigurisë kibernetike për t'u mbrojtur kundër sulmeve kibernetike dhe për të vendosur norma dhe ligje të qarta rreth luftës kibernetike për të parandaluar keqpërdorimine saj.

Gjithashtu duke u larguar nga rrethanat specifike të konfliktit në Ukrainë, del në pah fakti se pushtimi në shkallë të plotë i Rusisë u parapri nga operacionet kibernetike që synonin formimin e hapësira të betejës duke theksuar se sulmet kibernetike mund të kalojnë vijën midis luftës dhe paqes.

KAPITULLI III

KRIMI KIBERNETIK NË SISTEMIN JURIDIK TË REPUBLIKËS SËSHQIPËRISË

3.1 Krimi kibernetik në Republikën e Shqipërisë

Krimi kibernetik si një çështje shumë e rëndësishme në shumë shtete, për shkak se vendi po bëhet gjithnjë e më i varur nga teknologjia, është kthyer në një shqetësim edhe në Republikën e Shqipërisë, e cila është edhe më e ndjeshme ndaj këtyre sulmeve, kjo pasi ka mungesë në infrastrukturën mbrojtëse në teknologji dhe informacion. Qeveria shqiptare e ka njohur krimin kibernetik si problem dhe ka bërë disa përpjekje për të trajtuar kërcënimin në rritje tëkrimit kibernetik, duke miratuar një sërë ligjesh, siç janë (Shkembi, 2015, p. 92):

- Ligji Nr.7895, datë 27.01.1995, "Kodi Penal i Republikës së Shqipërisë";
- Ligji Nr.9887, datë 10.03.2008, "Për Mbrojtjen e të Dhënave Personale";
- Ligji Nr.9880, datë 25.2.2008 “Për Nënshkrimin Elektronik “i ndryshuar”,
- Ligji Nr.9918, datë 19.05.2008, "Për komunikimet elektronike në Republikën e Shqipërisë";
- Ligji Nr.107, datë 15.10.2015,"Për identifikimin elektronik dhe shërbimet e besuara", i ndryshuar;
- Ligji Nr.2/2017, "Për sigurinë kibernetike";
- Ligji Nr.10/2023 “Për Informacionin e Klasifikuar”.

Edhe pse Shqipëria ka një kuadër ligjor, krimi kibernetik po kthehet në një problem serioz për vendin duke e bërë sigurinë e secilit prej nesh lehtësisht të cënueshme.

Mashtrimi online, duke përfshirë mashtrimet e phishing dhe vjedhjen e identitetit, është një nga kategoritë më të përhapura të krimit kibernetik në Shqipëri. Sulmet ransomware, në të cilat autorët e veprave penale me natyrë kibernetike kërkojnë pagesë në këmbim të rifitimit të aksesit në sistemet e rrëmbyera, synojnë gjithashtu organizata dhe individë.

Për hetimin dhe luftimin e krimit kibernetik, qeveria shqiptare ka ngritur pranë Policisë së Shtetit një njësi të dedikuar kundër krimit kibernetik. Shqipëria është gjithashtu anëtare e Qendrës Evropiane të Krimit Kibernetik të Bashkimit Evropian (EC3) dhe ka punuar me shtete të tjera në rajon për të luftuar krimin kibernetik. Megjithatë, nevojitet më shumë punë për të rritur ndërgjegjësimin dhe edukimin e shoqërisë shqiptare dhe sipërmarrjeve për rrezikun qëna vjen nga krimi kibernetik dhe nevojën për sigurinë kibernetike.

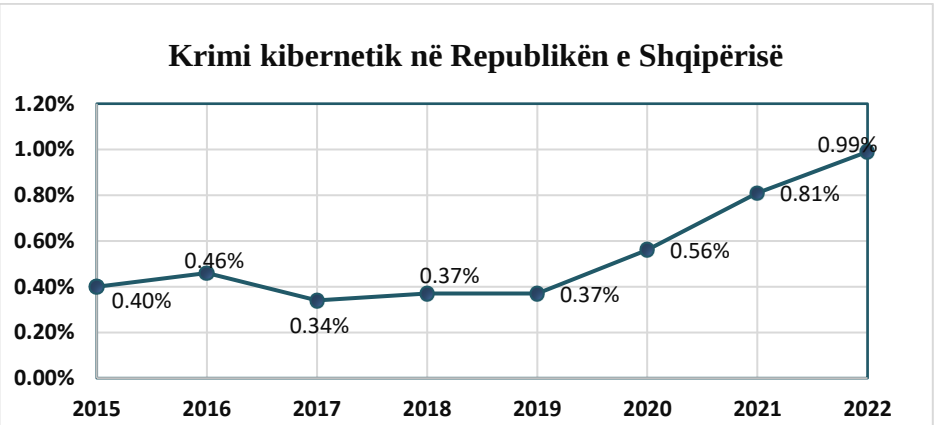
Republika e Shqipërisë, si një vend në zhvillim, investon në teknologjinë e informacionit si një mjet për të përmirësuar nivelin e jetesës dhe ofrimin e shërbimeve publike. Por, megjithëse përdorimi i teknologjive digjitale të reja sjell përparësi dhe përfitime të mëdha, ka edhe sfida në fushën e sigurisë kibernetike, pasi shfrytëzon dobësitë e këtyre sistemeve. Shqipëria është angazhuar për të përmirësuar situatën e sigurisë kibernetike, ndërsa në fushën e teknologjisë së informacionit dhe revolucionit mbi digjitalizimin e shërbimeve publike, ka hartuar një kuadër ligjor që i përshtatet nevojave aktuale.

Shqipëria është përmirësuar në Indeksin Global të Sigurisë Kibernetike krahasuar me vitin 2017, duke u renditur nga vendi i 89-të, në vendin e 62-të, në mbarë botën dhe në vendin e 36 në nivel Evropian (Vendimi nr. 1084, 2020). Për sa i përket Republikës së Shqipërisë duke u bazuar në të dhënat e Raportit të Prokurorit të Përgjithshëm mbi gjendjen e kriminalitetit në Shqipëri për vitin 2022, pesha që zë krimi kibernetik në numrin total të procedimeve penale të regjistruara në shkallë vendi është 0,99 % (Prokuroria e Përgjithshme, 2022, pp.173-176). Pavarësisht peshës së vogël në raport me veprat e tjera penaleështë i dukshëm trendi në rritje i veprave të krimit kibenetik ndër vite.

Sipas **Figurës 1**, tendenca tregon një rritje të qëndrueshme të përqindjes së krimit kibernetiknë Shqipëri ndër vite, me një rritje të konsiderueshme në vitin 2021 dhe në vitin 2022. Nga viti 2015 në 2016, ka pasur një rritje modeste prej 0.06%, që tregon një zhvendosje graduale drejt krimit kibernetik. Përqindja e rritjes ra pak në vitin 2017 në masën 0.34%, por mbeti relativisht e qëndrueshme në vitin 2018 dhe në vitin 2019 në masën 0.37%. Në vitin 2020, pati një rritje të dukshme krahasuar me vitet paraardhëse, që shkon në masën 0.56%, dhe nëvitin 2021, përqindja u dyfishua në masën 0.81%.
Ky trend rritje domethënës mund t'i atribuohet pandemisë COVID-19, e cila detyroi shumë individë dhe organizata të mbështeten më shumë në teknologjitë digjitale. Rritja e aktivitetitnë internet u dha më shumë mundësi autorëve të veprave penale me natyrë

kibernetike për të kryer aktivitetet e tyre të paligjshme. Rritja në masën 0.99% në vitin 2022 është një tregues që krimi kibernetik mbetet një shqetësim në rritje në Shqipëri, që kërkon një reagim të menjëhershëm të strukturave politik bërëse dhe ligj zbatuese që jo vetëm ta adresojnë këtë çështje me seriozitetin që i takon, por edhe të marrin masa si në planin e brendshëm ashtu edhe në atë ndërkombëtarë.

Figura 1



3.2 Parashikimet e veprave me natyrë kibernetike në Kodin Penal

Kodi Penal i Republikës së Shqipërisë parashikon në disa nene të tij edhe veprat penale me natyrë kibernetike, të cilat nuk janë të përmbledhura në një seksion të posaçëm, por gjatë leximit të kodit, mund t'i gjejmë në nenet:

- **Neni 74/a - Shpërndarja kompjuterike e materialeve pro gjenocidit ose krimeve kundër njerëzimit**

Ky nen është një dispozitë e shtuar me ligjin Nr.10 023 të vitit 2008 (Kodi Penal, neni74/a). Dispozita ka të bëjëme shpërndarjen kompjuterike të materialit që promovon ose justifikon akte që përbëjnë gjenocid ose krime kundër njerëzimit. Kjo dispozitë penalizon dy lloje sjelljesh: ofertën publike dhe shpërndarjen e qëllimshme për publikun nëpërmjet sistemeve kompjuterike. Materialet e shpërndara duhet të mohojnë, minimizojnë, miratojnë ose justifikojnë aktet që përbëjnë gjenocid ose krime kundër njerëzimit në një mënyrë të ndjeshme. Në përgjithësi, kjo dispozitë tregon se Shqipëria mban një qëndrim të fortë kundër promovimit ose justifikimit të akteve që përbëjnë gjenocid ose krime kundër njerëzimit. Ai njeh gjithashtu rëndësinë e rregullimit të aktiviteteve në internet dhe parandalimin e shpërndarjes së materialeve të dëmshme

nëpërmjet sistemeve kompjuterike.

