ISBN 978-9928-210-08-1
ISSN 2413-1334

Konferenca e III-të Shkencore Ndërkombëtare

VËLLIMI I PARË

Policimi dhe SIGURIA

Krimi kompjuterik, kërcënimi kibernetik dhe siguria kombëtare

NËNTOR
2018

PROCEEDINGS
Botim i Akademisë së Sigurisë, Tiranë 2018

POLICIMI DHE SIGURIA
AKADEMIA E SIGURISË

KONFERENCA E III-TË NDËRKOMBËTARE

Krimi kompjuterik, kërcënimi kibernetik dhe siguria kombëtare

PROCEEDINGS

Vëllimi I

AKADEMIA E SIGURISË

Në bashkëpunim me :

Me mbështetjen e:

Botuar nga Akademia e Sigurisë, Tiranë 2018

CIP Katalogimi në botim BK Tiranë

Akademia e Sigurisë
Krimi kompjuterik, kërcënimi kibernetik dhe siguria kombëtare : konferenca III-të ndërkombëtare : Tiranë, 2018 : proceedings / Akademia e Sigurisë ; red. Albert Hitoaliaj. – Tiranë : Akademia e Sigurisë, 2018
Vol. 1 ; 267 f. ; 16.5cmx24cm.

ISBN 978-9928-210-08-1

1.Policia 2.Siguria kombëtare 3.Kriminologjia 4.Konferenca

351.74 (062)
343 (062)

"POLICIMI DHE SIGURIA"
ISSN 2413-1334
Viti i III-të i botimit

NR 12
NËNTOR
2018

BORDI EDITORIAL

AKADEMIA E SIGURISË
ISBN 978-9928-210-08-1
ISSN 2413 - 1334

KONFERENCA E III-të SHKENCORE NDËRKOMBËTARE
"Krimi kompjuterik, kërcënimi kibernetik dhe siguria kombëtare"

Komiteti shkencor/ Scientific Committee

Kryetar i Bordit/Chair

Prof. Dr. Ismet ELEZI
Kriminolog

Anëtarët/Members

Prof. Dr. Xhovani ARCUDI
Profesor, Universiteti i Romës "Tor Vergata", Itali
Prof. Dr. Vasilika HYSI
Kriminologe, ligjvënëse
Prof. Dr. Ilirjan MANDRO
Dekan i Fakultetit të Sigurisë dhe Hetimit, Akademia e Sigurisë
Prof. Dr. Irakli KOÇOLLARI
Rektor i Kolegjit të Lartë Universitar "Akademia Profesionale e Biznesit"
Prof. Dr. Laura TAFARO
Profesor, Universiteti i Barit, Itali
Prof. Dr. Kseanela SOTIROFSKI
Rektore e Universitetit "Aleksandër Moisiu", Durrës
Prof. Dr. Emiljano GIARDINA
Profesor, Universiteti i Romës "Tor Vergata", Itali
Prof. Dr. Ethem RUKA
Rektor i Kolegjit të Lartë Universitar "Luarasi"
Gen. (ret.) Volker HELBAUER
Kryetar i Këshillit të Kolegjit Universitar ISPE-Kosovë
Prof. Asc. Idriz HAXHIAJ
Zëvendësshef i Misionit të Shqipërisë në NATO, Bruksel
Prof. Asc. Ferdinand ELEZI
Prokuroria e Apelit, Durrës - Anëtar
Dr. Vilma TOMÇO
Drejtoreshë e Përgjithshme e Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike
Dr. Bilbil MEMAJ
Drejtori/Rektori i Akademisë së Sigurisë
Dr. Xhavit SHALA
Drejtor i Qendrës së Kërkimeve Shkencore, Akademia e Sigurisë
Dr. Sandër LLESHI
Këshilltar për Sigurinë, Këshilli i Ministrave
Dr. Frank HARRIS
MSc, D. Crim. J., University of Portsmouth
Z. Ismail SMAKIQI
Drejtor i Përgjithshëm i Akademisë së Kosovës për Siguri Publike
Dr. Albert HITOALIAJ
Redaktor shkencor/Lektor, Akademia e Sigurisë, Tiranë

AKADEMIA E SIGURISË
ISBN 978-9928-210-08-1
ISSN 2413 - 1334

KONFERENCA E III-të SHKENCORE NDËRKOMBËTARE
"Krimi kompjuterik, kërcënimi kibernetik dhe siguria kombëtare"

Komiteti organizator/Organizational Committee

Kryetari/Chair

Dr. Bilbil MEMAJ, Drejtori/Rektori i Akademisë së Sigurisë.

Zëvendëskryetari

Dr. Xhavit SHALA, Drejtori i Qendrës së Kërkimeve Shkencore, Akademia e Sigurisë

Anëtarët/Members

Prof. Asc. Dr. Sokol SADUSHI, Drejtor i Shkollës së Magjistraturës
Z. Brian THIESSEN, OSCE, Law Enforcement Development Officer Security Cooperation Department
Prof. Asc. Dr. Elton NOTI, Zëvendësrektor, Universiteti "Aleksandër Moisiu" Durrës
Znj. Anna MARINELI, Team Leader Project "Countering Serious Crime in the Western Balkans", Ministria e Brendshme
MSc. Arjan MUÇAJ, Prokuror në Prokurorinë e Përgjithshme, Tiranë
Prof. Dr. Laura TAFARO, Profesor, Universiteti i Barit, Itali
MSc. Edlira BEJKO, Drejtore drejtorie në Autoritetin Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike
Magjistër Dr. (Proc.) Armando GURAKUQI, Prokuror në Prokurorinë pranë Gjykatës së Shkallës së Parë, Tiranë
Prof. Dr. Emiljano GIARDINA, Profesor, Universiteti i Romës "Tor Vergata", Itali
Dr. Bajram IBRAJ, Ushtrues detyre, Drejtor/Rektor i Kolegjit ISPE
Prof. Asc. Dr. Gaqo TANKU, Lektor, Universiteti "Aleksandër Moisiu", Durrës
Dr. Artur BEU, Oficer Kontakti i Policisë së Shtetit, Itali
Z. Giovanni PASQUA, Ekspert afatgjatë për burimet njerëzore pranë Projektit Pameca V.
MSc. Dashamir ÇALI, Shef i sektorit të hetimit të krimeve kompjuterike, departamenti i policisë kriminale në Policinë e Shtetit
MSc. Bilbil DERVISHI, Qendra e Kërkimeve Shkencore, Akademia e Sigurisë, Tiranë

Koordinatorët / Coordination

MSc. Anisa AGASTRA, Koordinatore e Përgjithshme, Qendra e Kërkimeve Shkencore, Akademia e Sigurisë
Dr. Irvin FANIKO, Koordinator, Qendra e Kërkimeve Shkencore, Akademia e Sigurisë
MSc. Qetësor GURRA, Koordinator, Fakulteti i Sigurisë dhe Hetimit, Akademia e Sigurisë

Redaktor Shkencor

Dr. Albert HITOALIAJ, Qendra e Kërkimeve Shkencore, Akademia e Sigurisë.

Punimet grafike

MSc. Andi OSMANI, Qendra e Kërkimeve Shkencore, Akademia e Sigurisë.

Realizimi teknik: Qendra e Kërkimeve Shkencore, Akademia e Sigurisë

AKADEMIA E SIGURISË

KONFERENCA E III-të SHKENCORE NDËRKOMBËTARE, nëntor 2018, Tiranë

KRIMI KOMPJUTERIK, KËRCËNIMI KIBERNETIK DHE SIGURIA KOMBËTARE

Në bashkëpunim me:
Organizatën e Traktatit të Atlantikut të Veriut (NATO),
Autoritetin Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK),
Universitetin Aleksandër Moisiu Durrës (UAMD).

Me mbështetjen e:
Organizatës për Siguri dhe Bashkëpunim në Evropë, Prezenca Shqipëri (OSCE),
Misionit PAMECA V,
IPA /2017 Countering Serious Crime in the Western Balkans.

Përmbajtja

SESIONI I/First Section
Aspekte strategjike të krimit kibernetik
dhe impakti në sigurinë kombëtare

SESIONI II/Second Section

Hetime profesionale të krimeve kibernetike


AKADEMIA E SIGURISË
1971

KONFERENCA E III-të SHKENCORE NDËRKOMBËTARE
Krimi kompjuterik, kërcënimi kibernetik dhe siguria kombëtare
Nëntor 2018, Tiranë

Fokusi i konferencës

Vrulli i zhvillimit të komunikimit masiv në hapësirën kibernetike (virtuale), sidomos pas vitit 2000, orienton drejt një problemi të ri që po kërcënon vrullshëm sigurinë kombëtare: lufta kibernetike dhe krimet kompjuterike. Këto krime, si aktivitete kriminale të zhvilluara në rrjeta, kërcënojnë informacionin, shkëmbimin e informacionit, hapësirën kibernetike dhe shoqërinë e sotme njerëzore. Kjo nxit drejt një lufte të re globale virtuale që kërkon rishikim të politikave e masave mbrojtëse. Në ditët e sotme kjo formë e krimit po përhapet vrullshëm në nivel individual, institucional, organizativ, kombëtar e ndërkombëtar. Zhvillimi i madh i teknologjisë dhe internetit ka mundësuar që pjesa më e madhe e aktiviteteve ekonomike, shkencore, sociale, ligjore, hetuese, policore, politike, etj., të mundësohen e të realizohen nëpërmjet kompjuterit dhe komunikimit virtual.

Nga aspekti hetimor, kjo veprimtari kriminale paraqet vështirësi për t'u gjurmuar, hetuar, ndjekur e zbuluar sepse nuk kufizohet nga kufijtë kombëtarë gjeografikë. Gjithashtu këto krime mund të përgatiten nga kudo dhe kundrejt çdo përdoruesi të kompjuterit, kërkojnë resurse të vogla materiale e humane, kryhen në kohë relativisht të shkurtër, me ose pa praninë e autorit në vendin e kryerjes së veprës penale, si dhe aftësimi për përdorim të kompjuterit nuk është i shtrenjtë dhe është i aksesueshëm nëpërmjet rrjetave e programeve kudo në botë. Autorët e këtyre veprave penale gjenden fizikisht në vende të ndryshme, nga ato ku vijnë pasojat e veprimeve të tyre, ndërkohë që legjislacionet vendase përgjithësisht kufizohen brenda territorit vendas. Nga aspekti strategjik, mbrojtja nga kërcënimet e reja të kufijve virtualë dhe rrjeteve e

sistemeve nga mashtrimet kompjuterike, është çështje e rëndësishme e sigurisë kombëtare. Sipas "Strategjisë për mbrojtjen kibernetike 2018-2020", trendi aktual tregon se incidentet e kësaj natyre do të vazhdojnë të rriten.

Ndërmarrja e projekteve, studimeve e kërkimeve në fushën e krimeve e luftës kibernetike përfshin aplikimet shkencore, punimet, trajtimet, studimet dhe analizat e thelluara lidhur me procedurat, metodat e teknikat hetimore brenda e jashtë vendit; vlerësimin e faktorit të rrezikut dhe ndikimit në shoqëri; digjitalizimin e komunikimit dhe format e reja të mbrojtjes, si dhe me programet, kurikulat e modulet ekzistuese për këtë formë krimi, në kuadër të ndërtimit të strategjive të nevojshme për zhvillimin e vazhdueshëm të kapaciteteve njerëzore e materiale, për përmirësimin e metodave hetimore dhe për bashkëpunime të fushave e nivele të ndryshme në nivel kombëtar e ndërkombëtar.