- **Neni 84/a - Kanosja me motive racizmi dhe ksenofobie nëpërmjet sistemit kompjuterik**

Kjo dispozitë e shtuar rishtazi me ligjin Nr.10 023 të vitit 2008, trajton kërcënimet racore dhe ksenofobike të bëra nëpërmjet sistemeve kompjuterike (Kodi Penal, neni 84/a). Në këtë nen parashikohet se kërcënimet serioze për të vrarë ose për të plagosur rëndë një person në bazë të përkatësisë etnike, kombësisë, racës ose fesë, të bëra nëpërmjet sistemeve kompjuterike dënohen me gjobë ose me burgim deri në tre vjet. Kjo dispozitë njeh efektet e dëmshme të kërcënimeve racore dhe ksenofobike dhe tregon se qeveria shqiptare i merr seriozisht këto kërcënime. Duke e kriminalizuar këtë sjellje, dispozita njeh nevojën për të rregulluar aktivitetin online dhe për të parandaluar përhapjen e mesazheve të dëmshme. Është e nevojshme të theksohetse dispozita nuk kërkon që të ndodhë dëmi ose lëndimi aktual. Vetë akti i bërjes së një kërcënimi serioz bazuar në përkatësinë etnike, kombësinë, racën ose fenë e një personi është mjaftueshëm për të garantuar dënimin. Kjo dispozitë gjithashtu pasqyron rëndësinë në rritjetë rregullimit të aktivitetit në internet dhe garantimit që interneti të mos përdoret si mjet përpërhapjen e gjuhës së urrejtjes dhe mesazheve diskriminuese

- **Neni 119/a/b - Shpërndarja e materialeve raciste ose ksenofobike nëpërmjet sistemit kompjuterik**

Ky nen fokusohet në shpërndarjen e materialeve raciste ose ksenofobike nëpërmjet sistemeve kompjuterike duke konsideruar si vepër penale ofrimin ose shpërndarjen e qëllimshme të përmbajtjes raciste ose ksenofobike përmes sistemeve kompjuterike. Përdorimi i sistemeve kompjuterike në këtë dispozitë është i rëndësishëm, pasi njeh rolin në rritje të teknologjisë në përhapjen e gjuhës së urrejtjes dhe mesazheve diskriminuese. Është e rëndësishme të theksohet se dispozita fokusohet veçanërisht në shpërndarjen e materialeve me përmbajtje raciste ose ksenofobike. Kjo njeh dëmin e shkaktuar nga mesazhe të tilla dhe nevojën për t'i adresuar ato përmes mjeteve ligjore.

- **Neni 143/b - Mashtrimi kompjuterik**

Ky nen sanksionon veprën penale të mashtrimit kompjuterik, që përfshin veprime të caktuara të kryera me qëllim të përfitimit ekonomik, me anë të mashtrimit ose dëmtimit të të tjerëve. Këto veprime përfshijnë futjen, ndryshimin, fshirjen ose heqjen e të dhënave

kompjuterike ose ndërhyrjen në funksionimin e një sistemi kompjuterik.

- **Neni 186/a - Falsifikimi kompjuterik**

Ky nen parashikon veprën penale të manipulimit të të dhënave kompjuterike. Në mënyrë të veçantë, i referohet futjes, ndryshimit ose fshirjes së të dhënave kompjuterike pa të drejtë për ta bërë këtë. Kjo shkelje bëhet më e rëndë kur të dhënat e manipuluara përdoren si të dhëna autentike. Kjo dispozitë njeh rëndësinë e integritetit dhe besueshmërisë së të dhënave dhe e konsideron ndërhyrjen e të dhënave kompjuterike si një shkelje të rëndë.

- **Neni 192/b - Hyrja e paautorizuar kompjuterike**

Kjo dispozitë e Kodit Penal sanksionon veprën penale të aksesit të paautorizuar në kompjuter. Kjo vepër kryhet kur dikush hyn ose tejkalon aksesin e autorizuar në një sistem kompjuterik, ose një pjesë të tij, në kundërshtim me masat e tij. Qëllimi i këtij neni është të mbrojë sistemet e rëndësishme kompjuterike nga aksesi i paautorizuar, i cili potencialisht mund të shkaktojë dëm serioz për sigurinë kombëtare, rendin publik ose shëndetin publik.

- **Neni 293/a/b/c/ç - Përgjimi i paligjshëm i të dhënave kompjuterike**

Ky nen ka të bëjë me përgjimin e paligjshëm të të dhënave kompjuterike. Kjo dispozitë parashikon se përgjimi i të dhënave të tilla me mjete teknike, përfshirë emetimet elektromagnetike nga një sistem kompjuterik, dënohet me burgim. Ashpërsia e dënimit rritet nëse vepra kryhet brenda ose kundër disa sistemeve kompjuterike me rëndësi publike. Gjithashtu, thekson rëndësinë e privatësisë dhe sigurisë së të dhënave në epokën digjitale. Ky nen njeh natyrën serioze të përgjimit të të dhënave kompjuterike dhe synon të pengojë individët nga përfshirja në aktivitete të tilla të paligjshme. Pra, mund të themi se neni në fjalë shërben si një kujtesë se mbrojtja e të dhënave kompjuterike është thelbësore për ruajtjen e integritetit dhe sigurisë së sistemeve kompjuterike dhe informacionit që ato përmbajnë.

Pika b, e këtij neni ka të bëjë me veprën penale të ndërhyrjes në të dhënat kompjuterike. Sipas këtij neni, çdo veprim i paautorizuar që shkakton dëmtim, shtrembërim, ndryshim, fshirje të të dhënave kompjuterike dënohet me burgim. Nëse kjo vepër kryhet në disa lloje të dhënash kompjuterike, si ato që lidhen me fushën ushtarake, sigurinë kombëtare, rendin publik, shëndetësinë, mbrojtjen civile, ose çdo të dhënë tjetër kompjuterike me rëndësi publike, dënimi është më i rëndë.

Në pikën c, të nenit 293 trajtohen ndërhyrjet në sistemet kompjuterike duke parashikuar se krijimi i pengesave të rënda dhe të paautorizuara për të dëmtuar funksionimin e një sistemi kompjuterik nëpërmjet veprimeve të tilla si futja, shtrembërimi, dëmtimi, ndryshimi ose fshirja e të dhënave është vepër penale e dënueshme me burg.

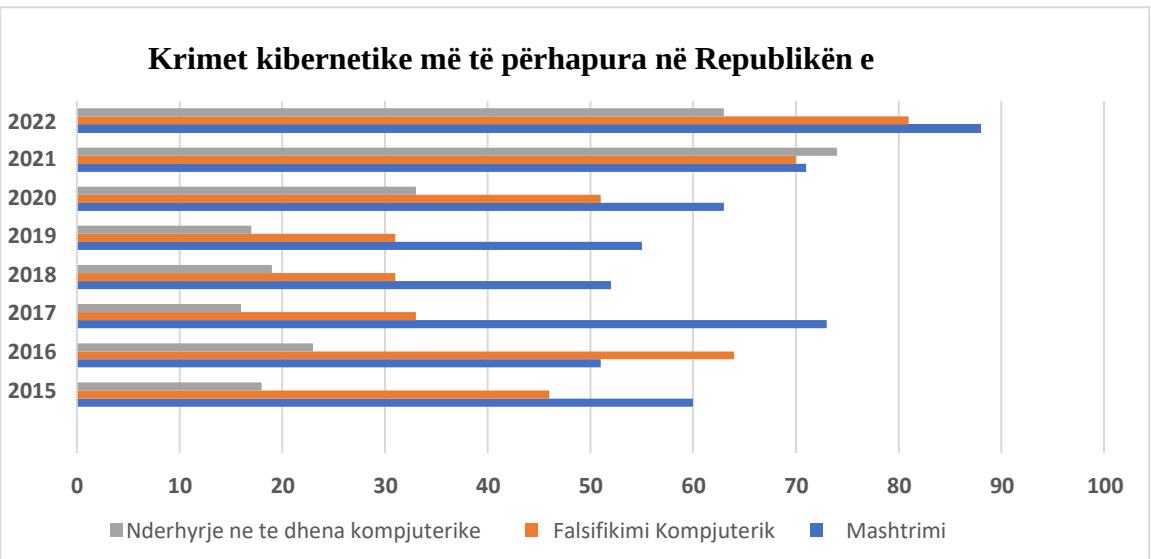
Në germën ç, neni 293 fokusohet në veprën penale të keqpërdorimit të pajisjeve në kuadër të krimit kibernetik. Ky nen targeton individët që prodhojnë, mbajnë, shesin, shpërndajnë ose vënë në përdorim një pajisje, program kompjuterik, fjalëkalim, kod aksesi ose të dhëna të ngjashme që synojnë akses të paautorizuar në një sistem kompjuterik ose një pjesë të tij.

Mbështetur në Raportet e Prokurorisë të Përgjithshëm mbi gjendjen e kriminalitetit në Shqipëri ndër vite vërehet se numri i veprave penale karakteristike të krimit kibernetik të raportuara ka luhatje ndër vite, por ka shfaqur një tendencë të përgjithshme rritëse. Duke analizuar veprat penale për (Prokuroria e Përgjithshme, 2022, pp173-176):

1. Mashtrim kompjuterik
2. Falsifikim Kompjuterik
3. Ndërhyrje në të dhëna kompjuterike

Siç ilustrohet edhe në **Figurën 2**, veprat e sipërpërmendura rezultojnë të jenë një çështje shqetësuese në Shqipëri dhe se numri i tyre është rritur me kalimin e viteve. Gjithashtu vlen të theksohet se këto të dhëna përfaqësojnë vetëm rastet e raportuara dhe mund të mos japin një pamje të plotë të përhapjes së krimit kibernetik në vend.

Figura 2



3.3 Sulmi kibernetik i 15 korrikut 2022 në Republikën e Shqipërisë

Më datë 15 korrik 2022 Republika e Shqipërisë u përball me një sulm kibernetik tejet serioz,i cili goditi shumë sisteme qeveritare pranë AKSHI-t me qëllim fshirjen e tyre. Në orën 13:00, platformat e sigurisë identifikuan fillimin e shpërndarjes së një sulmi DoS në rrjet, që preku disa institucione. Pas identifikimit të këtij sulmi, u ndërmorën menjëherë masat e bllokimit, për të parandaluar përhapjen dhe u ngrit një rast emergjence me ekspertëte Microsoft në nivelin më lartë të reagimit ndaj sulmeve kibernetike, njohur si "Crisis Case" (Raporti i plotë i sulmit kibernetik të 15 korrikut 2022). Gjatë bashkëbisedimeve të vazhdueshme me ekipin e sigurisë, inxhinierët e ekipit rekomanduan aktivizimin e një opsioni shtesë për reagim në raste sulmesh kibernetike. Ky veprim lejoi zbulimin e autorëve të krimit kibernetik një ditë më vonë, më datë 16 korrik. Pas identifikimit të tyre, u arrit gjithashtu bllokimi i përhapjes së sulmit dhe izolimi i të gjitha sistemeve për të parandaluar dëmet e mëtejshme. Ekipi i Detektimit dhe Reagimit të Microsoft (DART) dhe Ekipi investigativ i krimit kibernetik të FBI-së kryen një investigim duke i ardhur në ndihmë vendit tonë dhe duke arritur në konkluzionin për datën e infiltrimit të aktorëve keqbërës, dhe duke identifikuar vulnerabilitetin e sistemit administrata.al. (Raporti i plotë i sulmit kibernetik të 15 korrikut 2022).

Ky sulm vuri në pah dhe vulnerabilitetin e sistemeve qeveritare duke e ndërgjegjësuar më shumë atë. Ndërgjegjësim ky i cili nuk mjaftoj pasi pak muaj më vonë në datë 9 shtator 2022, vendi ynë u përball me një tjetër sulm. Këtë herë target ishte Drejtoria e Përgjithshme e Policisë së Shtetit, një organ thelbësor në strukturat shtetërore. Sipas raportit të dhënë nga Microsoft DART dhe ekipi investigativ i krimit kibernetik të FBI, ngjarjet dhe kohëzgjatja e sulmit të 15 korrikut nuk lidhet me sulmin e 9 shtatorit ndaj sistemeve dhe infrastrukturave të Drejtorisë së Përgjithshme të Policisë së Shtetit (Raporti i plotë i sulmit kibernetik të 15 korrikut 2022). Konsiderohen dy sulme të ndryshme, me origjinë dhe karakteristika të ndryshme, ndaj dy institucioneve të palidhura me njëra-tjetrën. Këto dy sulme kanë sjell shtimin e vëmendjes për rëndësinë e masave parandaluese dhe rrezikshmërinë e këtyre sulmeve. Aktualisht falë angazhimit të ekipeve të Microsoft-it si DART-i është bërë e mundur rikuperimi i të dhënave dhe funksionimi i portaleve. Kjo situatë duhet të jetë një mësim dhe për organet shtetërore të cilët jo vetëm duhet të marrin masat për të rritur sigurinë në rrjet, por edhe për ndërgjegjësimin e

shoqërisë mbi rrezikshmërinë e krimit kibernetik. Qeveria shqiptare pas këtyre konkluzioneve deklarojë seky sulm keqbërës është kryer nga hakerues iranian, qëndrim ky që u mbështet edhe nga SHBA dhe BE. Për këtë çështje, pranë Gjykatës së Shkallës së Parë Tiranë është regjistruar një procedim penale, për veprat penale:

1. "Përgjim i paligjshëm i të dhënave kompjuterike";
2. "Ndërhyrja në të dhënat kompjuterike";
3. "Ndërhyrja në Sistemet kompjuterike";
4. "Keqpërdorimi i pajisjeve".

Vepra këto të të parashikuara nga nenet 293/a, 293/b, 293/c dhe 293/ç, të Kodit Penal. Siç deklarohet në deklaratën për shtyp të Prokurorisë së Përgjithshme, të dy sulmet kibernetikë të ndodhura në 15 korrik dhe 9 shtator 2022, kanë të njëjtën natyrë dhe kanë ardhur nga i njëjti burim, dhe si të tilla po hetohen si një procedim i vetëm. Prokuroria e Tiranë në hetimin e kësaj çështje po bashkëpunon me të gjitha agjencitë ligj zbatuese dhe partnerët ndërkombëtarë.

Aktualisht në Republikën e Shqipërisë në kuadër të strategjive në këtë fushë janë zbatuar disa masa për të adresuar këto kërcënime, duke përfshirë:

- Mbledhja dhe ndarja efektive e inteligjencës
- Masa të forta të sigurisë kibernetike
- Bashkëpunimi shumëpalësh në nivel rajonal dhe ndërkombëtar
- Planifikimi i emergjencës për të ndërmarrë veprime të menjëhershme ndaj kërcënimeve të mundshme.
- Trajnimi dhe edukimi i personelit dhe qytetarëve se si të menaxhojnë këto sulme.

Ka një bashkëpunim ndërinstitucional në kuadër të parandalimit dhe luftës ndaj krimit kibernetik, bashkëpunim ky që i detyron këto institucione të raportojnë pranë organizatave ndërkombëtare ku Republika e Shqipërisë është palë, apo pranë BE-së lidhur me masat që Shqipëria ka marrë në kuadër të luftës kundër krimeve kibernetike. Struktura të tilla janë Ministria për Evropën dhe Punët e Jashtme, Ministria e Mbrojtjes dhe Ministria e Brendshme (Strategjia për Mbrojtjen Kibernetike 2021-2023, pp.7-9). Në kuadër të këtyre raportimeve dhe detyrave të dala prej tyre, në vitin 2022 Shqipërisë si palë në Konventën e Budapestit i është lënë si detyrë të nënshkruajë edhe Protokollin e

dytë shtesë të Konventës “Për bashkëpunimin e zgjeruar dhe zbulimin e provave elektronike”, detyrë kjo që rezulton të jetë realizuar pasi ky protokolli është nënshkruar (European Commission. 2022).

Shqipëria ka qenë në linjë me qëndrimin e BE lidhur me negociatat për një Konventë të Kombeve të Bashkuara për krimin kibernetik, bazuar në Rezolutën e Këshillit të Sigurisë të OKB 74/247. Pavarësisht këtyre arritjeve në fushën e bashkëpunimit ndërkombëtare që lidhet me krimin kibernetik në raportin e Komisionit Evropian për Shqipërinë, është lënë detyrë që bazuar në Strategjinë Kombëtare për sigurinë kibernetike 2020-2025 Shqipëria duhet të ketë një ligj të ri për krimin kibernetik. Sipas këtij raporti, lufta kundër krimit kibernetik mbetet një nga fushat ku nevojitet ende punë për tu bërë. Shqipëria duhet hartojë një legjislacion efektiv që ti përgjigjet nevojave për identifikim, gjurmimin dhe ndjekjen penale të autorëve të këtyre krimeve. Strategjia Kombëtare për sigurinë kibernetike 2020-2025 gjithashtu parashikon një sërë objektivash siç janë (Strategjia Kombëtare për sigurinë kibernetike 2020-2025, 2020):

- Krijimi i ekipeve të reagimit ndaj incidenteve të sigurisë kompjuterike (CSIRT) në të gjithë sektorët e industrisë në nivel kombëtar. Këto ekipe do të jenë përgjegjëse për reagimin dhe menaxhimin e incidenteve të sigurisë kibernetike.
- Edukimi dhe rritja e kapaciteteve profesionale në fushën e sigurisë kibernetike. Ekziston nevoja për të përmirësuar trajnimet për sigurinë kibernetike në sektorin publik dhe për të promovuar ndërgjegjësimin për praktikat e sigurisë kibernetike midis punonjësve të qeverisë dhe publikut.
- Përmirësimi i bashkëpunimit ndërinstitucional në luftën kundër krimit kibernetik.
- Përditësimi i kuadrit ligjor për sigurinë kibernetike.

3.3.1 Si u trajtua sulmi kibernetik nga NATO: Rasti i Shqipërisë

Në muajin gusht dhe shtator 2022, Shqipëria u përball me një sulm kibernetik shkatërrues, që bëri qeverinë shqiptare, si një vend anëtar në NATO, të konsideronte mundësinë për të aktivizuar nenin 5, vendim ky që mund të kishte çuar të gjitha vendet anëtare të NATO-s drejtë një konfrontimi me Iranin.

”Në përfundim, Shqipëria vendosi të mos e ndërmerrte atë veprim, i cili do të rrezikonte përshkallëzimin e situatës dhe të krijonte tension mes aleatëve të fuqishëm”(Miller, 2022).

Në aspektin dypalësh Shqipëria ndërpreu marrëdhëniet diplomatike me Iranin, si kundërpërgjigje ndaj këtij sulmi, veprim ky që ndërmerret për herë të parë, për një situatë të tillë. Në aspektin shumëpalësh pati një reagim të NATO-s, me një deklaratë, në të cilën Aleanca njihte deklarimin e bërë nga Shqipëria dhe vendet e tjera aleate se sulmi është kryer nga shteti iranian dhe mbështeste qeverinë shqiptare në forcimin e kapaciteteve për mbrojtjenkibernetike (Statement by the North Atlantic Council, 2022.). Ndërsa Sekretari i Përgjithshëm i NATO-s. Jens Stoltenberg tha në Konferencën e Romës për mbrojtjen kibernetike se:

“Kërcënimi për krimin kibernetik është real dhe po rritet, ndaj dhe mbrojtja kibernetike është kaq e rëndësishme” (Stoltenberg,2022.)

Ai gjithashtu theksoi se Italia dhe Shtetet e Bashkuara janë shembull i mbrojtjes së fortë kibernetike, duke treguar angazhimin e tyre për t'u mbrojtur kundër këtyre kërcënimeve. Italia publikoi së fundmi Strategjinë e saj Kombëtare të Sigurisë Kibernetike, shoqëruar me krijimin e Agjencisë Kombëtare të Sigurisë Kibernetike. Në mënyrë të ngjashme, Shtetet e Bashkuara miratuan legjislacionin për të përmirësuar gjurmimin e sulmeve kibernetike dhe monitorimine pagesave të ransomware. Këto masa proaktive u mundësojnë autoriteteve të përgjigjen me shpejtësi ndaj sulmeve, të identifikojnë modelet dhe të lajmërojnë objektivat e mundshëm. Iniciativa të tilla, të pasqyruara nga shumë përpjekje të tjera brenda NATO-s, kontribuojnë në forcimin e qëndrueshmërisë së kombeve dhe në forcimin e mbrojtjes kolektive kundër sulmeve kibernetike (Stoltenberg,2022.).

KAPITULLI IV

SFIDAT E KRIMIT KIBERNETIK DHE ZGJIDHJET E MUNDSHME

4.1 Përgjegjësia individuale në sulmet kibernetike: A i favorizojnë strukturat shtetërore këto sulme?

Për ti dhënë përgjigje kësaj pyetje lind nevoja për një analizë të elementëve të veprës penalenë raport me krimin kibernetik. Çdo jurist kur vjen në dijeni të një ngjarjeje bën pyetjen se cila është vepra penale e konsumuar dhe menjëherë për ti dhënë përgjigje kësaj pyetje fillon dhe analizon elementët përbërës të veprës penale. Së pari, është objekti, i cili i referohet marrëdhënies juridike që është cënuar. Më pas, ana objektive, e cila përfshin veprimet ose mosveprimet e shkelësit, pasojat që rezultojnë, lidhjen ndërmjet veprimit dhe pasojave, kohën dhe vendin e veprës penale, si dhe metodat dhe mjetet e përdorura. Nga ana tjetër, subjekti përfaqëson individin e përfshirë, i cili duhet të plotësojë kriterin e moshës dhe të mbajë përgjegjësi për veprimet e tij. Së fundi, ana subjektive e cila përfshin vullnetin, motivin dhe qëllimin e shkelësit. Së bashku, këta elementë ndihmojnë në analizimin dhe kuptimin e aspekteve të ndryshme të një vepre penale.