Në këtë konferencë do të diskutohet rreth masave strategjike, organizative dhe teknike të sigurisë kibernetike në sistemet e komunikimit dhe të informacionit, lidhur me rrezikun e krimeve kompjuterike dhe kërcënimeve kibernetike. Kjo konferencë shërben në kuadrin shkencor, për të ndihmuar institucionet, programet, agjencitë, ekspertët për të nxitur debate konstruktive akademike e për të dhënë sugjerime për masa e politika për mbrojtjen nga kërcënimet në rritje në sigurinë publike në hapësirën kibernetike dhe në aspektin hetimor sa më efektiv, me qëllim nxitjen e bashkëpunimeve në nivel ndërkombëtar e kombëtar, dhënien e ekspertizave e praktikave që ofrojnë risi dhe rekomandimet përkatëse për politikat në vazhdim të Policisë së Shtetit e më gjerë.

Objekti i konferencës

Objekti kryesor i kësaj konference, është paraqitja e analizave e prognozave, nga aspekti i hetimit të krimeve kompjuterike dhe kërcënimeve kibernetike të sigurisë kombëtare e ndërkombëtare. Këto do të konkretizohen me punime të mirëfillta shkencore për të nxitur debate dhe për të trajtuar në nivel të gjerë, kombëtar e ndërkombëtar, rëndësinë dhe nevojën e zgjerimit të dijeve dhe aplikimit të tyre përballë sfidës së hetimit, kërcënimeve të reja të kufijve virtualë dhe parandalimit të krimeve kibernetike në Shqipëri, si dhe hartimin e politikave, masave, kurrikulave e trajnimeve për këtë çështje.

Qëllimi i konferencës

Trajtim në mënyrë shkencore rreth *aspektit proceduralo-hetimor* të krimeve kompjuterike; *aspektit analitik strategjik* të kërcënimeve të krimeve kibernetike dhe terrorizmit kibernetik në sigurinë kombëtare dhe *aspektit akademik,* për paraqitjen e praktikave ekzistuese dhe rekomandime të mëtejshme të kurrikulave, programeve e trajnimeve për fushën e krimeve kibernetike te punonjësit e policisë e më gjerë.

Synimi i konferencës

Kjo konferencë synon të bashkojë njëzëri akademikët, shkencëtarët, profesionistët dhe ekspertët e fushave të shkencave kompjuterike, prokurorë, gjyqtarë, oficerë të policisë gjyqësore, e të tjerë për të ndarë eksperiencat, praktikat, punimet shkencore dhe gjetjet për të gjitha aspektet gjithëpërfshirëse të fushës së krimeve kibernetike.

Tipi konferencës

Konferenca është shkencore ndërkombëtare, në një auditor me staf akademik të

Akademisë së Sigurisë, studiues dhe ekspertë vendas dhe të huaj të çështjeve të sigurisë, drejtues dhe specialistë të strukturave të Policisë së Shtetit, agjencive të tjera ligjzbatuese, përfaqësues të misioneve të huaja policore që asistojnë Policinë e Shtetit, përfaqësues të institucioneve akademike partnere në vend dhe të akademive, kolegjeve, universiteteve policore partnere të huaja.

Struktura e konferencës

Konferenca organizohet në tre sesione:

Sesioni I

Aspektet ligjore, procedurale e hetimore të krimeve kompjuterike, me nënçështje si:

- trajtimi i krimit kompjuterik sipas legjislacionit shqiptar;
- hapat dhe procedurat hetimore për krimet kibernetike;
- parimet, veçoritë dhe trajtimi i provave kompjuterike;
- hulumtime mbi kërkimet, evidentimet, këqyrjet dhe sekuestrimin e provave në fushën e rrjeteve dhe hapësirës kibernetike;
- analiza të thelluara për provat elektronike: mënyrat e paketimit, transportimit e magazinimit;
- paraqitja e formave të mbledhjes dhe ruajtjes së informacionit elektronik;
- problematikat e hetimit të sistemeve dhe të dhënave kompjuterike: praktika vendase e të huaja;
- procedurat hetimore dhe masat e veprimit nga oficerë të policisë gjyqësore për krimet kompjuterike: risi dhe rekomandime;
- veprat penale nëpërmjet krimeve kibernetike;
- roli i policisë në përpjekjet në luftën kibernetike: paraqitja e nevojave për bashkëpunim;
- institucionet e drejtësisë në Shqipëri përballë krimeve kibernetike: problematika, praktika e sugjerime;
- risitë e policisë shqiptare në parandalimin, zbulimin e goditjen e krimeve kompjuterike.

Sesioni II

Analiza strategjike dhe masat organizative të sigurisë kibernetike. Terrorizmi kibernetikë, rreziqet dhe kërcënimet, me nënçështje si:

- analiza strategjike të hapësirës kibernetike dhe kërcënimeve me natyrë kriminale e terroriste pas vitit 2000;
- koncepti i ri i kufijve virtual dhe kërcënimet e sigurisë publike e kombëtare;
- kriza globale e të dhënave personale: kontrolli, kërcënimet dhe mbrojtja e tyre;
- koncepti i inteligjencës artificiale dhe luftës kibernetike;
- raportimi dhe vlerësimi i impaktit të krimit kibernetik; si mund ta inkurajojmë për ta raportuar më shpesh atë?
- paraqitje kronologjike të formave të kërcënimeve të terrorizmit kibernetik;
- bashkëpunimi ndërkombëtar për parandalimin e sulmeve kibernetike;
- kërcënimet kibernetike: impakti dhe shpërndarja e tyre në institucionet shtetërore në Shqipëri;
- bashkëpunimet mes ligjit dhe qeverisjes për të tejkaluar me sukses krimet dhe kriminelët kibernetikë;
- siguria dhe terrorizmi kibernetik;
- paraqitja e profileve të autorëve tipik të krimeve kibernetike;

- praktika dhe rekomandime për mbrojtjen e sigurisë kibernetike brenda dhe jashtë vendit;

- lufta e informacionit *online,* një problem i ri i mbrojtjes së sigurisë kombëtare;

- trajtimi i rritjes së mjeteve miqësore "hacking"; hetime dhe masat për parandalim;

- përpjekjet në nivel kombëtar e ndërkombëtar për parandalimin e krimeve kibernetike;

- menaxhimi i rrezikut të kompjuterizimit të informacionit dhe terrorizmit kibernetik;

- digjitalizimi dhe globalizimi i rrjeteve; kërcënimet e krimet kibernetike në botë, Europë, Ballkan e në Shqipëri;

- format e reja të mbrojtjes nga kërcënimet e jashtme e të brendshme të rrjetave kompjuterike: risi dhe praktika;

- analizë të formave të reja të kërcënimeve nga mashtrimet kompjuterike dhe krimet kibernetike në Shqipëri;

- kërcënimet e sulmeve kibernetike ndaj sigurisë kombëtare të Shqipërisë;

- lufta në hapësirën kibernetike të Ballkanit: pozicioni i Shqipëri dhe niveli i rrezikut;

- sabotimet kompjuterike në vendet fqinje, në Shqipëri e në Europë;

- manipulimet në hapësirën kibernetike dhe rrjetet kompjuterike me anë të terrorizmit kibernetik;

- tekno-terrorizmi dhe veçoritë e tij;

- hakerat, sulmet dhe shfrytëzimi i sistemit kompjuterik;

- shpjegime psikosociale të profileve të terrorizmit kibernetik: simptoma, shkaqe e pasoja.

Sesioni III

Zhvillimi i një platforme për edukim dhe trajnime, për mbrojtjen ndaj krimeve kompjuterike e sulmeve kibernetike, me nënçështje si:

- trajtimi i kurrikulave, programeve mësimore e trajnuese në fushën e krimeve kompjuterike e kërcënimeve kibernetike;

- evidentim të kurrikulave ekzistuese për punonjësit e policisë për trajtimin e krimeve kibernetike: praktika të policisë shqiptare si dhe të policive të vendeve të rajonit dhe jo vetëm;

- rekomandime për kurrikula, programe, trajnime e *workshop*-ëve në akademinë e sigurisë për çështje të kërcënimeve të sigurisë publike e kombëtare nga krimet kompjuterike e kibernetike;

- bashkëpunime në nivele akademike, brenda e jashtë vendit, për nxitjen dhe shpërndarjen të punonjësit e policisë dhe jo vetëm, të njohurive, risive apo praktikave të identifikimit, menaxhimit, hetimit, zbulimit e parandalimit të krimeve kompjuterike.

Pjesëmarrja në konferencë

Pjesëmarrja ishte e hapur: për staf akademik, studentë të Akademisë së Sigurisë, ekspertë e studiues nga radhët e strukturave të Policisë së Shtetit e agjencive të tjera të zbatimit të ligjit, akademikë të institucioneve të tjera të arsimit të lartë publik e privat në vend, studiues e ekspertë të çështjeve të hetimit dhe të sigurisë në vend dhe vende partnere, përfaqësues nga organizma ndërkombëtare partnere të Policisë së Shtetit etj.


AKADEMIA E SIGURISË
AS
1971

~ Sesioni I ~

Aspekte strategjike të krimit kibernetik dhe impakti në sigurinë kombëtare

NATO and Cyber Defence

■ **Ms. Chelsey SLACK**
North Atlantic Treaty Organization (NATO)
Division of Cyber Defence
(Divizioni i Mbrojtjes Kibernetike), Bruksel

Abstrakt

Cyber attacks present a clear challenge to the security of the Alliance and could be as harmful to modern societies as a conventional attack. Recent headlines of cyber attacks targeting critical infrastructure, democratic processes, and their increasing presence in military operations highlight the need for the Alliance to step up its efforts on cyber defence. Cyber defence is therefore a top priority for NATO and its Allies, recognising that strong and resilient cyber defences enable the Alliance to carry out its core tasks of collective defence, crisis management, and cooperative security. The remarks as part of the conference will provide an overview of NATO's current efforts in the area of cyber defence, including recent developments from the 2018 NATO Summit in Brussels. A particular focus will be placed on NATO Allies' national implementation of the Cyber Defence Pledge, as well as the recognition of cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea. NATO's cyber defence partnerships – with other countries, international organisations, industry and academia – will also be highlighted.

Keywords:
NATO, Cyber Defence, cyber attacks, critical infrastructure, Cyber Defence Pledge.

Estonia's cyber defence structure and some of the major challenges

■ **Mr. Tanel SEPP**
Estonian MOD, Cyber Policy Department
Ministria e Mbrojtjes Estoneze (MOD),
Departamenti i Politikave Kibernetike

Abstrakt

This paper attempts to address the Estonia's cyber defence structure and some of the major challenges and tie it up to the strategic level exercise that Estonia did last year – EU CYBRID 2017. EU Defence Ministers participated last year, in "EU CYBRID 2017", a strategic table-top cyber defence exercise. The exercise, the first of its kind, was organised by the Estonian Presidency of the Council of the European Union, the Estonian Ministry of Defence and the European Defence Agency (EDA). The objective of EU CYBRID 2017 was the raising of awareness of cybersecurity incident coordination at political level and of the potential effects of offensive cyber-campaigns. It focused on situational awareness, crisis response mechanisms and strategic communication.

Keywords:
Estonia, cybersecurity, strategic communication, cyber defence structure, crisis response.


AKADEMIA E SIGURISË
AS
1971

CyberChallenge.IT: Të edukojmë brezin e ardhshëm italian të ekspertëve të kibernetikës

■ **Emilio COPPA**
CyberChallenge.IT Anëtar i Bordit Teknik, Universiteti Sapienza i Romës
coppa@di.uniroma1.it.

■ **Daniele Cono D'ELIA**
CyberChallenge.IT Anëtar i Bordit Teknik, Universiteti Sapienza i Romës
delia@dis.uniroma1.it.

■ **Camil DEMETRESCU**
CyberChallenge.IT Koordinator Kombëtar, Universiteti Sapienza i Romës
demetres@dis.uniroma1.it.

■ **Alberto Marchetti SPACCAMELA**
Drejtor i Qendrës së Inteligjencës Kibernetike dhe Sigurisë së Informacionit, Universiteti Sapienza i Romës,
alberto@dis.uniroma1.it.

■ **Paolo PRINETTO**
Drejtor i Konsorciumit Kombëtar Ndëruniversitar për Informatikën (CINI) dhe i CINI Laboratori Kombëtar i Sigurisë Kibernetike, Universiteti Politeknik i Torinos,
paolo.prinetto@polito.it.

Abstrakt

Instituti kërkimor "CybersecurityVentures" ka parashikuar se brenda vitit 2021 do të hapen rreth 3.5 milionë vende pune të reja në fushën e sigurisë kibernetike. Plotësimi i mungesës së talenteve në këtë fushë është thelbësor dhe kërkon përpjekje të koordinuara në kohë nga ana e arsimtarëve, kompanive dhe qeverive. Në këtë punim ne përshkruajmë CyberChallenge.IT, një program në kërkim të talenteve në fushën e sigurisë kibernetike për studentë të grup moshës 16-22 vjeç, i prototipuar në Qendrën për Inteligjencën Kibernetike dhe Sigurinë e Informacionit të Universiteti Sapienza, në Romë, në vitin 2017, dhe i shtrirë në tetë universitete italiane që prej vitit 2018. Programi i organizuar nga Laboratori Kombëtar i Sigurisë Kibernetike CINI, me mbështetjen e Sistemit Informativ Italian për Sigurinë e Republikës, synon të tërheqë studentë të shkëlqyer në fushën e sigurisë kibernetike me rritje të shpejtë, duke adresuar sfidat intelektuale dhe mundësitë e saj unike të karrierës.
Në vitin 2018, programi pranoi rreth 1.900 regjistrime dhe përzgjodhi 160 nxënës premtues nga shkollat e mesme dhe universitetet nga i gjithë vendi, të cilët morën pjesë në një program trajnues 3 mujor i cili mbulonte një spektër të gjerë temash në fushën e sigurisë kibernetike. Programi arriti kulmin në një konkurs kombëtar final të kapjes së flamurit (capture-the-flagcompetition-CTF) ndërmjet tetë ekipeve italiane të përbëra nga studentët më të mirë të çdo vendndodhje të CyberChallenge.IT. Fituesit e konkursit kombëtar u përzgjodhën nga ekipi kombëtar i sigurisë kibernetike i Italisë, i cili përfaqësoi vendin në Sfidën e Sigurisë Kibernetike Evropiane të vitit 2018.

Fjalëkyçe:
siguria kibernetike, trajnimi, CTF, arsimimi, mungesa të aftësive.

1. Hyrje

Mungesa e profesionistëve të aftë në një çështje që sa vjen e bëhet më shumë kritike: në fushën e sigurisë kibernetike, vihet re, ndërsa kompanitë dhe qeveritë përpiqen me vështirësi të plotësojnë pozicione pune me rëndësi të veçantë, të lidhura me të[1, 2]. Një raport i institutit kërkimor "Cybersecurity Ventures" i vitit 2017, ka vlerësuar një mungesë prej rreth 3.5 milion profesionistësh në këtë fushë deri në vitin 2021[3]. Ndërsa organizatat, pranojnë tani faktin, se investimi në sigurinë kibernetike, është thelbësor për të luftuar kostot në rritje të sulmeve kibernetike, disa vende janë duke zhvilluar programe të dedikuara në kërkim të talenteve, shoqëruar me edukimin e brezave të ardhshëm të profesionistëve të aftë.

Rritja e një komuniteti entuziastësh kërkon që t'i tërheqësh ata sa më herët të jetë e mundur gjatë zhvillimit të tyre, të paktën që nga shkolla e mesme, duke stimuluar interesin e tyre për sigurinë kibernetike. Duke qenë se *motivimi* luan një rol themelor në këtë proces, një format trajnimi i vlerësuar gjerësisht bazohet tek konkurset ku pjesëmarrësve u kërkohet të zgjidhin sfida të sigurisë kibernetike në arena virtuale që simulojnë skenarë të botës reale[4]. Midis tyre, lojërat e Kapjes së Flamurit (CTF) janë mjaft të përhapura[5]. Në një CTF, organizatorët përgatisin sfida që mund të zgjidhen qoftë individualisht ose në grup, duke nxitur bashkëpunimin e frytshëm ndërmjet pjesëmarrësve. Zgjidhja e një sfide kërkon kapjen e një *flamuri*, që është një "sekret" i

[1] Evans, K., &Reeder, F. (2010). *A human capital crisis in cyber security: Technical proficiency matters* . CSIS.
[2] Vogel, R. (2016). *Closing the cybersecurity skiles gap* . Revista Salus, 4(2), 32.
[3] Morgan, S. (2017). *Cybersecurity Jobs Report, 2017 Edition. Një raport special nga Botuesit në CybersecurityVentures* . Grupi Herjavec.

fshehur në vetë sfidën nga organizatorët e konkursit. Duke kapur flamuj, konkurrentët fitojnë pikë në varësi të nivelit të vështirësisë së sfidës. Dy formate të zakonshme të CTF janë stili i *rrezikut*, ku qëllimi është të zgjidhim sfida individuale, dhe stili i *sulmit/mbrojtjes*, ku kopje identike të së njëjtit grup të shërbimeve kompjuterike vulnerabël që operojnë në një arenë virtuale janë të aksesueshëm nga pjesëmarrësit, të cilët përpiqen të sulmojnë kopjet e pjesëmarrësve të tjerë ndërsa mbrojnë të vetat, duke zbuluar dhe riparuar dobësitë.

Vende si SHBA-ja, Britania e Madhe, Australia kanë organizuar konkurse CTF në nivel kombëtar për vite me radhë, me thirrje të hapura për entuziastët e kibernetikës, ndërkohë që më shumë vende po iniciojnë programet e tyre të financuara nga shteti apo kompanitë private. Konferenca të tilla si DEF CON organizojnë konkurse të njohura CTF që tërheqin ekipet më të mira në mbarë botën. Një përpjekje e vazhdueshme nga Agjencia e Bashkimit Evropian për Sigurinë e Rrjetit dhe Informacionit (ENISA) është e fokusuar në organizimin e një konkursi vjetor të titulluar *Sfida Evropiane e Sigurisë Kibernetike* (ECSC), ku ekipet kombëtare të BE-së mund të konkurrojnë me njëri-tjetrin, duke promovuar një kulturë etike të sigurisë kibernetike dhe duke edukuar një komunitet të individëve të talentuar që do të udhëheqë fuqinë punëtore evropiane të sigurisë kibernetike në dekadat e ardhshme[6]. Këto iniciativa jo vetëm kontribuojnë për përballimin e mungesës së ekspertizës, por gjithashtu kanë rolin themelor social të sigurimit të ekspertëve të ardhshëm të kibernetikës në një mjedis të sigurt dhe realist të trajnimit, duke i paraprirë mundësisë që këta individë t'i testojnë aftësitë e tyre në mënyrë të paligjshme në sistemet e botës reale.

Në këtë punim, ne ilustrojmë *CyberChallenge.IT*, një projekt për trajnimin në fushën e kibernetikës, i organizuar nga Laboratori Kombëtar i Sigurisë Kibernetike (CINI) dhe i mbështetur nga Sistemi Informativ Italian për Sigurinë e Republikës. Qëllimi i programit, i cili ka për qëllim zbulimin dhe promovimin e talenteve kibernetike të moshës 16-22 vjeçare që jetojnë në Itali, është të riorientojë një pjesë të fuqisë punëtore drejt çështjeve me rëndësi kritike për vendin, duke adresuar kështu mungesën e ekspertizës në fushën e sigurisë kibernetike. Si një objektiv i lidhur, *CyberChallenge.IT* synon të sigurojë një pikënisje për studentët e talentuar që kanë potencial të bëhen lojtarë të rëndësishëm që mund të përfaqësojnë Italinë në konkurset ndërkombëtare të CTF, si ECSC dhe DEF CON. *CyberChallenge.IT* u krijua në vitin 2017 në bashkëpunim *me Qendrën për Inteligjencën Kibernetike dhe Sigurinë e Informacionit* (CIS) të Universitetit Sapienza të Romës.

2. Formati i projektit

Në këtë seksion, përshkruhen zgjedhjet e formatit të programit *CyberChallenge.IT*, duke diskutuar audiencën e tij kryesore të targetuar, dhe se si mund të ofrohet ai në të gjithë vendin, fazat e ndryshme të nevojshme për ta zbatuar, dhe qëndrueshmëria e tij.

2.1 Audienca e targetuar

Programi i dedikohet studentëve që jetojnë në Itali me aftësi të shkëlqyera të logjikës

[4] Cheung, R. S., Cohen, J. P., Lo, H. Z., & Elia, F. (2011). *Challenge basen learning in cyber security education* . Në punimet e Konferencës Ndërkombëtare për Sigurinë dhe Menaxhimin (SAM).
[5] Vigna, G. (2011). *The 2010 international capture the flagcompetition* . IEEE Security&Privacy, 9(1), 12-14.
[6] Panfil, G., &Tulvan, A. (2016). *Education in the Field of Cybersecurity-Need and Purpose* . Eur. J. Pub. Ord. & Nat'l Sec., 29.

dhe të programimit, por pa njohuri të mëparshme të koncepteve të sigurisë kibernetike. Grup mosha është 16-22 vjeç, që në përgjithësi mbulon studentë si të shkollës së mesme dhe asaj të lartë. Duke qenë se aksesi në *CyberChallenge.IT* jepet duke kaluar një test të pranimit pavarësisht nga mosha, aktivitetet e trajnimit janë të njëjta për të gjithë studentët e pranuar. Një audiencë natyrore përfaqësohet nga ish-pjesëmarrës të olimpiadave të informatikës, që përfshin studentë të ndryshëm të shkollave të mesme. Programi gjithashtu synon të rrisë numrin e studenteve femra në sigurinë kibernetike.

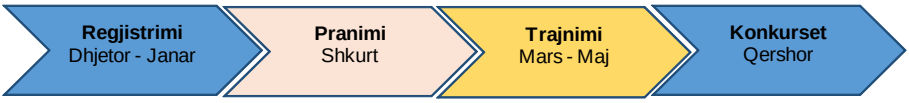


Figura 1: Fazat e *CyberChallenge.IT*.

2.2 Vendet e zhvillimit të programit

Një aspekt i rëndësishëm i programit kombëtar është që t'i ofrohet studentëve nga rajone të ndryshme të vendit një mundësi për të marrë pjesë. *CyberChallenge.IT* është i hapur për të 44 universitetet italiane që janë anëtare të *Laboratorit Kombëtar të Sigurisë Kibernetike*, CINI. Secili universitet pjesëmarrës është përgjegjës për testimin e pranimit dhe për aktivitetet e trajnimit të zhvilluara në vendin përkatës, si dhe për konkursin e *Kapjes së Flamurit*, CTF, që përfshin ekipin lokal të studentëve të pranuar, siç u diskutua në seksionin 2.3.

2.3 Fazat

CyberChallenge.IT artikulohet në 5 faza kryesore, të ilustruara në *Figurën 1.*

*Regjistrimi***.** Studentët e interesuar aplikojnë duke u regjistruar në një ueb-portal të dedikuar[7]. Përveç detajeve personale, secili aplikant paraqet informacionin në lidhje me pozicionin e tij aktual të studimit dhe shpjegon se përse është i interesuar në program.