Në rastet e krimeve kibernetike kur analizojmë anën subjektive që lidhet me motivin dhe qëllimin, rezulton të jenë të përfshirë edhe shtetet. Kjo lidhje ekziston kryesisht në rastet e hakerimit të sistemeve shtetërore. Në rastin e **Ukrainës** rezultoi se qëllimi i hakerimit ishte të krijohej destabilitet në vend. Rasti i **Shqipërisë**, duke analizuar ngjarjet që ndodhën në vitin 2022, rezulton se sulmi kibernetik ndodhi pikërisht pas paralajmërimit të liderëve iranian për mos lejimin nga Shqipëria të mbajtjes së Samitit Botëror të Iranit të Lirë, i parashikuar të mbahej në korrik 2022. Fillimisht u paralajmërua për një akt terrorist, paralajmërim ky që çoi në shtyrjen e Samitit, por rezultoi në hakerimin e platformave qeveritare. Si rezultat i lidhjes së hakeruesve me liderat iranian, Republika e Shqipërisë vendosi ndërprerjen e marrëdhënieve diplomatike me shtetin e Iranit, me argumentin se ky ifundit kishte shkelur sigurinë kombëtare të shtetit Shqiptar. Kjo mase është proporcionale me seriozitetin dhe nivelin e rrezikut të sulmit kibernetik, i cili solli si pasojë fshirjen e sistemeve dhe vjedhjen e të dhënave shtetërore, vjedhjen e komunikimeve elektronike brenda sistemit qeveritar dhe paralizimin e shërbimeve publike. Kjo situatë solli pasiguri dhe kaos në vend. Në mbështetje të kësaj analize dhe

mbi bazë të të dhënave të publikuara në faqen zyrtare të FBI-së rezulton se, shtetasit iranian të identifikuar si hakerues zënë vendin kryesor.

Një rast tjetër i rëndësishëm për t'u përmendur është padyshim dhe sulmi **Rus ndaj Estonisë**,një shtet i njohur gjerësisht për lidhjen e tij të fortë me internetin. Kjo ngjarje ka ndodhur në fund të muajit prill të vitit 2007. Motivi i sulmit mund të gjurmohet në vendimin e marrë nga qeveria estoneze për të zhvendosur (ose më saktë, për të hequr) statujën e "Ushtarit të Bronztë" nga sheshi qendror i Talinit. Kjo statujë shërbeu si një memorial për të nderuar çlirimtarët sovjetikë. Si rezultat i këtij veprimi politik, grupe të ndryshme hakerash rus filluannjë sërë sulmesh DDoS, duke paralizuar në mënyrë efektive të gjithë sistemin estonez. Kjo përfshinte faqet e internetit bankare, gazetat, ministritë, madje edhe faqen zyrtare të Parlamentit. Këto sulme bënë që vendi të bëhej i paarritshëm dhe jofunksional për disa orë.

Së pari dhe më e rëndësishmja, incidenti i Estonisë theksoi se lidhja e fortë me teknologjinë e bën vendin më vulnerabël ndaj sulmeve kibernetike. Së dyti, ky sulm është padyshim shembulli fillestar i luftës kibernetike për motive politike, ku përgjegjësia dhe përfshirja, megjithëse kryesisht në aspektin e mbështetjes logjistike dhe organizative, janë qartësisht të dukshme në nivel shtetëror. Së fundmi, vlen të theksohet se qeveria estoneze kërkoi aplikimin e Nenit 5 të Traktatit të NATO-s. Ky veprim përfshinte kërkesën për ndërhyrje ushtarake nga aleatët për të mbrojtur një vend anëtar që ishte sulmuar. Fakt ky i cili nuk mund të vërtetohej si pasojë e sfidës për sigurimin e provave të drejtpërdrejta të përfshirjes së Rusisë. Për më tepër, justifikimi i çdo veprimi nga Aleanca Atlantike në përgjigje të një ngjarjeje të tillë të paprekshme dhe pjesërisht të panjohur si një sulm kibernetik ishte i vështirë. Si përgjigje, i vetmi veprim i ndërmarrë nga NATO ishte krijimi i Qendrës Bashkëpunuese të Ekselencës për Mbrojtjen Kibernetike (CCDCOE).

4.2 Sfidat e krimit kibernetik: Mbrojtja kundër kërcënimeve në zhvillim

Krimi kibernetik është një problem kompleks dhe me zhvillim të shpejtë që paraqet disa sfida. Një nga sfidat më të rëndësishme është natyra globale e krimit kibernetik. Autorët e veprave penale me natyrë kibernetike mund të veprojnë nga kudo në botë dhe të synojnë viktima në vende të ndryshme, duke e bërë sfiduese për agjencitë e zbatimit të

ligjit gjurmimin e tyre dhe sjelljen e tyre para drejtësisë. Një sfidë tjetër është teknologjiavazhdimisht në zhvillim, e cila u mundëson autorëve të veprave penale me natyrë kibernetiktë shfrytëzojnë vazhdimisht dobësitë në sistemet software dhe hardware. Prandaj, është thelbësore që agjencitë e zbatimit të ligjit dhe ekspertët e sigurisë të jenë të përditësuar me zhvillimet më të fundit për të parandaluar dhe për t'iu përgjigjur efektivisht krimit kibernetik. Mungesa e ndërgjegjësimit të qytetarëve për rreziqet që lidhen me përdorimin e teknologjisë digjitale është një sfidë tjetër. Shumë njerëz përfshihen në sjellje të rrezikshme në internet që i bën ata të prekshëm ndaj krimit kibernetik. Kjo mungesë ndërgjegjësimi gjithashtu mund ta bëjë më sfidues për agjencitë e zbatimit të ligjit hetimin e krimit kibernetik dhe sjelljen e autorëve para drejtësisë.

Mungesa e bashkëpunimit ndërkombëtar është gjithashtu një sfidë e rëndësishme në luftimin e krimit kibernetik. Për shkak të natyrës globale të krimit kibernetik, është thelbësore që agjencitë e zbatimit të ligjit dhe qeveritë të punojnë së bashku për ta luftuar atë në mënyrë efektive (National Center for Justice and the Rule of Law University of Mississippi School of Law, 2007).Sfida tjetër është mungesa e burimeve dhe fondeve të nevojshme për të luftuar në mënyrë efektive krimin kibernetik. Hetimet e krimit kibernetik mund të kërkojnë burime intensive, duke kërkuar njohuri dhe pajisje të specializuara. Megjithatë, shumë agjencive të zbatimit të ligjit dhe qeverive mund ti mungojnë burimet dhe fondet e nevojshme për të ndërtuar ekspertizën dhe infrastrukturën e nevojshme për të luftuar në mënyrë efektive krimin kibernetik.

Gjithashtu dhe juridiksioni për krimin kibernetik është një çështje komplekse që ngre pyetje të rëndësishme për sovranitetin e shtetit. Natyra globale dhe pa kufij e hapësirës kibernetike e bën të vështirë përcaktimin se cilat ligje zbatohen për aktivitete specifike dhe cila qeveri ka juridiksion mbi to. Kjo mund të krijojë sfida për agjencitë e zbatimit të ligjit në hetimin dhe ndjekjen penale të autorëve të veprave penale me natyrë kibernetik, si dhe për qeveritë në rregullimin e aktivitetit në internet. Nga njëra anë, qasja territoriale pohon se një qeveri ka juridiksion mbi të gjitha aktivitetet që burojnë ose drejtohen nga brenda territorit të saj. Kjo qasje thekson sovranitetin e shtetit dhe autoritetin e tij për të rregulluar veprimtarinë brenda kufijve të tij. Megjithatë, kjo qasje mund të jetë sfiduese për t'u zbatuar në hapësirën kibernetike, ku informacioni digjital mund të transmetohet lehtësisht përtej kufijve. Nga ana tjetër, doktrina pohon se një qeveri ka juridiksion mbi aktivitetin që ka një efekt të rëndësishëm brenda territorit të saj, edhe nëse vetë aktiviteti zhvillohet jashtë territorit. Kjo qasje thekson ndikimin e aktivitetit në internet tek

individët dhe komunitetet brenda një juridiksioni të caktuar, pavarësisht se ku filloi aktiviteti. Megjithatë, kjo qasje mund të ngrejë gjithashtu pyetje në lidhje me shtrirjen e autoritetit të një qeverie dhe aftësinë e saj për të rregulluar veprimtarinë jashtë kufijve të saj. Si pasojë e këtyre mospërputhjeve, çështjet juridiksionale në krimin kibernetik nxjerrin në pah nevojën për bashkëpunim dhe koordinim ndërkombëtar ndërmjet qeverive për të adresuar këtë problem global. Kjo kërkon një ekuilibër midis mbrojtjes së sovranitetit të shtetit dhe adresimit të natyrës transnacionale të krimit kibernetik. Si e tillë, është e rëndësishme që qeveritë të punojnë së bashku për tëzhvilluar dhe zbatuar korniza ligjore efektive për rregullimin dhe zbatimin e ligjeve në hapësirën kibernetike.