*Pranimi***.** Testimi i pranimit përzgjedh studentët me aftësi të dallueshme logjike, programuese dhe të zgjidhjes së problemeve, pa njohuri të mëparshme mbi sigurinë kibernetike. Testimi konsiston në dy faza: një testim *online* në formën e kuicit, i cili gjeneron një listë të shkurtër fillestare të pjesëmarrësve, të cilët më pas pranohen të marrin pjesë në një testim në vend, që zhvillohet në secilin ambient lokal. Ndërsa testimi *online* është i aksesueshëm nëpërmjet ueb-portalit të *CyberChallenge.IT*, testimi në vend ka nevojë për ambiente që ofrojnë kompjuterë për një testim të programimit. Qëllimi i procedurës së pranimit është të përzgjidhen 20 studentë nga çdo vend lokal.

*Trajnimi***.** Programi i trajnimit, i zhvilluar gjatë një periudhe kohore prej tre muajsh nga marsi deri në maj, synon të ofrojë një prezantim shkencor, teknik dhe etik të sigurisë kibernetike, së bashku me aftësitë e nevojshme për të marrë pjesë në konkurset CTF të *CyberChallenge.IT*. Programi ka një kohëzgjatje totale rreth 70 orë mësim dhe zhvillohet në çdo vend në intervale kohore në përputhje me aktivitetet e shkollave/universiteteve të tjera (p.sh., të premteve pasdite, të shtunave në mëngjes). Ndryshe nga konkurset e tjera kombëtare, ku garuesit trajnohen vetë duke u angazhuar në sfida që janë publikisht të disponueshme në *Web*, *CyberChallenge.IT* synon të ofrojë një

[7] https://www.*CyberChallenge.IT*.

platformë trajnimi të nivelit hyrës, duke i udhëhequr studentët në zgjidhje hap pas hapi të sfidave të CTF me kompleksitet në rritje, pa pasur njohuri të mëparshme të koncepteve të sigurisë kibernetike.

Konkursi lokal. Një konkurs lokal i CTF në stilin e *rrezikut* organizohet për të përzgjedhur ekipet më të mira të studentëve nga secili vend. Pas konkursit, një panair i rekrutimeve lejon sponsorët lokalë që të takohen me studentët.

Konkursi kombëtar. Programi kulmon në një event kombëtar me pjesëmarrjen e ekipeve më të mira të studentëve nga çdo vend, bazuar në:

1. një *konkurs* kombëtar në vend të *CTF të sulmit/mbrojtjes* ;
2. një *ceremoni* kombëtare të dhënies së *çmimeve* të drejtuar nga përfaqësues nga institucionet italiane;
3. *një panair të rekrutimit* , ku talentet më të mira italiane të kibernetikës takohen me sponsorët kombëtarë.

Gjatë të gjitha fazave të programit, përveç testimit të pranimit, pjesëmarrësit punojnë në laptopët e tyre.

2.4 Qëndrueshmëria

Pjesëmarrja në *CyberChallenge.IT* është pa pagesë për të gjithë studentët. Për këtë arsye, programi kërkon mbështetje substanciale financiare në mënyrë që të jetë funksional. Përveç burimeve njerëzore të nevojshme për të organizuar aktivitetet dhe për të trajnuar studentët, *CyberChallenge.IT* përballet me disa kosto materiale. Për shembull, konkursi përfundimtar ka nevojë për marrjen me qira të një ambienti të përshtatshëm, i cili duhet të jetë i pajisur me tavolina të lidhura me kabllo për ekipet, si dhe lehtësira të rrjetëzimit për ta bërë atë të përshtatshëm për zhvillimin e një konkursi për sigurinë kibernetike.

Burimi kryesor i financimit të *CyberChallenge.IT* janë sponsorizimet nga kompanitë dhe institucionet publike dhe private. Në të vërtetë, sponsorizimi i *CyberChallenge.IT* përfaqëson një mundësi unike për kompanitë: të edukojë një komunitet të ekspertëve të sigurisë kibernetike, të nxisë edukimin e talenteve të reja, të krijojë kontakte të reja me universitete të shquara italiane dhe autoritete kombëtare dhe të rrisë vizibilitetin e tyre në aktiviteteve të rëndësishme shoqërore me ndikim të rëndësishëm në opinionin publik, siç dëshmohet nga mbulimi i gjerë mediatik i edicioneve të vitit 2017 dhe 2018 (seksioni 3.4).

Garat në fushën kibernetike janë katalizatorë të interesit dhe mjete të fuqishme të komunikimit, siç dëshmohet nga shumë kompani që organizojnë lojërat e CTF. *CyberChallenge.IT* nuk bën përjashtim; konkurset rajonale në vendet lokale, *Sfida Kombëtare Finale* dhe pjesëmarrja në *Sfidën Evropiane të Sigurisë Kibernetike* (ECSC) janë mbajtësit e një lidhje territoriale të një identiteti dhe reputacioni të veçantë.

Sponsorizimi i *CyberChallenge.IT* nënkupton krijimin e një mundësie të përbashkët. Duke mbështetur projektin, kompanitë janë partnere dhe jo thjesht sponsore, bashkëgjeneruese të një kulture të sigurisë kibernetike që kontribuon në rritjen ekonomike të Italisë.

Sponsorizimet kombëtare. Sponsorizimet kombëtare ofrojnë vizibilitet në të gjithë vendin, duke filluar nga publikimi i logos së sponsorëve në bluzat zyrtare të *CyberChallenge.IT* dhe në seksionin kombëtar për sponsorët, në varësi të nivelit të përfshirjes së tyre, përfshirë mundësinë për të folur në ceremoninë e çmimeve, pjesëmarrjen në panairin e rekrutimit, përmendjen e emrit të tyre në postimet në

twitter dhe mediat sociale, dhe konsultimi i CV-ve të studentëve.

Sponsorizimet lokale. Sponsorizimet lokale ofrojnë vizibilitet në një ose më shumë nga vendet që presin *CyberChallenge.IT* dhe ofrojnë, ndër të tjera, përfitimet e mëposhtme: publikimi i logos në seksionin e sponsorëve lokalë të faqes kryesore të internetit të *CyberChallenge.IT*; pjesëmarrje në panairin e rekrutimit në vendin lokal; CV-të e studentëve që regjistrohen në ceremoninë e çmimeve lokale. Sponsorit lokalë janë të rëndësishëm për të mbuluar shpenzimet lokale në vendet e pjesëmarrjes.

3. Zbatimi

Në këtë seksion ne do tëpërshkruajmë edicionin e vitit 2018 të projektit, duke diskutuar një shembull konkret të modelit të përshkruar në seksionin 2. Në vitin 2018, në program morën pjesë 8 universitete, duke mbuluar rajone të ndryshme të Italisë: Universiteti Politeknik i Milanos, Universiteti Politeknik i Torinos, Universiteti Sapienza i Romës, Universiteti Ca 'Foscari i Venecias, Universiteti i Xhenovës, Universiteti i Milanos, Universiteti Parthenope i Napolit dhe Universiteti i Padovës. Programi u sponsorizua nga Aizoon, Almaviva, Cisco, ENI, Generali, IBM në nivel *platinum*, Blue5, Leonardo, NTT Data, Rrjetet Palo Alto, Instituti Poligrafik dhe Zecca të shtetit italian në nivelin e *arit* dhe Ernst&Young (EY) dhe Grupi Var në nivelin e *argjendit*.

Figura 2: Statistika tëpjesëmarrësve në Sfidën Kibernetike të vitit2018.

3.1 Pranimi

Regjistrimet u kërkuan nga data 4 dhjetor deri më 20 janar 2018. Në program u paraqitën 1866 aplikime nga i gjithë vendi. Një numër fushatash në *Facebook* i bënë publicitet ngjarjes, duke targetuar kategori të ndryshme të studentëve. Fushata të dedikuara shënjuan vajza të interesuara në fushën e teknologjisë dhe informatikës. Njoftime për shtyp njoftuan për ngjarjen në mbarë vendin dhe ftuan studentët që të merrnin pjesë.

Procedura e pranimit u strukturua në dy faza: një testim paraprak *online*, dhe një testim në vend. Pas regjistrimit në portal, pjesëmarrësit duhet të kalonin një testim online që konsistonte në testime në formë kuici me synimin për të vlerësuar aftësitë e tyre logjike dhe programuese. Nga një total prej 1866 përdoruesve të regjistruar, 1105 përfunduan testimin *online* dhe 1026[8] prej tyre u pranuan në fazën e dytë të procedurës së pranimit.

Për të trajtuar numrin e lartë të kandidatëve (mesatarisht 127 studentë nga çdo vend), pranimi në vend u zhvillua në një ditë dhe u nda në dy pjesë. Në pjesën e parë, në mënyrë të ngjashme me testimin paraprak *online*, studentët duhet t'i përgjigjeshin pyetjeve që synonin vlerësimin e logjikës dhe aftësive programuese të tyre. Nga 1026 studentë të pranuar, 646 prej tyre morën pjesë në pjesën e parë të testimit në vend dhe 441 u pranuan në pjesën e dytë.

Pjesa e dytë e testimit në vend i kërkonte studentëve të zgjidhnin sfida të

[8] Ky ishte numri maksimal i kandidatëve që 8 vendet tona mund të trajtonin gjatë testimit në vend.

programimit të frymëzuara nga probleme të cilat krijohen në fushën e sigurisë kibernetike. Për shembull, një nga sfidat e propozuara ishte e lidhur me format e kyçjes në një formë të caktuar (*patternlocks*) të përdorura në mekanizmat e vërtetimit në telefonat e zgjuar (*smartphones*) modernë. Studentët duhet të shkruanin një program në gjendje të llogariste numrin e formave të mundshme të kyçjes me gjatësi deri në një konstante "K" të ofruar së të dhënave (*input*-it), që mund të realizohet në një tabelë 3x3. Ndërsa kjo sfidë i lejonte kandidatët të përdorin çdo gjuhë moderne programimi sipas zgjedhjes së tyre për të zbatuar zgjidhjen, sfida të tjera të testimit u kërkonin specifikisht studentëve, të shkruanin një program, në gjuhën e programimit "C". Kjo është bërë për të vlerësuar aftësinë e tyre për të trajtuar detaje të nivelit të ulët të arkitekturave moderne të llogaritjes (*computing*).

Nga 441 studentë që morën pjesë në pjesën e dytë të testimit në vend, 160 u pranuan në program e trajnimit, p.sh. 20 në vend.

3.2 Trajnimi

CyberChallenge.IT ka për qëllim tu ofrojë studentëve të pranuar një prezantim të plotë të temave themelore të ndërtimit me të cilat duhet të jetë i njohur çdo ekspert në fushën e sigurisë kibernetikenë ditët e sotme. Për këtë qëllim, fillimisht CINI bëri një identifikim të grupit të elementëve thelbësorë të kibernetikës, ndërsa ekspertë akademikë nga i gjithë vendi u përfshinë në përgatitjen e materialeve trajnuese shumë cilësore që mund të mbulonin këto tema. Për shfrytëzimin e këtyre materialeve, çdo ambient shpenzoi 18 orë leksion duke u fokusuar në tema të tilla si kriptografia (arti i shkrimit apo zgjidhjes së kodeve), programimi i sigurt, autentifikimi dhe kontrolli i aksesit, sulmet kibernetike, protokollet e rrjetit, mbrojtje lokale në thellësi, siguria e përdoruesve fundorë, dhe teknologjia *blockchain*. Përveç kësaj, aspektet etike kanë luajtur një rol vendimtar në të gjithë programin e trajnimit. Për të angazhuar interesin e studentëve dhe për t'i përgatitur ata për konkurset finale, si dhe CTF të tjera ndërkombëtare të organizuara në të gjithë botën, programi përfshiu 48 orë trajnim praktik. Falë një partneriteti me Laboratorin Hacking-Lab, *CyberChallenge.IT* ishte në gjendje tu ofronte universiteteve pjesëmarrësve dhe studentëve të tyre akses në një koleksion të madh sfidash të CTF që u përdorën nga instruktorët gjatë sesioneve praktike.