4.3 Zgjidhjet e mundëshme

Adresimi i krimit kibernetik kërkon një qasje gjithëpërfshirëse dhe të koordinuar, duke përfshirë aktorë dhe strategji të shumta. Lufta kundër krimit kibernetik kërkon një qasje të shumanshme, duke përfshirë masa teknike dhe ligjore. Për sa i përket legjislacionit, ka disahapa që mund të ndërmerren për të adresuar krimin kibernetik:

- **Forcimi i ligjeve ekzistuese:** Ligjet ekzistuese mund të forcohen për të siguruar që ato të mbulojnë në mënyrë efektive krimin kibernetik. Kjo mund të përfshijë ndryshimin e ligjeve ekzistuese ose miratimin e ligjeve të reja për të adresuar kërcënimet kibernetike. Qeveritë mund të punojnë me agjencitë e zbatimit të ligjit, ekspertët e sigurisë kibernetike dhe palë të tjera të interesuara për të identifikuar boshllëqet në ligjet ekzistuese dhe për të zhvilluar zgjidhje efektive. Forcimi i ligjeve mund të arrihet në një sërë mënyrash, duke përfshirë ashpërsimin e dënimeve, duke u dhënë agjencive të zbatimit të ligjit më shumë burime, duke nxitur bashkëpunimin ndërkombëtar dhe duke rritur ndërgjegjësimin e publikut për rreziqet që lidhen me krimin kibernetik. Mund të jetë gjithashtu i suksesshëm për të luftuar krimin kibernetik hartimi i ligjeve të reja që trajtojnë llojet e reja të krimit kibernetik. Kërkohet një strategji gjithëpërfshirëse që përfshin bashkëpunimin ndërmjet aktorëve të ndryshëm, duke përfshirë agjencitë e zbatimit të ligjit, qeveritë, organizatat e sektorit privat dhe publikun për të luftuar në mënyrë efektive kriminkibernetik. Por nga ana tjetër është thelbësore të kuptojmë se vetëm ligjet janë të pamjaftueshme për të trajtuar krimin kibernetik.
- **Bashkëpunimi ndërkombëtar:** Krimi kibernetik është një çështje transnacionale

dhe bashkëpunimi ndërkombëtar është thelbësor në hetimin dhe ndjekjen penale e autorëve të veprave penale me natyrë kibernetike. Qeveritë mund të punojnë së bashku për të harmonizuar ligjet dhe procedurat e tyre dhe të bashkëpunojnë në hetimin dhe ndjekjen penale të krimit kibernetik. Kjo mund të përfshijë shkëmbimine informacionit, provave, ekspertizës përtej kufijve dhe ofrimin e ndihmës së ndërsjellë juridike në rastet e krimit kibernetik.

- **Ndërtimi i kapaciteteve:** Ndërtimi i kapaciteteve është thelbësor për hetimin dhe ndjekjen efektive të krimit kibernetik. Qeveritë mund të investojnë në trajnimin e oficerëve të zbatimit të ligjit, gjyqtarëve dhe prokurorëve mbi teknikat e hetimit dhe ndjekjes së krimit kibernetik. Kjo mund të përfshijë zhvillimin e programeve të specializuara të trajnimit, krijimin e partneriteteve me institucionet akademike apo ekspertët e industrisë, dhe sigurimin e burimeve dhe mbështetjes për zhvillimin e vazhdueshëm profesional. Ndërtimi i kapaciteteve për të parandaluar dhe hetuar krimin kibernetik kërkon marrjen e aftësive, informacionit dhe burimeve të nevojshme.
- **Rritja e aftësive të zbatimit të ligjit:** Qeveritë mund të investojnë në teknologji dhe infrastrukturë për të mbështetur hetimin dhe ndjekjen penale të krimit kibernetik. Kjo mund të përfshijë krijimin e njësive të specializuara për krimin kibernetik ose investimin në teknologjinë e avancuar. Agjencitë e zbatimit të ligjit mund të kenë nevojë gjithashtu të zhvillojnë teknika dhe metoda të reja për hetimin e krimit kibernetik, të tilla si përdorimi i analitikës së të dhënave, inteligjenca artificiale dhe pajisje të tjera.
- **Forcimi i sigurisë kibernetike:** Masat efektive të sigurisë kibernetike mund të ndihmojnë në parandalimin e shfaqjes së krimit kibernetik. Qeveritë mund të miratojnë ligje që kërkojnë që organizatat apo institucionet të zbatojnë masat e duhura të sigurisë kibernetike dhe të vendosin sanksione në rastet kur nuk zbatohen këto masa. Kjo mund të përfshijë kërkesën që këto entitete të raportojnë incidentet kibernetike dhe zbatimin e standardeve të detyrueshme të sigurisë.
- **Rritja e ndërgjegjësimit të publikut:** Edukimi i publikut mbi rreziqet dhe ndikimine krimit kibernetik mund të ndihmojë në parandalimin e individëve që të bien viktimë e sulmeve kibernetike. Kjo mund të përfshijë nisjen e fushatave të ndërgjegjësimit publik, zhvillimin e burimeve arsimore dhe ofrimin e trajnimit dhe mbështetjes për grupet vulnerabël, si fëmijët dhe të moshuarit.

- **Mbështetja e viktimave:** Viktimat e krimit kibernetik shpesh pësojnë dëmtime serioze financiare, emocionale dhe psikologjike, prandaj është thelbësore që viktimattë informohen dhe të edukohen për llojet e ndryshme të krimit kibernetik. Viktimat ekrimit kibernetik kërkojnë qasje të shpejtë në burime që mund të ndihmojnë në rikuperimin e tyre. Kjo mund të mbulojë mbështetjen financiare, udhëzimet ligjore dhe shërbimet e këshillimit. Këto burime mund të ofrohen nga qeveritë dhe organizatat jofitimprurëse që punojnë së bashku. Viktimat e krimit kibernetik duhet të jenë në gjendje t'i raportojnë ngjarjet autoriteteve të zbatimit të ligjit në mënyrë të lehtë dhe efektive. Dedikimi i një linje telefonike ose mekanizmi raportimi në internet që u ofron viktimave mbështetje dhe udhëzime të shpejta në këtë kategori.

4.3.1 Konventa Digjitale e Gjenevës: një hap para në luftën kundër krimitkibernetik

Siç u përmend dhe me sipër në situatën e vështirë në të cilën ndodhemi lind nevoja për mjete të reja legjislative jo vetëm nga ana shtetërore por dhe nga entët privat, në këtë pjesë vlen të përmendet dhe propozimi i bërë nga Microsoft-i për një konventë të re e quajtur "*KonventaDigjitale e Gjenevës*". Konventa e propozuar përfshin dispozita për mbrojtjen e infrastrukturës civile dhe vendosjen e mekanizmave për mbajtjen e vendeve përgjegjëse për shkeljen e rregullave, të cilat mund të jenë të rëndësishme për luftimin e krimit kibernetik. Sipas Microsoft, qëllimi i kësaj konvente është që:

"Të angazhohen qeveritë që të mbrojnë civilët nga sulmet e shteteve në kohë paqe. Dhe ashtu si Konventa e Katërt e Gjenevës pranoi se mbrojtja e civilëve kërkonte përfshirjen aktive të Kryqit të Kuq, mbrojtja kundër sulmit kibernetik të shteteve kërkon ndihmën aktive të kompanive teknologjike. Sektori i teknologjisë luan një rol unik si reagimi i parë i internetit, dhe për këtë arsye ne duhet të angazhohemi për veprime kolektive që do ta bëjnë internetin një vend më të sigurt, duke afirmuar një rol si një Zvicër Digjitale neutrale që ndihmon klientët kudo dhe ruan besimin e botës."

(Microsoft, n.d.)

Konventa Digjitale e Gjenevës është një grup rregullash që synojnë mbrojtjen e civilëve dhe organizatave nga sulmet kibernetike në kohë paqeje. Propozimi u paraqit nga

Microsoft në vitin 2017 dhe synon të sigurojë një kornizë për bashkëpunimin dhe diplomacinë ndërkombëtare për çështjet e sigurisë kibernetike. Ideja e Konventës Digjitale së Gjenevës është që të zbatohen parimet e Konventave të Gjenevës, të cilat rregullojnë zhvillimin e luftës dhe mbrojnë civilët dhe të burgosurit e luftës, në sferën digjitale. Konventa e propozuar do të vendoste një sërë rregullash që rregullojnë sulmet kibernetike dhe do të krijonte mekanizma për t'i mbajtur vendet përgjegjëse për shkeljen e këtyre rregullave. Rregullat e propozuara përfshijnë dispozita për mbrojtjen e infrastrukturës civile, si spitalet dhe rrjetet e energjisë elektrike, nga sulmet kibernetike. Ajo gjithashtu përshkruan përgjegjësitë e qeverive në reagimin ndaj sulmeve kibernetike dhe ofrojnë udhëzime për bashkëpunimin ndërkombëtar dhe shkëmbimin e informacionit. Ky propozim është i rëndësishme për disa arsye.

1. Njeh kërcënimin në rritje të sulmeve kibernetike të sponsorizuara nga shteti dhe nevojën për bashkëpunim ndërkombëtar për të adresuar këtë kërcënim. Duke vendosur rregulla dhe mekanizma të qarta për t'i mbajtur vendet përgjegjëse, mund të ndihmojë në parandalimin e sulmeve kibernetike dhe në parandalimin e përshkallëzimit të konfliktit në sferën digjitale.
2. Ofron një kornizë për mbrojtjen e infrastrukturës civile nga sulmet kibernetike. Kjo është veçanërisht e rëndësishme në një botë gjithnjë e më të ndërlidhur, ku një sulm kibernetik në infrastrukturën e një vendi mund të ketë efekte valëzuese në të gjithë globin.
3. Thekson rëndësinë e sjelljes etike dhe të përgjegjshme në sferën digjitale. Konventa Digjitale e Gjenevës u bën thirrje qeverive të respektojnë privatësinë dhe sigurinë e qytetarëve të tyre dhe të përdorin teknologjinë në mënyra që promovojnë paqen dhe stabilitetin.

Konventa Digjitale e Gjenevës parashikon tre parime kryesore që duhen njohur dhe respektuar në mënyrë që çdo përpjekje të jetë e suksesshme ("A Digital Rights Approach to the Tech Accord and The Digital Geneva Convention," n.d., p. 2):

1. Duhet të zhvillohet një proces i hapur, me shumë aktorë që përfaqësojnë qeveritë, sektorin e teknologjisë, grupet e shoqërisë civile dhe akademinë;
2. E gjithë bota duhet të përfaqësohet dhe të përfshihet aktivisht, nga veriu dhe jugu, lindja dhe perëndimi dhe jo vetëm "të dyshuarit e zakonshëm";
3. Procesi nuk mund të mbyllet në komitete që fshihen pas gjuhës teknike, ai duhet

të jetë i hapur dhe transparent, në mënyrë që të gjithë të mund të shohin se çfarë po ndodh dhe të kërkojnë llogari nga qeveritë e tyre, sektori i teknologjisë dhe të tjerët.

Gjithashtu sipas propozimit të bërë Microsoft-i nënvizon faktin se nëse nuk zbatohen këto parime bazë dhe procesi kthehet në grupe të mbyllura, të ngushta, atëherë bota do të qëndrojë aty ku është aktualisht. Konventa Digjitale e Gjenevës mund të ndihmojë në lehtësimin e këtij bashkëpunimi duke vendosur rregulla dhe parime të përbashkëta për trajtimin e krimit kibernetik në vende të ndryshme. Konventa mund të ndihmojë gjithashtu në promovimin e praktikave më të mira të sigurisë kibernetike midis qeverive dhe organizatave, të cilat mund të ndihmojnë në parandalimin e krimit kibernetik. Së fundi, konventa e propozuar mund të ndihmojë gjithashtu në rritjen e ndërgjegjësimit për rreziqet e krimit kibernetik dhe nevojën për bashkëpunim ndërkombëtar për të adresuar këtë problem.

Si përfundim, Konventa Digjitale e Gjenevës është një propozim i rëndësishëm që kërkon të vendosë një sërë rregullash ndërkombëtare që rregullojnë sigurinë kibernetike. Kjo Konventë, e propozuar nga Microsoft, nuk është një instrument ligjor detyrues. Është një angazhim vullnetar i shteteve për t'iu përmbajtur disa parimeve dhe normave në hapësirën kibernetike, të ngjashme me marrëveshjet e tjera jodetyruese siç është Manuali i Talinit.

Ndërsa shumë vende kanë shprehur mbështetje për parimet e përshkruara në Konventën Digjitale të Gjenevës, ka një sërë sfidash për zbatimin e saj. Një sfidë është mungesa e konsensusit midis shteteve se çfarë përbën sulm kibernetik dhe reagimi i duhur ndaj tij. Një sfidë tjetër është vështirësia në zbatimin e parimeve dhe vënien e shteteve para përgjegjëse për shkeljet. Për më tepër, disa kritikë argumentojnë se Konventa Digjitale e Gjenevës është e kufizuar në fushëveprim dhe nuk trajton disa nga çështjet më urgjente në hapësirën kibernetike. Pavarësisht këtyre sfidave, Konventa Digjitale e Gjenevës ka qenë me ndikim në formësimin e bisedës globale rreth normave kibernetike dhe nevojës për bashkëpunim dhe llogaridhënie më të madhe në hapësirën kibernetike.

4.3.2 Manuali i Talinit: Një udhëzues gjithëpërfshirës për luftën kibernetike

Manuali i Talinit (Schmitt, 2013) është një udhëzues gjithëpërfshirës që ofron njohuri mbi zbatimin e ligjit ndërkombëtar në kontekstin e luftës kibernetike. I shkruajtur nga një grup

ekspertësh ligjor të njohur si Grupi Ndërkombëtar i Ekspertëve, të cilët ekzaminuan skenarë të ndryshëm dhe parime ligjore të rëndësishme në fushën e krimit kibernetik. Manuali trajton tema të tilla si përkufizimi i luftës kibernetike, përgjegjësia e shtetit për operacionet kibernetike, ligji i konfliktit të armatosur në hapësirën kibernetike dhe mbrojtja e infrastrukturës kritike. Ky manual shërben si një burim i vlefshëm për të kuptuar kuadrin ligjor që rregullon aktivitetet kibernetike dhe promovon stabilitetin në hapësirën kibernetike.

Manuali i Talinit, duke qenë një dokument jo detyrues, nuk ka zbatim të drejtpërdrejtë në të drejtën e brendshme apo ndërkombëtare. Megjithatë, udhëzimet dhe analizat e tij mund të informojnë dhe ndikojnë në zhvillimin dhe zbatimin e kornizave ligjore që lidhen me sigurinë kibernetike. Qeveritë mund të rishikojnë legjislacionin e tyre ekzistues dhe të konsiderojnë përfshirjen e parimeve dhe interpretimeve nga Manuali i Talinit në ligjet e tyre të brendshme. Kjo mund të përfshijë përditësimin e ligjeve në lidhje me krimin kibernetik, mbrojtjen e të dhënave, mbrojtjen e infrastrukturës kritike dhe përgjegjësinë e shtetit për operacionet kibernetike. Gjithashtu ky manual mund të përdoret si referencë për të zhvilluar dhe përditësuar politikat dhe strategjitë kombëtare të sigurisë kibernetike. Shtetet mund t'i referohen Manualit të Talinit gjatë negociatave dhe diskutimeve mbi marrëveshjet ndërkombëtare ose traktatet që lidhen me sigurinë kibernetike, pasi interpretimet dheudhëzimet e manualit mund të ndikojnë në gjuhën dhe dispozitat e përfshira në marrëveshjetë tilla, duke rritur efektivitetin e tyre dhe respektimin e parimeve ligjore ndërkombëtare.

PËRFUNDIME

"Le ta pranojmë, e ardhmja është tani. Tashmë po jetojmë në një shoqëri kibernetike, ndaj duhet të ndalojmë së injoruari atë, apo të pretendojmë se nuk po na prek".

(Cit. Marco Ciapelli)

Realitetet e reja të teknologjisë dhe informatikës janë duke u zhvilluar në mënyrë të përshpejtuar duke sjellë incidente të drejtpërdrejta në sfera të ndryshme të shoqërisë, gjë kjo që kërkon një mbrojtje juridike nga sistemi ligjor veçanërisht nga e drejta penale. Me kalimin e kohës zhvillohet teknologjia në mënyrë eksponenciale duke krijuar mjete të reja materiale dhe jo materiale që përmirësojnë jetën e përditshëm. Pikërisht krimet e kryera përmes pajisjeve teknologjike shtohen me të njëjtën shpejtësi duke u gjendur përball krimeve të reja, të lidhura rreptësisht me përdorimin e sistemeve kmpjuterike dhe digjitale. Shifrat e autorëve të veprave penale me natyrë kibernetike, po ashtu, rritet gjatë gjithë kohës, pasi bëhet më e lehtë marrja e aftësive për të kryer krime përmes kompjuterëve dhe rrjetit dhe nëtë njëjtën kohë, metodat e anashkalimit të masave të sigurisë rriten. Përditësimi i vazhdueshëm i teknologjive dhe krimeve që lidhen me to duhet të korrespondojnë me një përditësim ekuivalent dhe të vazhdueshëm të prodhimit apo përditësimit të legjislacionit që rregullon llojet e krimeve kibernetike.

Krimi kibernetik është një problem serioz dhe në rritje në botën tonë gjithnjë e më digjitale.Ai i referohet çdo aktiviteti kriminal që përfshin përdorimin e teknologjisë, si kompjuterët, telefonat ose internetin. Ndikimi i krimit kibernetik mund të jetë i rëndësishëm, si financiarisht ashtu edhe në aspektin e sigurisë personale dhe shtetërore. Për të luftuar krimin kibernetik, është e rëndësishme të zbatohen masa efektive të sigurisë kibernetike, të tilla si fjalëkalime të forta, software të updatuar dhe antivirus. Për më tepër, individët dhe organizatat duhet të qëndrojnë vigjilentë dhe të jenë proaktivë në mbrojtjen e tyre kundër kërcënimeve kibernetike, duke përfshirë të qëndruarit të informuar. Operacionet sulmuese në hapësirën kibernetike paraqesin sfida unike për rendin juridik ndërkombëtar, të cilat po trajtohen nga komuniteti ndërkombëtar. Gjithashtu siç dhe u analizua më sipër, është bërë thelbësore përcaktimi i një përkufizimi universal i krimit kibernetik në ligj për të vendosur kufij të qartë ligjor dhe për të lehtësuar

zbatimin efektiv të ligjit. Përcaktimi i një përkufizimi ezaurues dhe universal shërben për disa qëllime të rëndësishme. Së pari, ai ofron një kornizë për identifikimin dhe ndjekjen penale të veprimtarisë kriminale në sferën digjitale. Duke përcaktuar qartë llojet e aktiviteteve që përbëjnë krimin kibernetik, zyrtarët e zbatimit të ligjit mund të hetojnë dhe ndjekin më mirë autorët e veprave penale me natyrë kibernetike, duke ndihmuar gjithashtu në parandalimin e shkelësve të mundshëm. Së dyti, përcaktimi i krimit kibernetik në ligj ndihmon për të siguruar që individët dhe organizatat të jenë të vetëdijshëm për detyrimet dhe përgjegjësitë e tyre ligjore kur bëhet fjalë për sigurinë kibernetike. Kjo mund të përfshijë kërkesat për zbatimin e masave specifike të sigurisë, raportimin e incidenteve dhe mbrojtjen e informacionit të ndjeshëm. Duke vendosur kërkesa të qarta ligjore, ligji mund të ndihmojë në nxitjen e praktikave më të mira të sigurisë kibernetike, duke kontribuar përfundimisht në një mjedis digjital më të sigurt. Së treti, përcaktimi i krimit kibernetik në ligj mund të ndihmojë në lehtësimin e bashkëpunimit ndërkombëtar në luftën kundër krimit kibernetik. Duke vendosur përkufizime dhe standarde të përbashkëta ligjore, vendet mund të punojnë së bashku në mënyrë më efektive për të hetuar dhe ndjekur penalisht autorët e këtyre veprave, duke shkëmbyer gjithashtu informacion dhe ekspertizën për të parandaluar sulmet e ardhshme.

Siç shpjegohet shkurt në seksionin "Sulmet kibernetike si krime me natyrë ndërkombëtare", debati brenda Gjykatës Ndërkombëtare Penale në lidhje me kualifikimin e sulmeve kibernetike si krim me natyrë ndërkombëtare është ende në vazhdim dhe nuk ka rezultuar në një përgjigje përfundimtare. Konkretisht, kualifikimi i sulmeve kibernetike si krime agresioni del si një pikë kritike mosmarrëveshjeje. Ekspertët juridikë, në varësi të qasjes që ndjekin, ende kanë mendime të ndryshme për këtë çështje. Trajtimi efektiv i krimit kibernetik si krim me natyrë ndërkombëtare nga pikëpamja e Ligjit Ndërkombëtar Penal mund të kërkojë ndryshime të mëtejshme në Statutin e Romës.