Së fundi, disa nga sponsorët lokalë dhe kombëtarë kontribuuan në programin e trajnimit me seminare teknike, që ofruan një këndvështrim industrial në një sërë temash të sigurisë kibernetike, duke diskutuar se si të përballemi me kërcënimet e vazhdueshme dhe të qëndrueshme të sigurisë kibernetike që cenojnë klientët e tyre.

Në total, programi i trajnimit zgjati tre muaj, nga muaji mars deri në muajin maj të vitit 2018.

3.3 Konkurset dhe ceremonia e dhënies së çmimeve

Për të përzgjedhur studentët më të mirë që morën pjesë në program, *CyberChallenge.IT* organizoi së pari një konkurs lokal në çdo ambient për të identifikuar kandidatët më të fortë lokalë dhe më pas një konkurs kombëtar ku ekipet nga vende të ndryshme garuan për të provuar aftësitë e tyre kibernetike.

Një kërkesë e rëndësishme për këto konkurse ishte disponueshmëria e një platforme të besueshme që mund të priste (*hosting*) lojërat. Për këtë qëllim, *CyberChallenge.IT* hartoi një zgjidhje të brendshme. Në të vërtetë, vendi nga Venecia, kishte përvojë të gjerë në organizimin e konkurseve të CTF-së dhe si i tillë ishte një partner i natyrshëm

për tu përfshirë për zbatimin e platformës sëlojërave. I frymëzuar nga DEF CON CTF, konkursi më i rëndësishme në botën e hakerave, *CyberChallenge.IT,* organizoi konkursin lokal si një CTF e stilit *të rrezikut* dhe konkursin kombëtar si një CTF e stilit *sulm/ mbrojtje*. Në mënyrë të ngjashme me platformën CTF, sfidat e propozuara gjatë konkurseve finale u zhvilluan së brendshmi me ndihmën e vendeve të ndryshme që morën pjesë në program.

Konkurset lokale u mbajtën më 8 Qershor dhe u zhvilluan në të njëjtën kohë në secilin vend të *CyberChallenge.IT* në të gjithë vendin. Studentët u lejuan të përdornin laptopët e tyre për të zgjidhur sfidat, duke shmangur kështu çdo pengesë jorealiste për mjetet që mund të përdoreshin. Për ta bërë këtë të mundur, platforma lejonte akses në distancë nga çdo vend në të gjithë vendin, duke kërkuar vetëm konfigurimin e një lidhjeje VPN. Pas 8 orëve në lojë, çdo vend përzgjodhi katër studentët më të mirë nga renditja lokale dhe u dha atyre të drejtë si ekip që do tëpërfaqësonin vendin lokal gjatë konkursit kombëtar. Gjatë ceremonisë lokale të dhënies së çmimeve, sponsorët patën mundësinë të takonin studentët dhe të angazhoheshin në një event të panairit të rekrutimit.

Konkursi kombëtar u mbajt më 26 qershor në Muzeun e Artit Klasik të Universitetit Sapienza të Romës. 8 ekipet luajtën për 8 orë kundër njëri-tjetrit në një CTF të stilit *sulm /mbrojtje*. Platforma u vendos (*host*) në vend, në një server të dedikuar, për të shmangur çështje të besueshmërisë së rrjetit dhe ekipet u lidhën drejtpërdrejtë me platformën falë një rrjeti lokal të lidhur me kabllo që ishte krijuar specifikisht për konkursin. Në mënyrë të ngjashme me CTF lokale, studentët mund të përdorin laptopët e tyre për të luajtur lojën.

Më 27 qershor, tre ekipeve kryesore iu dhanë çmime gjatë një ceremonie që përfshinte institucione të ndryshme akademike, industriale dhe institucione qeveritare. Përveç kësaj, panairi i rekrutimit u krijoi mundësi sponsorëve kombëtarë të takonin pjesëmarrësit e *CyberChallenge.IT*, duke diskutuar mundësitë për trajnim të mëtejshëm dhe punësim.

3.4 Impakti

CyberChallenge.IT pati një ndikim thelbësor në komunitetin italian të kibernetikës dhe dha një kontribut për rritjen e ndërgjegjësimittë opinionit publik për rëndësinë e investimit në sigurinë kibernetike.

Pasqyrimi në media. Edicioni i *CyberChallenge.IT* për vitin 2018 pati një pasqyrim të gjerë në shtyp dhe në media në të gjithë vendin. Artikuj të ndryshëm u shfaqën në agjencitë kombëtare të lajmeve dhe gazeta si *La Repubblica* , *Corriere della Sera* , *Il Manifesto* , *Avvenire, Il Sole 24 ore, L'Espresso* , *Agenzia Giornalistica Italia* , *ANSA* , dhe disa të tjera. Gjithashtu, *CyberChallenge.IT* u prezantua në raportime të ndryshme nga rrjeti kombëtar i transmetimeve, di *RAI* dhe *Mediaset* .

Një pasojë e rëndësishme e pasqyrimit të *CyberChallenge.IT* në medien kombëtare ishte një përmirësimi i ndërgjegjësimit sa i takon kërcënimeve të sigurisë kibernetike. Në të vërtetë, *CyberChallenge.IT* kontribuoi në një shpjegim që u bë për audiencën e gjerë se pse krimi kibernetik është shumë i rëndësishëm në ditët e sotme për jetën tonë të përditshme, duke theksuar se si edhe veprime të vogla naive, si për shembull të zgjedhim një fjalëkalim të dobët, mund të na kanosë një risk për sigurinë tonë. Edukimi është realisht jetik që Italia të përmirësojë nivelin e saj të pjekurisë së sigurisë kibernetike dhe të ndihmojë industritë kombëtare të konkurrojnë në tregun global.

Mundësi punësimi. Tregu i sigurisë kibernetike është rritur në mënyrë eksponenciale gjatë dekadës së fundit. Siç e kemi observuar tashmë, një problem kyç me të cilin përballen organizatat private dhe publike është mungesa e ekspertëve të trajnuar shumë mirë, të disponueshëm në tregun e punës. *CyberChallenge.IT* luan një rol të rëndësishëm në këtë skenar, duke u përpjekur të tërheqë talente të reja drejt sigurisë kibernetike, duke i trajnuar ata, dhe duke ndihmuar qeverinë dhe industritë të krijojnë kontakt me studentë me aftësi të dallueshme. Në vitin 2018, një nga përfitimet e ofruara për sponsorat kombëtarë ishte mundësia për të vlerësuar CV-të e pjesëmarrësve në programin trajnues, mundësisht duke lehtësuar mundësitë e punësimit. Si një objektiv afatgjatë, *CyberChallenge.IT* synon të ndërtojë një rrjet të ekspertëve të kibernetikës në të gjithë vendin që do të jetë shumë i rëndësishëm për sigurinë kibernetike dhe rritjen ekonomike të Italisë.

Ekipi kombëtar italian i sigurisë kibernetike. Nucleo di Sicurezza Cibernetica (NSC) i ka besuar zyrtarisht Laboratorit Kombëtar të Sigurisë Kibernetike, CINI, detyrën e formimit të ekipit kombëtar italian të sigurisë kibernetike duke përzgjedhur talentet më të mira nga programi *CyberChallenge.IT*. Ekipi kombëtar do të marrë pjesë në edicionin e vitit 2018 të *Sfidës Evropiane të Sigurisë Kibernetike* (ECSC), konkurs i organizuar nga Agjencia e Bashkimit Evropian për Sigurinë e Rrjetit dhe të Informacionit (ENISA), që do të zhvillohet në Londër nga data 14 deri më 18 tetor.

Në vitin 2017, ekipi kombëtar, i mbështetur nga Ministria Italiane për Zhvillimin Ekonomik (MISE), mori pjesë për herë të parë në ECSC, duke fituar medaljen e bronzit (*ex-aequo* me Mbretërinë e Bashkuar). Ekipi ishte i formuar nga fituesit e edicionit të vitit 2017 të *CyberChallenge.IT* dhe të rinj të tjerë të talentuar nga Universiteti Ca' Foscari i Venecias dhe Universiteti Politeknik i Milanos.

Zhvillimi i komunitetit. Një nga rezultatet kyçe të programit *CyberChallenge.IT* është krijimi i një rrjeti entuziastësh të sigurisë kibernetike. Realisht, programi dëshmoi se ishte instrumental në zhvillimin e një komuniteti që shtrihet shumë përtej kufijve të mjediseve akademike që e kanë krijuar dhe pritur (*host*) atë.

Studentë nga vendet e *CyberChallenge.IT* po fillojnë të ndërtojnë ekipe lokale të pavarura me qëllimin për të konkurruar në konkurset ndërkombëtare të CTF që organizohen në të gjithë botë. Për shembull, pjesëmarrësit nga edicioni i vitit 2017 të *CyberChallenge.IT* themeluan ekipin *The Roman Xpl0it*, i cili ka arritur tashmë nivelet më të larta në lojëra të ndryshme ndërkombëtare CTF që atëherë.

Akoma dhe më shumë mbresëlënëse është historia e *mHackeroni* . Ky ekip i pavarur, u krijua në vitin 2018, duke bashkuar forcat e 5 ekipeve italiane CTF (*The Roman Xpl0it, JBZ, Tower of Hanoi, n0pwnintended, c00kiesATvenice)* me qëllimin final për pranimin e ekipit italian në DEF CON, konkursi më i rëndësishëm i hakerave CTF në të gjithë botën. *mHackeroni* mori vendin e dytë gjatë kualifikimi të DEF CON dhe shkoi në Las Vegas në verën e vitit 2018 për të luajtur lojën në vend, ku u rendit në vendin e 7^{të}. Ky ishte rezultati më i mirë në historinë e komuniteti italian të hakerimit që prej krijimit të DEF CON në vitin 1993.

4. Konkluzione

Në këtë punim, ne kemi përshkruar *CyberChallenge.IT*, një program kombëtar italian trajnues për sigurinë kibernetike kushtuar studentëve të moshës 16-22 vjeç. Ndryshe nga sfidat kibernetike *(cyber challenges)* të zhvilluara në shumicën e vendeve

të tjera, *CyberChallenge.IT* jo vetëm organizon konkurse kombëtare të CTF, por gjithashtu përfshin një program arsimor formues që synon të ndihmojë studentët e shkëlqyer të njihen me elementët thelbësorë të sigurisë kibernetike dhe të trajnohen me aktivitete të zgjeruara praktike. Edicioni i tretë i programit, i cili do të mbahet në vitin 2019, po vjen me më shumë vende të përfshira dhe me ambicien për të përmirësuar procesin dhe për të kontribuar në barazinë gjinore duke tërhequr vajza të talentuara në fushën e sigurisë kibernetike.

Mirënjohje

Programi *CyberChallenge.IT* mbështetet me krenari nga Sistemi Informativ Italian për Sigurinë e Republikës. Projekti nuk do të kishte qenë i mundur pa punën e madhe të shumë njerëzve. Ne i detyrohemi Roberto Baldonit, i cili i pari pati idenë e krijimit të *CyberChallenge.IT* dhe ka pasur një rol të rëndësishëm në formësimin e projektit dhe prototipimin e tij në Universitetin Sapienza të Romës në vitin 2017. Ne, dëshirojmë të falënderojmë gjithashtu, Angela Miola-n dhe të gjithë ekipin e CINI-t për mbështetjen e tyre të paçmueshme. Luana Colia dhe Gabriella Caramagno, kanë kontribuar shumë në organizimin e projektit, ndaj ne jemi mirënjohës ndaj tyre për mbështetjen. Shumë falënderime i shkojnë Marco Squarcina dhe Francesco Palmarini, të cilët kanë zhvilluar infrastrukturën e CTF të *CyberChallenge* të vitit 2018 dhe kanë koordinuar përpjekjet në krijimin e sfidave për konkurset finale. Ne vlerësojmë përzemërsisht punën e madhe të së gjithë instruktorëve të universiteteve pjesëmarrëse, të cilët kanë kontribuuar në aktivitetet trajnuese. *CyberChallenge.IT* është bërë i mundur, falë mbështetjes së paçmuar të një numri partnerësh industrialë, që kanë financuar programin dhe kanë marrë pjesë në sesionet e trajnimeve me studentët. I falënderojmë me mirënjohje të gjithë ata, duke theksuar vlerën themelore e shoqërore të investimit të tyre. E fundit, por jo më pak e rëndësishmja: falënderojmë të gjithë studentët tanë të *CyberChallenge.IT* për pasionin dhe entuziazmin e tyre. Ata janë shpresa jonë e vetme për një botë më të mirë!