Për sa i përket NATO-s, ku pika kyçe është siguria, duke përfshirë operacionet dhe misionet, si dhe përmirësimi i qëndrueshmërisë së tërë Aleancës, kjo realizohet nëpërmjet forcimit të aftësive të NATO-s nëpërmjet edukimit, trajnimit dhe bashkëpunimit midis shteteve antare në fushën kibernetike. Ndërsa për sa i përket legjislacionit vendas krimit kibernetik në Republikën e Shqipërisë është e rëndësishme që Shqipëria të marrë masa proaktive për të luftuar krimin kibernetik dhe për të mbrojtur qytetarët e saj. Krimi kibernetik është një kërcënim në rritje në Shqipëri, por nuk është një kërcënim i pakapërcyeshëm. Një nga sfidat kryesore me të cilat përballet Shqipëria në luftën kundër

krimit kibernetik është mungesa e ndërgjegjësimit dhe mirëkuptimit të publikut të gjerë dhe zyrtarëve të zbatimit të ligjit. Ende Shqipëria nuk është e vetëdijshme për rreziqet që sjell krimi kibernetik, ndërkohë që autoriteteve të zbatimit të ligjit mund t'u mungojnë trajnimet dhe burimet e nevojshme për të hetuar dhe ndjekur penalisht autorët e këtyre veprave penale me natyrë kibernetike. Për të adresuar këto sfida, Shqipëria duhet të marrë një qasje të shumanshme për të luftuar krimin kibernetik. Kjo duhet të përfshijë rritjen e ndërgjegjësimit të publikut për kërcënimet kibernetike dhe mënyrën e mbrojtjes kundër tyre, investimin në trajnime dhe burime për zyrtarët e zbatimit të ligjit dhe zhvillimin e kornizave ligjore më të forta për të ndjekur penalisht kriminelët kibernetikë. Një hap tjetër i rëndësishëm është krijimi i bashkëpunimeve me vende të tjera dhe organizata ndërkombëtare për të shkëmbyer informacion dhe ekspertizë mbi krimin kibernetik. Shqipëria mund të përfitojë nga përvoja dhe njohuritë e vendeve të tjera dhe të punojë së bashku për të parandaluar krimin kibernetik. Prandaj mund të themi se, është bërë shumë, po bëhet shumë, por ende ka shumë për të bërë. Kjo është për shkak se shumë shpesh shfaqen pasiguritë në interpretimet nga jurisprudenca lidhur me dispozitat të cilat rregullojnë fenomenin e krimeve kompjuterike në Shqipëri.

Së fundi, një aspekt tjetër që duhet marrë parasysh, edhe pse jo rreptësishtë ligjor, është rëndësia e ndërgjegjësimit për krimet kompjuterike. Shpesh, përdoruesit e sistemeve kompjuterike nuk janë plotësisht të vetëdijshëm për rreziqet që lidhen me përdorimin e pajisjeve dhe shfletimin në internet. Kjo mungesë e vetëdijes ndikon gjithashtu në të kuptuarit se si informacioni personal përdoret dhe ruhet në internet ose brenda sistemeve kompjuterike. Është thelbësore të njihet realiteti i krimeve kompjuterike, veçanërisht tani që teknologjia dhe mjetet kompjuterike janë pjesë integrale e jetës sonë dhe kërkojnë përditësime të vazhdueshme. Ndërgjegjësimi mund të arrihet përmes fushatave edukative, njoftimeve të shërbimeve publike, bashkëpunimeve me media dhe kompani teknologjike, bashkëpunim me agjencitë e zbatimit të ligjit, partneritete me sektorin privat dhe organizatat joqeveritare gjithashtu dhe duke përfshirë sigurinë kibernetike në arsim. Duke u ofruar përdoruesve informacionin e nevojshëm për këto teknologji dhe rreziqet e tyre, ne mund të shpresojmë për masa më të mira sigurie dhe një përdorim më të përgjegjshëm të avantazheve që ofron teknologjia.

REFERENCA

Burime ligjiore

A/RES/74/247, Resolution adopted by the General Assembly on 27 December 2019 (2020).Marrë nga: https://digitallibrary.un.org/record/3847855

Council of Europe, Convention on Cybercrime, 23 November 2001. Marrë nga : https://rm.coe.int/1680081561 [aksesuar më 13.06.2023]

Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. EUR-Lex.Marrë nga: http://data.europa.eu/eli/dec_framw/2005/222/oj [aksesuar më 2.06.2023]

Council of Europe, Convention on Cybercrime, 23 November 2001. Marrë nga: https://www.refworld.org/docid/47fdfb202.html [aksesuar më 5.06.2023]

Council of Europe. Additional Protocol to the Convention on Cybercrime, concerning thecriminalisation of acts of a racist and xenophobic nature committed through computer systems, Strasbourg 28 January 2003. Marrë nga: https://rm.coe.int/168008160f [aksesuar më 2.06.2023]

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. EUR-Lex. Marrë më 2 qershor nga: http://data.europa.eu/eli/dir/2013/40/oj [aksesuar më 10.05.2023]

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. EUR-Lex. Marrë më 2 qershor nga: http://data.europa.eu/eli/dir/2013/40/oj [aksesuar më 14.06.2023]

European Commission (2020) Lex - 52020JC0018 - en - EUR-lex, EUR-Lex. Available at:https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN%3A2020%3A18%3AFIN [aksesuar më 12.06.2023]

Kodi Penal i Republikës së Shqipërisë. Miratuar me ligjin nr.7895, datë 27.1.1995. Marrënga : https://www.drejtesia.gov.al/wp-content/uploads/2017/11/Kodi_Penal-1.pdf

Konventa për Krimin në Fushën e Kibernetikës. Fletorja Zyrtare e Republikës së Shqipërisë.Marrë nga: https://www.pp.gov.al/rc/doc/konventa_per_krimin_ne_fushen_e_kibernetikes_786.pdf [aksesuar 2.06.2023]

Ligji Nr. 9887, datë 10.03.2008, "Për mbrojtjen e të dhënave personale". Marrë nga : https://mb.gov.al/wpcontent/uploads/2018/02/ligji_9887_per_mbrojtjen_e_te_dhenave_personale.pdf [aksesuar më 12.04.2023]

Ligj Nr.10 178, datë 29.10.2009 "Për Miratimin e Aktit Normativ, me fuqinë e Ligjit, Nr.8, Datë 30.9.2009, të Këshillit të Ministrave "Për një ndryshim në Ligjin Nr.9880, Datë 25.2.2008 "Për Nënshkrimin Elektronik". Marrë https://akshi.gov.al/wpcontent/uploads/2018/03/ligj_nenshkrimi_elektronik_41.pdf [aksesuar më 12.04.2023]

Ligji Nr. 9918, datë 19.05.2008, "Për komunikimet elektronike në Republikën e Shqipërisë". Marrë nga :https://qbz.gov.al/preview/06981d97-2974-488a-8f8c-00dfa462c4e4/cons/20200210 [aksesuar më 12.04.2023]

Ligji Nr.2, datë 26.01.2017, "Për sigurinë kibernetike". Marrë nga: https://qbz.gov.al/eli/ligj/2017/01/26/2 [aksesuar më 12.04.2023]

Ligji Nr.107, datë 15.10.2015,"Për identifikimin elektronik dhe shërbimet e besuara", i ndryshuar Marrë nga: https://qbz.gov.al/eli/fz/2016/259/47f82d11-2170-41c2-976092c5ba9ebcae;q=ligjin%20nr.%20123%2F2016,%20dat%C3%AB%2015.12.2016 [aksesuar më 12.04.2023]

Ligji Nr. 10/2023, "Për Informacionin e Klasifikuar". Marrë nga : https://qbz.gov.al/preview/96199dbd-cac9-4bff-8cca%20fa3142867412 [aksesuarmë 12.04.2023]

Ligj Nr.10 024, datë 27.11.2008 ""Për disa ndryshime dhe shtesa në Ligjin Nr.8331, datë 21.4.1998 "Për ekzekutimin e vendimeve penale"". Marrë nga: https://www.pp.gov.al/rc/doc/ligj_nr_10_024_date_27_11_2008_53.pdf [aksesuarmë 12.04.2023]

Ligj Nr.10 024, datë 27.11.2008 ""Për disa ndryshime dhe shtesa në Ligjin Nr.8331, datë 21.4.1998 "Për ekzekutimin e vendimeve penale"". Marrë nga: https://www.pp.gov.al/rc/doc/ligj_nr_10_024_date_27_11_2008_53.pdf [aksesuarmë 12.04.2023]

The North Atlantic Treaty (1949), (Article 5). Marrë nga: https://www.nato.int/cps/en/natolive/official_texts_17120.htm

Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence (CETS No. 224) (2022) Councile of Europe. Marrë nga: https://www.coe.int/en/web/conventions/full-list?module=treaty- detail&treatynum=224 [aksesuar më 6.06.2023]

The European Parliament and the Council of the European Union, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016

concerning measures for a high common level of security of network and information systems across the Union. Marrë nga: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L1148 [aksesuar më 3.06.2023]

The European Parliament and the Council of the European Union. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Marrë nga: //data.europa.eu/eli/dir/2022/2555/oj [aksesuar më 1.06.2023]

Libra

Chaumette, A. (2018). International Criminal Responsibility of Individuals in Case of Cyberattacks, International Criminal Law Review, 18(1), 1-35. Marrë nga: https://doi.org/10.1163/15718123-01801004

Chawki, M., Darwish, A., Khan, M. A., & Tyagi, S. (2015). *Cybercrime, digital forensicsand jurisdiction*. Springer.

Lucas, G. R. (2017). Ethics and cyber warfare: The quest for responsible security in the age of Digital Warfare. Oxford University Press.

Jonathan, C. Faculty of Law, Monash University Principles of Cybercrime, fq.10. Marrënga: http://ir.kluniversity.in/xmlui/bitstream/handle/123456789/710/4.Principles%20of%20Cybercrime.pdf?sequence=1&isAllowed=y\

National Center for Justice and the Rule of Law University of Mississippi School of Law. (2007). Combating cyber crime: essentialtools and effective organizationalstructures aguide for policymakers and managers. National Center for Justice and the Rule of Law.