Bibliografia

1. Cheung, R. S., Cohen, J. P., Lo, H. Z., & Elia, F. (2011). *Challenge basen learning in cyber security education* Në punimet e Konferencës Ndërkombëtare për Sigurinë dhe Menaxhimin (SAM).
2. Evans, K., & Reeder, F. (2010). *A human capital crisis in cybersecurity: Technical proficiency matters* . CSIS.
3. Panfil, G., & Tulvan, A. (2016). *Education in the Field of Cybersecurity-Need and Purpose* . Eur. J. Pub. Ord. & Nat'lSec., 29.
4. Morgan, S. (2017). *Cybersecurity Jobs Report, 2017 Edition. Një raport special nga Botuesit në CybersecurityVentures* . Grupi Herjavec.
5. Vigna, G. (2011). *The 2010 international capture the flagcompetition* . IEEE Security&Privacy, 9(1), 12-14.
6. Vogel, R. (2016). *Closing the cybersecurity skiles gap* . Revista Salus, 4(2), 32.

Perceptimet shqiptare për krimin kompjuterik dhe sigurinë kibernetike

■**Dr. Xhavit SHALA**
Drejtor i Qendrës së Kërkimeve Shkencore,
Akademia e Sigurisë
xhavit.shala@asp.gov.al

Abstrakt

Qëllimi i këtij punimi është skanimi, analizimi dhe vlerësimi i perceptimeve të qytetarëve të Republikës së Shqipërisë për krimin dhe sigurinë kibernetike në Shqipëri. Të dhënat që përdoren në këtë punim janë siguruar nëpërmjet anketimit të kryer me pjesëmarrje të gjerë të qytetarëve, të cilët iu përkasin shtresave e profesioneve të ndryshme. Këto të dhëna na informojnë mbi perceptimet e qytetarëve lidhur me rolin dhe ndikimin e teknologjisë së informacionit e komunikimit në raport me shoqërinë e individin; nivelit e njohurive mbi veprat penale në fushën kompjuterike dhe të kërcënimit të krimit kibernetik, nivelin e sigurisë kibernetike si dhe të perceptimeve të tyre rreth legjislacionit e hetimit të këtij krimi si dhe rrugëve të parandalimit të tij. Nëpërmjet analizimit të këtyre perceptimeve synohet evidentimi i problematikave, faktorëve ndikues si dhe dhënia e rekom7andimeve për përmirësimin e politikave për parandalimin e reduktimin e tyre, në shërbim të përmirësimit të mëtejshëm të procesit të një policimi bazuar në inteligjencë dhe të sigurisë tonë kombëtare. Gjatë këtij punimi janë aplikuar metodat dhe instrumentet bazë kërkimore shkencore. Gjetjet e këtij punimi vërtetojnë plotësisht hipotezën tonë se krimi kompjuterik dhe kërcënimi kibernetik vazhdojnë të gjejnë përhapje në Shqipëri ndërmjet të tjerave dhe për shkak të mangësive të theksuara të ndërgjegjësimit/sensibilizimit dhe të edukimit të kategorive shoqërore e shtresave shoqërore me rrezikun e përdorimit të pakontrolluar e të pasigurt të internetit e të teknologjisë së informacionit e komunikimit. Në përfundim të punimit jepen rekomandimet përkatëse për zhvillimin e politikave për të përmirësuar punën në vazhdim lidhur me mënyrën e trajtimit, menaxhimit, parandalimit dhe reduktimit të krimit e kërcënimit kibernetik në vendin tonë.

Fjalëkyçe:

Vepra penale në fushën kompjuterike, krimi kibernetik, internet, anketim, siguria kibernetike, kërcënimi kibernetik, edukim, trajnim.

1. Hyrje

Teknologjia e informacionit si një tërësi e teknologjive për mbledhjen, ruajtjen, gjetjen, përpunimin, analizimin, dhe transmetimin e informacionit si dhe interneti, gjithnjë e më tepër po ndërthuret me jetën ekonomike, sociale e politike të individëve, familjeve, organizatave, shteteve e kombeve. Megjithatë, ashtu siç është e pafund lista e shërbimeve që ofron përdorimi i internetit dhe hapësirës kibernetike, po aq duket së janë dhe rreziqet që kërcënojnë këto shërbime nëse keqpërdoret interneti dhe hapësira kibernetike. Keqpërdorimi i internetit dhe hapësirës kibernetike i kthen këto në rreziqe e kërcënime në një "Thembër Akili" për shoqërinë bashkëkohore të informacionit. Interneti ju mundëson edhe kriminelëve një mundësi më shumë për t'u rritur dhe përhapur. Sot nuk mund të flitet ndaras për krimin kompjuterik, kërcënimin kibernetik apo sigurinë kibernetike, por për individ, familje, shoqëri, organizata, kombe, kriminalitet, kërcënime e siguri, të gjitha së bashku në një hapësirë kibernetike. Tashmë edhe njerëzit nuk janë më të zakonshëm si dikur. Ata janë bërë *cybercitizens*, banorë të hapësirës kibernetike, "qytetarë digjital" të lidhur më shumë se kurrë më njëri tjetrin. Për këtë Bashkimi Evropian ka përcaktuar në strategjinë e tij për sigurinë kibernetike se të drejtat themelore, demokracia dhe sundimi i ligjit duhet të mbrohen në hapësirën kibernetike[1].

Zhvillimi i vrullshëm i komunikimit masiv në hapësirën kibernetike (virtuale), sidomos pas vitit 2000, po i përball strukturat e Policisë së Shtetit, të agjencive të tjera të zbatimit të ligjit si dhe strukturat e sigurisë me një problematikë të re, në një rritje

[1] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels, 7.2.2013.

progresive të veprave penale në fushën kompjuterike, por edhe të kërcënimit kibernetik. Veprat penale në fushën kompjuterike, janë aktivitete kriminale të zhvilluara në rrjete që kanë si objekt keqpërdorimin e sistemeve dhe të dhënave kompjuterike. Kjo formë e re e veprimtarisë kriminale, e njohur ndërkombëtarisht dhe e pranuar edhe në Shqipëri si krimi kibernetik[2] është e vështirë për t'u hetuar. Në vendin tonë, në vitin 2017, krahasuar me vitin 2010 janë evidentuar 335% më shumë vepra penale në fushën e krimeve kompjuterike dhe janë zbuluar vetëm 27% të autorëve të këtyre veprave penale[3].

Ndërkohë, janë rritur ndjeshëm kërcënimet[4]/sulmet kibernetike, si përpjekje të qëllimshme për të marrë akses, manipuluar, ndërhyrë ose dëmtuar integritetin, konfidencialitetin, sigurinë ose disponibilitetin e të dhënave të sistemeve kompjuterike, pa pasur autoritet ligjor për ta bërë këtë[5]. Kriminelët kibernetikë po përdorin metoda gjithnjë e më të sofistikuara për t'u futur në sistemet e informacionit dhe vjedhjen e të dhënave kritike. Rritja e spiunazhi ekonomik dhe aktivitetet e sponsorizuara nga shteti në hapësirën kibernetike përbëjnë një kategori të re të kërcënime për qeveritë dhe kompanitë e BE-së[6].

Në strategjinë tonë të sigurisë kombëtare sulmet kibernetike klasifikohen tashmë në rreziqet e nivelit të parë. Ato kanë potencial për të dëmtuar rëndë shkëmbimin e informacionit në institucionet publike, të telekomunikacionit dhe sistemin financiar e bankar, duke shkaktuar edhe ndërprerje të shërbimeve jetike[7].

Për identifikimin e problematikave që lidhen me krimin dhe sigurinë kibernetike, të faktorëve ndikues e të rrugëve për përballimin e tyre, përveç të tjerave është e domosdoshme të administrohen dhe analizohen edhe perceptimet e shqiptarëve - *cybercitizens* rreth këtyre çështjeve. Për këtë arsye është organizuar një anketim i gjerë i kategorive e profesioneve të ndryshme të shoqërisë shqiptare dhe janë analizuar perceptimet e tyre rreth rolit e ndikimit të teknologjisë së informacionit e komunikimit e në raport me shoqërinë e individin; nivelit të njohurive të tyre mbi veprat penale në fushën kompjuterik, të kërcënimit të krimit kibernetik e të nivelit të sigurisë kibernetike si dhe perceptimet e tyre rreth legjislacionin, hetimit dhe rrugëve të parandalimit të këtyre veprave penale dhe jo vetëm. Për më tepër në vijim të punimit.

2. Metodologjia e anketimit

2.1 Marrja e kampioneve

Nisur nga qëllimi i punimit, për të organizuar një anketim të gjerë u përzgjodhën për të anketuar qytetarë të shtresave e profesioneve dhe konkretisht: gjyqtarë, prokurorë, kandidatë për magjistrat, përfaqësues të biznesit të vogël, përfaqësues të biznesit të madh, punonjës të sistemit bankar, punonjës policie, punonjës të Gardës së Republikës,

[2] Dokumenti i Politikave për Sigurinë Kibernetike 2015-2017, miratuar me VKM Nr. Nr. 973, datë 02.12.2015. Faqe 8.

[3] Informacion përmbledhës i analizave të Sektorit për Hetimin e Krimeve Kompjuterike, për vitet 2016 2018, dinamika e punës, prioritetet, kërkesat".

[4] Kërcënimet mund të kenë origjina të ndryshme, duke përfshirë sulme kriminale, të motivuara politikisht, sulme terroriste apo të sponsorizuar nga shtetet si dhe fatkeqësi natyrore e gabime të paqëllimshme

[5] Dokumenti i Politikave për Sigurinë Kibernetike 2015-2017, miratuar me VKM Nr. Nr. 973, datë 02.12.2015. Faqe 7. Burim i cituar.

[6] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels, 7.2.2013. Burim i cituar.

studentë, nëpunës, arsimtarë, punëtorë, fermerë, pension, të pa zënë në punë.

Të gjithë kategoritë e mësipërme, të shënjuara, u përzgjodhën sepse janë jo vetëm *cybercitizens*, por edhe aktorë e faktorë në hapësirën kibernetike shqiptare.

2. 2. Përmbajtja e pyetësorit

Për të gjitha kategoritë u përdor i njëjti model pyetësori. Pyetësori u konceptua dhe u ndërtua me gjashtë pjesë:

- Në pjesën e parë u kërkuan të dhënat demografike të personit që plotëson pyetësorin si mosha, gjinia, arsimi e profesioni.

- Në pjesën e dytë u synua të merret informacion rreth perceptimeve të të anketuarve për teknologjinë e informacionit & komunikimit dhe sigurinë që ofron ajo, raportet e saj me shoqërinë, privatësinë e individit si dhe etikën në komunikimet *online*.

- Në pjesën e tretë u synua të sigurohet informacioni i nevojshëm për njohuritë e të anketuarit rreth veprave penale në fushën e krimeve kompjuterike si dhe të perceptimeve të tyre rreth aktiviteteve kriminale në fushën kibernetike, pavarësisht nëse ata janë përfitues apo të dëmtuar nga këto aktivitete.

- Në pjesën e katërt u kërkua të merret informacioni i duhur rreth perceptimeve të të anketuarve për gjendjen aktuale të kriminalitetit në fushën kibernetike, formave më të përhapura, gjinisë, moshës, arsimit, shtrirjes gjeografike dhe motiveve që i shtyjnë autorët të përfshihen në krimin kibernetik. Këto të dhëna të grumbulluara, na ndihmojnë të realizojmë një analizë të gjendjes së kriminalitetit në fushën kibernetike nisur nga treguesit subjektivë.

- Në pjesën e pestë u synua të sigurohet informacioni i nevojshëm me perceptimet e të anketuarve rreth nivelit të sigurisë kibernetike dhe shkallës së kërcënimit kibernetik në Shqipëri.

- Në pjesën e gjashtë dhe të fundit u kërkua të sigurohet informacioni i nevojshëm për perceptimet e të anketuarve rreth legjislacionit, hetimi dhe parandalimi të krimit kibernetik.

Pyetjet janë ndërtuar në mënyrë të tillë që të na sigurojnë informacion të krahasueshëm. Pyetësori është tërësisht i standardizuar, me pyetje të mbyllura dhe të orientuara në përgjigje. Alternativat e përgjigjeve janë të vendosura në formë matrice, në trajtën e shkallëve të rëndësisë (1, 2, 3, 4, 5)[8].

Nga pyetësori i standardizuar ne arritëm të sigurojmë nga burime parësore informacion të krahasueshëm. Ky informacion i grumbulluar na mundësoi të bëjmë analiza të kryqëzuara të të dhënave të cilat ndikuan ndjeshëm në gjetjet interesante të këtij punimi si dhe në hartimin e rekomandimeve rreth krimit kompjuterik e sigurisë kibernetike në Shqipëri.

2.3. Mënyra e shpërndarjes dhe plotësimit të pyetësorit

Për herë të parë ne organizuam anketimin *online* me programin "Enalyzer", duke ju dhënë mundësi pjesëtarëve të grupeve të përzgjedhura, që sipas dëshirës së tyre të merrnin pjesë në këtë anketim, duke plotësuar *online* nga kompjuteri apo *smartphone*-i i tyre, në adresën elektronike https://surveys.enalyzer.com/?pid=f2q2s5r7, pyetësorin

[7] Strategjia e Sigurisë Kombëtare të Republikës së Shqipërisë, miratuar me Ligjin Nr. 103/2014.

[8] Sipas nivelit i korrespondon: shkalla 1 – aspak ; shkalla 2 – pak; shkalla 3 – disi; shkalla 4 – mjaftueshëm dhe shkalla 5 – shumë. Të anketuarit zgjedhin gjithmonë një shkallë vlerësimi për çdo kategori apo nënkategori, sipas pyetjeve të pyetësorit.

e përgatitur nga ana jonë.

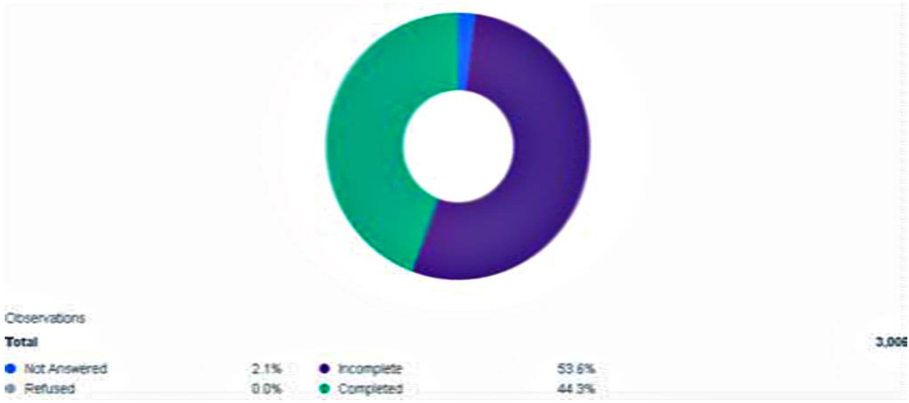
2.4. Realizimi i procesit të anketimit

Procesi i anketimit u zhvillua në një hark kohor prej 7 ditësh. Deri më datën 14 shtator 2018, në ora 11:53, në anketim kanë marrë pjesë 3006 persona. Nga këta 44.3% (1334 persona) e kanë përfunduar plotësisht anketimin, 53.6% (1611 persona) nuk e kanë përfunduar plotësisht anketimin ndërsa 2.1% nuk e kanë plotësuar atë (Grafiku 1).

Në analizën tonë, shifra prej 53.6% e pjesëmarrësve që nuk e kanë përfunduar plotësisht anketimin lidhet si me mungesën e një përgjegjshmërive sociale të një pjesë jo të vogël të pjesëtarëve të grup-shënjestrave të përzgjedhura për të marrë pjesë në anketime të tilla për probleme kaq të rëndësishme për shoqërinë shqiptare po aq dhe me mungesën e eksperiencës së tyre në anketimet *online* apo dhe për arsye teknike, pasi nuk kanë klikuar në fund të procesit të plotësimit të pyetësorin në "End Survey".

Grafiku 1

Powered by Enalyzer | September 14, 2018, 11:53



Për interesa të këtij studimi, ne do të përpunojmë dhe analizojmë treguesit dhe përgjigjet e atyre pjesëmarrësve në anketim që e kanë kompletuar intervistën nga pyetja e parë deri tek e fundit. Këta përbëjnë 44.3% të pjesëmarrësve ose gjithsej 1334 persona. Ky kampion përmbush plotësisht standardet ndërkombëtare të një anketimi profesional.

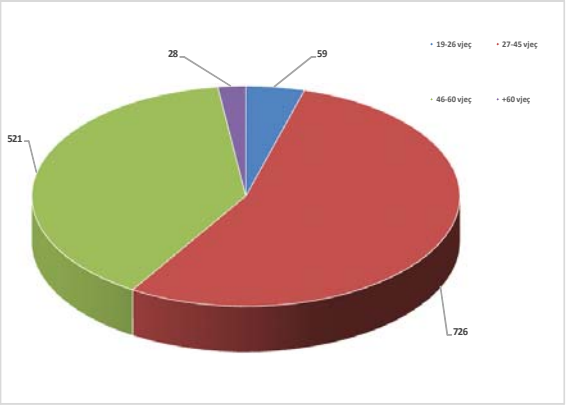
3. Përbërja e kampioneve sipas grupmoshës, gjinisë, arsimit e profesionit

Në pjesën e parë të pyetësorit janë përfituar të dhënat rreth grupmoshës, gjinisë, arsimit e profesionit si më poshtë.

3.1 Grupmosha e kampioneve

Të anketuarit sipas grupmoshave në paraqitje tabelore dhe grafike janë si më poshtë:

GRUPMOSHA			
		Frekuenca	Përqindja
Të Vlefshme	19-26 vjeç	59	4.4
	27-45 vjeç	726	54.4
	46-60 vjeç	521	39.1
	+60 vjeç	28	2.1
	Total	1334	100.0

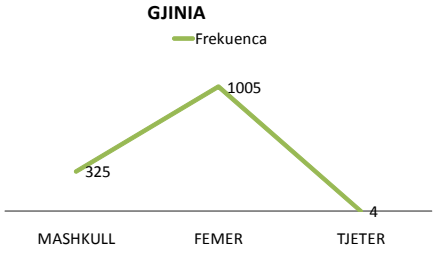


Nga analiza krahasuese e gjetjeve të mësipërme mund të arrijmë në përfundimin se, në anketim kanë marrë pjesë nga të gjithë grupmoshat të cilave iu është adresuar pyetësori. Më shumë e përfaqësuar është grupmosha 27-45 vjeç dhe 46-60 vjeç. Duket këto dy grupmosha kanë pasur më shumë interes për fushën e krimeve dhe sigurisë kibernetike. Më pak të përfaqësuara janë grupmoshat mbi 60 vjeç dhe 19-26 vjeç.

3.2 Gjinia e kampioneve

Të anketuarit sipas gjinisë, në paraqitje tabelore dhe grafike janë si më poshtë:

GJINIA			
		Frekuenca	Përqindja
Të Vlefshme	MASHKULL	325	24.4
	FEMER	1005	75.3
	TJETER	4	.3
	Total	1334	100.0

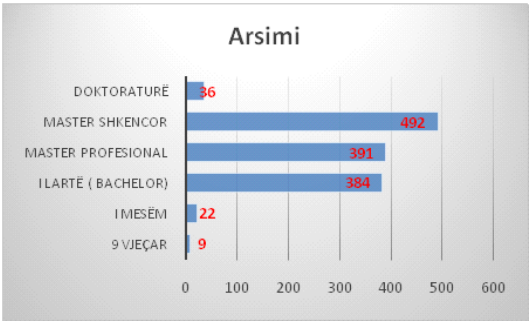


Nga kjo mund të arrijmë në përfundimin se të anketuarit femrat kanë qenë më të interesuara dhe më të ndjeshme për tematikën e anketimit, me një përgjegjshmëri më të madhe sociale se meshkujt si dhe më të sakta në plotësimin e pyetësorit nga fillimi në fund.

- Niveli arsimor i kampionimit.

Niveli arsimor i të anketuarve, në paraqitje tabelore dhe grafike është si më poshtë:

ARSIMI			
		Frekuenca	%
Të Vlefshme	9 vjeçar	9	0.7
	I Mesëm	22	1.6
	I lartë (Bachelor)	384	28.8
	Master Profesional	391	29.3
	Master Shkencor	492	36.9
	Doktoraturë	36	2.7
	Total	1334	100.0

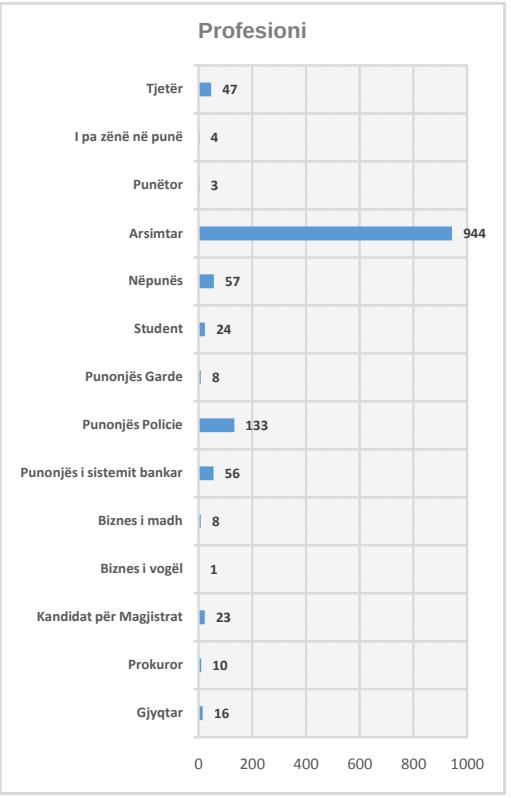


Nga analiza krahasuese e të dhënave të mësipërme, mund të arrijmë në përfundimin se 97.7% e kampionimit ka një nivel të lartë arsimor (bachelor, master dhe doktoraturë). Kjo na bën optimist në cilësinë e përgjigjeve të tyre, por njëkohësisht na obligon që në të ardhmen të organizojmë një anketim tjetër në mënyrë që të njohim dhe perceptimet dhe shkallën e njohurive për krimin kibernetik të grupmoshave nën 26 vjeç, të cilat janë shumë aktive në përdorimin e internetit dhe të teknologjisë së informacionit.

- Kampionimi sipas përbërjes profesionale.