Schmitt, M. N. (Ed.). (2013). Tallin Manual on the intenational law applicable to cyberwarfare. Cambridge University Press . Marrë nga: https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2017-Tallinn-Manual-2.0.pdf

Schjolberg, S. (2008). The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva, fq 4. Marrë nga: https://cybercrimelaw.net/documents/cybercrime_history.pdf

Raporte

European Commission. (2022). (rep.). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region. Brussels .Marrë nga:

https://neighbourhood-enlargement.ec.europa.eu/system/files/2022-10/Albania%20Report%202022.pdf

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1. C.J. Reports 1996, fq. 226. Marrë nga: https://www.icj-cij.org/public/files/case-related/95/095- 19960708-ADV-01-00-EN.pdf

Prokuroria e Përgjithshme, Raporti vjetor i kriminalitetit 2022, fq 173-176. Marrë nga:https://www.pp.gov.al/rc/doc/Raporti_Vjetor_kriminaliteti_2022_Kuvendit_Prok uroria_e_Pergjithshme_6915.pdf

Prokuroria e Përgjithshme, Raporti vjetor i kriminalitetit 2022, fq 173-176. Marrë nga:https://www.pp.gov.al/rc/doc/Raporti_Vjetor_kriminaliteti_2022_Kuvendit_Prok uroria_e_Pergjithshme_6915.pdf

Raporti i plotë i sulmit kibernetik të 15 korrikut 2022, një analizë e detajuar, sipas gjithë etapave që nga 15-16 korriku 2022. Marrë nga: https://akshi.gov.al/wp-content/uploads/2022/09/Raporti-i-plot%C3%AB-i-sulmit-kibernetik-t%C3%AB-15-korrikut-2022.pdf

Tema diplome

De Vito, V. S. (2020, September 4). (thesis). Attacchi informatici e diritto penale internazionale: il crimine di aggressione nel cyberspazio. Marrë nga:https://www.cybersecurity360.it/nuove-minacce/attacchi-informatici-e-diritto- penale-internazionale-il-crimine-di-aggressione-nel-cyberspazio/

De Vivo, M.C. (2012). (thesis). 'Informatica e diritto, XXXVIII', in G. Ricci (ed.) Diritto,crimini e tecnologie, fq. 25–27.Marrë nga: http://www.ittig.cnr.it/EditoriaServizi/AttivitaEditoriale/InformaticaEDiritto/IeD2012_02_DevivoRicci.pdf

CONTI, L. (2014). (thesis). I reati informatici analisi critica di alcune fattispecie ed esamedi relativi casi giuridici, fq.44-45. Marrë nga: https://amslaurea.unibo.it/9489/4/Tesi_-_Laura_Conti.pdf

Simoncelli, L. (2014). (thesis). I crimini informatici, la disciplina nell'ordinamento italiano e la cooperazione internazionale, fq.4-7. Marrë nga: https://tesi.luiss.it/16811/1/623502.pdf

Understanding cybercrime and developing a monitoring device, Bachelor`s thesis Information Technology, fq.6-7. Marrë nga: https://core.ac.uk/download/pdf/84800659.pdf

Shkembi, A. (2015). (thesis). Krimi kibernetik harmonizimi i legjislacionit Shqiptar me ateEuropian , fq.92. Marrë nga: https://uet.edu.al/wp-content/uploads/2021/11/Aldo_Shkembi.pdf

Gazeta online

Kërcënimet për një sulm terrorist, muxhahedinët e mek në durrës shtyjnë samitin e iranittë lirë. (2022, July 22).Shqiptarja.Com. Marrë nga: https://shqiptarja.com/lajm/kercenimet-per-nje-sulm-terrorist-muxhahedinet-e-mek-ne-durres-shtyjne-samitin-e-iranit-te-lire

Miller, M. (2022, October 5). Albania weighed invoking nato's article 5 over iranian cyberattack. Politico . Marrë nga: https://www.politico.com/news/2022/10/05/why- albania-chose-not-to-pull-the-nato-trigger-after-cyberattack-00060347

Sulmi kibernetik, rama: i gjithë stafi i ambasadës së iranit të largohet brenda 24 orëve ngashqipëria. (2022, September 7). Marrë nga: https://shqiptarja.com/lajm/sulmi-kibernetik-rama-i-eshte-kerkuar-trupes-diplomatike-te-iranit-te-largohet-brenda- 24-oreve

Standage, T. (2017) 'The crooked timber of humanity', *The Economist*, 5 October. Marrë nga: https://www.economist.com/1843/2017/10/05/the-crooked-timber-of-humanity

Statement by the North Atlantic Council concerning the malicious cyber activities againstAlbania.Marrë nga: https://www.nato.int/cps/en/natohq/official_texts_207156.htm#:~:text=Allies%20acknowledge%20the%20statements%20by,the%20daily%20lives%20of%20citizens

Burime të tjera

A digital rights Approach to the tech accord and The Digital Geneva Convention fq.2. Marrë nga: https://www.accessnow.org/wp-content/uploads/2018/08/DGC-tech- accord-human-rights.pdf

A digital rights approach to the tech accord and the digital geneva convention, 2018, fq.3-5. Marrë nga:https://www.accessnow.org/wp-content/uploads/2018/08/DGC-tech-accord-human-rights.pdf

ARENA, M. (2021). La Convenzione di Budapest del Consiglio d'europa sulla repressione della criminalita' informatica. *Ciro Press*, fq.3–25. Marrë nga: https://www.lex.unict.it/sites/default/files/crio/papers/CRIO_Papers_n59_Arena.p df

Internet Organised Crime Threat Assessment (IOCTA) 2021, Europol, fq.8. Marrë nga: https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organis ed_crime_threat_assessment_iocta_2021.pdf

Keynote address by NATO Secretary General Jens Stoltenberg at the NATO Cyber Defence Pledge Conference in Italy. Marrë nga: https://www.nato.int/cps/en/natohq/opinions_208925.htm

Kumar, Dr.S. (2022) 'Historical genesis and evolution of cyber crime and cyber security laws in India', International Research Journal of Engineering and Technology (IRJET), 09(08), (Fp. 1362–1363). Marrë nga:https://www.irjet.net/archives/V9/i8/IRJET-V9I8226.pdf

Maigre, M. (2022). NATO's Role in Global Cyber Security, fq. 2–4. Marrë nga: https://www.gmfus.org/sites/default/files/2022-04/Maigre%20-%20NATO%20-%20Geopolitics%20-%20Cyber%20-%20final.pdf

Martino, L. (n.d.). La quinta dimensione della conflittualità. La rilevanza strategica del cyberspace e i rischi di guerra cibernetica. Center for cyber security and international relations studies CSSII, (fq.5). Marrë nga https://www.dsps.unifi.it/upload/sub/martino-la-quinta-dimensione-2-1.pdf

Ministria e Mbrojtjes (2020), Strategjia për Mbrojtjen Kibernetike 2021-2023, (fq.7-9). Marrë nga: https://www.mod.gov.al/images/PDF/2020/Strategjia-Mbrojtjen-Kibernetike-2021-2023.pdf

Miller, M. (2022, October 5). Albania weighed invoking nato's article 5 over iranian cyberattack. Politico . Marrë nga: https://www.politico.com/news/2022/10/05/why- albania-chose-not-to-pull-the-nato-trigger-after-cyberattack-00060347

NATO, "Fjalimi kryesor i Sekretarit të Përgjithshëm të NATO-s Jens Stoltenberg në hapjen e seminarit të transformimit të NATO-s", Organizata e Traktatit të Atlantikut të Veriut.

Nato. (2008, April 3). Bucharest summit declaration issued by NATO heads of state and government (2008). NATO.Marrë nga: https://www.nato.int/cps/en/natolive/official_texts_8443.htm

North Atlantic Treaty Organisation. CCDCOE. (n.d.). Marrë nga:https://ccdcoe.org/organisations/nato/ [aksesuar më 13.06.2023]

North Atlantic Treaty Organization. (2021, April). NATO cyber defence. Marrë nga:https://www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet- cyber-defence-en.pdf

North Atlantic Treaty Organization. (2001) North Atlantic Treaty Organization NATO.International Organizations. Marrë nga: https://www.drejtesia.gov.al/wp-content/uploads/2019/03/KARTA-E-KOMBEVE-TE-BASHKUARA-1.pdf [accessed 16 may 2023]

Policimi dhe siguria, Krimi kompjuterik,kërcënimi kibernetik dhe siguria kombëtare, fq.17.Marrë nga:http://www.acnss.com/wp-content/uploads/2020/06/Policimi_dhe_siguria_nr_13-1.pdf

Prokuroria e Përgjithshme, sulmi kibernetik ndaj TIMS. Marrë

nga:https://www.pp.gov.al/Tirane/Media/Sulmi_kibernetik_ndaj_TIMS_Prokuroria_e _Tiranes_nis_hetimet_per_disa_vepra_penale.html

PURSER, S. (2014). Standards for Cyber SecurityEuropean Union Network and Information Security Agency (ENISA) . In Standards for Cyber Security (fq. 101–104). IOS Press.Marrë nga: https://www.enisa.europa.eu/publications/articles/standards-for-cyber-security

Sari A. (2023). International Law and Cyber Operations: Current Trends and Developments, fq.3-4. Marrë nga: https://rm.coe.int/64th-cahdi-pr-aurel-sari-presentation/1680aaaf48

Statement by the North Atlantic Council concerning the malicious cyber activities againstAlbania. Marrë nga: https://www.nato.int/cps/en/natohq/official_texts_207156.htm#:~:text=Allies%20acknowledge%20the%20statements%20by,the%20daily%20lives%20of%20citizens

Strategjia Kombëtare e Sigurisë Kibernetike 2020 – 2025, vendimi nr. 1084, datë 24.12.2020.Mar nga: https://cesk.gov.al/legjislacioni/2020/strategjia_kombetare_sigurise_kibernetike.p df

Taddei, N. (2015). Cyberwar, lo strumento bellico del futuro? Il caso Russo-Georgiano,fq.10-15. Marrë nga:https://www.cssii.unifi.it/upload/sub/Pubblicazioni/2015_Taddei_Niccol%C3%B 2.pdf

Team GAIT. (n.d.). THE NOTPETYA CASE Attack against Ukraine on 27th of June 2017.Marrë nga: file:///C:/Users/HP/Downloads/The%20NotPetya%20case_Team%20GAIT.pdf

UN General Assembly, Definition of Aggression, 14 December 1974, A/RES/3314. Marrë nga: https://crimeofaggression.info/documents/6/General_Assembly_%20Resolution_%203314.pdf