Të anketuarit sipas profesionit, në paraqitje tabelore dhe grafike janë si më poshtë:

Profesioni			
		Frekuenca	%
Të Vlefshme	Gjyqtar	16	1.2
	Prokuror	10	0.7
	Kandidat për Magjistrat	23	1.7
	Biznes i vogël	1	0.1
	Biznes i madh	8	0.6
	Punonjës i sistemit bankar	56	4.2
	Punonjës Policie	133	10.0
	Punonjës Garde	8	0.6
	Student	24	1.8
	Nëpunës	57	4.3
	Arsimtar	944	70.8
	Punëtor	3	0.2
	I pa zënë në punë	4	0.3
	Tjetër	47	3.5
	Total	1334	100.0



Nga analiza krahasuese e gjetjeve të mësipërme të përbërjes profesionale të kampionimit mund të arrijmë në përfundimin se ai ka një përfaqësim e larmi ku numrin më të madh e përbëjnë arsimtarët (70.8%) dhe punonjësit e policisë (10%) ndërsa më pak nga bota e biznesit dhe punëtorët. Kategoritë që përfaqësohen në këtë kampionim jo vetëm janë vetë përdorues të internetit dhe teknologjisë së informacionit, por janë dhe aktorë në luftën kundër krimit kibernetik (gjyqtarët, prokurorët, punonjësit e policisë dhe arsimtarët). Gjithashtu mund të arrijmë në përfundimin se arsimtarët, në raport me gjyqtarët, prokurorët dhe punonjësit e policisë, tregojnë një nivel përgjegjshmëri më të madhe sociale, duke u angazhuar në anketime në probleme kaq të rëndësishme për shoqërinë shqiptare, siç është krimi kompjuterik dhe siguria kibernetike.

4. Gjetjet e procesit të anketimit dhe analizimi i tyre

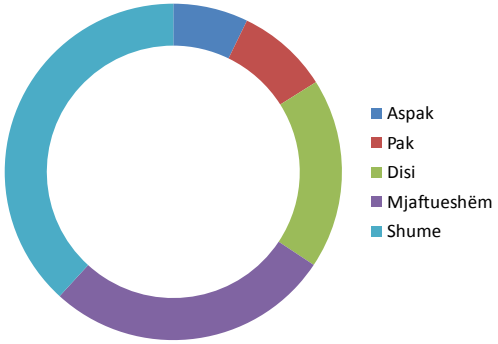
Në këtë punim, për shkak dhe të hapësirës në dispozicion, ne do të analizojmë një pjesë së të dhënave të këtij anketimi e kryesisht ato që lidhen me perceptimet për sigurinë kibernetike. Sipas Strategjisë së Bashkimit Evropian për Sigurinë Kibernetike, për një hapësirë kibernetike të hapur, të sigurt dhe të mbrojtur, siguria kibernetike përpiqet të ruajë disponueshmërinë dhe integritetin e rrjeteve dhe infrastrukturës, si dhe fshehtësinë e informatave që mbahen në to[9]. Ndërsa, Organizata Ndërkombëtare e Standardizimit (ISO) përkufizon sigurinë kibernetike si "ruajtje të konfidencialitetit, integritetit dhe disponueshmërisë së informatave në hapësirën kibernetike". Definicionet e tjera e definojnë sigurinë kibernetike si objektiv të dëshiruar të fushës së sigurisë së TI-së, në të cilën rreziqet e hapësirës globale kibernetike ngushtohen deri në një minimum të pranueshëm[10].

4.1 Gjetjet lidhur me perceptimet e të anketuarve për sigurinë kibernetike sipas pyetjeve të adresuara

- Përgjigjet e të anketuarve për pyetjen se sa ndikon zhvillimi i teknologjisë së informacionit dhe komunikimit në fushën e privatësisë, më paraqitje tabelore dhe grafike janë si më poshtë:

Sipas jush, sa ndikon zhvillimi i teknologjisë së informacionit dhe komunikimit në fushën e privatësisë

		Frekuenca	%
Të Vlefshme	Aspak	96	7.2
	Pak	118	8.8
	Disi	244	18.3
	Mjaftueshëm	366	27.4
	Shume	510	38.2
	Total	1334	100.0



Nga studimi i përgjigjeve të anketuarve për pyetjen se sa ndikon zhvillimi i teknologjisë së informacionit dhe komunikimit në fushën e privatësisë gjejmë se, për të anketuarit ky zhvillim ndikon disi, mjaftueshëm dhe shumë në fushën e privatësisë në masën 18.3%, 27.4% dhe 38.2%.

Nga analiza e gjetjeve të mësipërme mund të arrijmë në përfundimin se për 83.9% të të anektuarve zhvillimi i teknologjisë së informacionit dhe komunikimit ndikon disi, mjaftueshëm dhe shumë në fushën e privatësisë.

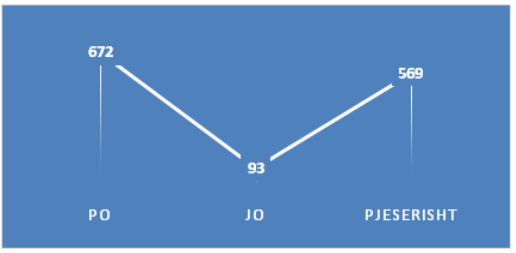
[9] https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf. faqe 3. Shfletuar me 28.10.2018.

[10] Strategjia Shtetërore për Sigurinë Kibernetike dhe Plani i Veprimit 2016 – 2019. Republika e Kosovës, Qeveria e Kosovës, Ministria e Punëve të Brendshme. Dhjetor 2015. Faqe 7.

- Përgjigjet e të anketuarve për pyetjen nëse e cenon zhvillimi i teknologjisë së informacionit dhe komunikimit privatësinë, në paraqitje tabelore dhe grafike janë si më poshtë:

A e cenon privatësinë zhvillimi i teknologjisë së informacionit & komunikimit

		Frekuenca	%
Të Vlefshme	PO	672	50.4
	JO	93	7.0
	PJESERISHT	569	42.7
	Total	1334	100.0



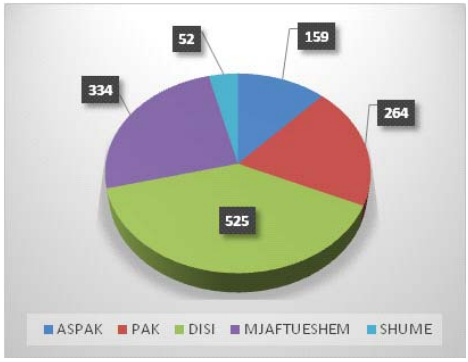
Nga studimi i përgjigjeve të anketuarve për pyetjen se nëse e cenon zhvillimi i teknologjisë së informacionit dhe komunikimit privatësinë gjejmë se, 50.4% e tyre mendojnë se zhvillimi i teknologjisë së informacionit dhe komunikimit cenon privatësinë; 42.7 % e cenon "pjesërisht" dhe vetëm 7% mendojnë se ky zhvillim teknologjik nuk e cenon privatësinë.

Nga analiza e gjetjeve të mësipërme mund të arrijmë në përfundimin se, për 93 % të të anketuarve zhvillimi i teknologjisë së informacionit dhe komunikimit cenon privatësinë qoftë dhe pjesërisht, shifër kjo shumë e lartë.

- Përgjigjet e të anketuarve për pyetjen se sa të sigurt e konsiderojnë komunikimin nëpërmjet teknologjisë së sotme të informacioni dhe komunikimit në paraqitje tabelore dhe grafike është si më poshtë:

Sa të sigurt e konsideroni komunikimin nëpërmjet teknologjisë së sotme të informacionit dhe komunikimit?

		Frekuenca	%
Të Vlefshme	ASPAK	159	11.9
	PAK	264	19.8
	DISI	525	39.4
	MJAFTUESHEM	334	25.0
	SHUME	52	3.9
	Total	1334	100.0



Nga studimi i përgjigjeve të anketuarve për pyetjen se sa të sigurt e konsiderojnë komunikimin nëpërmjet teknologjisë së sotme të informacioni dhe komunikimit gjejmë se 11.9% e të anketuarve nuk ndjehen "aspak" të sigurt në komunikimin nëpërmjet teknologjisë së sotme të informacioni dhe komunikimit. Ndërkohë që 19.8% ndjehen "pak", 39.4% ndjehen "disi", 25% ndjehen mjaftueshëm dhe vetëm 3.9% ndjehen "shumë" të sigurt në komunikimet nëpërmjet kësaj teknologjie.

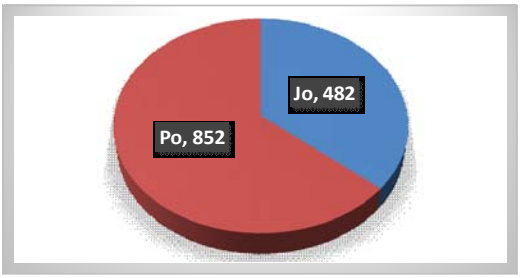
Në përfundim të analizës së të dhënave statistikore (tabelore dhe grafike) të kësaj pjese të përgjigjeve të të anketuarve mund të arrijmë në përfundimin se, shumica e të anketuarve mendojnë se zhvillimi i teknologjisë së sotme të informacionit dhe komunikimit luan rol të rëndësishëm në të gjithë aspektet e jetës duke përfshirë biznesin, komunikimin dhe edukimin, aksesin në informacion e shërbime publike dhe në fushën e privatësisë. Për shumicën e të anketuarve ky zhvillim teknologjik, cenon privatësinë. Për 31.7% të tyre ky komunikim nuk është aspak i sigurt ose është pak i sigurt.

Format kryesore nga të cilat të anketuarit e ndjejnë veten më të kërcënuar janë si më poshtë:

- Nga sulmet me viruse e ndjejnë veten të cenuar 63.9% e të anketuarve.

A e keni ndjerë veten të cenuar nga sulmi me viruse

		Frekuenca	%
Të Vlefshme	Jo	482	36.1
	Po	852	63.9
	Total	1334	100.0



A e keni ndjerë veten të cenuar nga mashtrime kompjuterike (*online*)

		Frekuenca	Përqindja
Të Vlefshme	Jo	1129	84.6
	Po	205	15.4
	Total	1334	100.0

– Nga mashtrimi kompjuterik e ndjejnë veten të cenuar 15.4% e të anketuarve

A keni ndjerë veten të cenuar nga hyrja e pa autorizuar kompjuterike

		Frekuenca	Përqindja
Të Vlefshme	Jo	1149	86.1
	Po	185	13.9
	Total	1334	100.0

– Nga hyrja e paautorizuar në kompjuter e ndjejnë veten të cenuar 13.9% e të anketuarve

A keni ndjerë veten të cenuar nga ndërhyrja në të dhënat kompjuterike

		Frekuenca	Përqindja
Të Vlefshme	Jo	1178	88.3
	Po	156	11.7
	Total	1334	100.0

– Nga ndërhyrja në të dhënat kompjuterike e ndjejnë veten të cenuar 11.7% e të anketuarve.

A keni ndjerë veten të cenuar nga përgjim të paligjshëm

		Frekuenca	Përqindja
Të Vlefshme	Jo	1153	86.4
	Po	181	13.6
	Total	1334	100.0

– Nga përgjimet e paligjshme e ndjejnë veten të cenuar 11.7% e të anketuarve

A keni ndjerë veten të cenuar nga vjedhja e identitetit

		Frekuenca	Përqindja
Të Vlefshme	Jo	1123	84.2
	Po	211	15.8
	Total	1334	100.0

– Nga vjedhja e identitetit e ndjejnë veten të cenuar 15.8% e të anketuarve.

A keni ndjerë veten të cenuar nga shkelje e të drejtës së autorit dhe pronësisë industriale			
		Frekuenca	Përqindja
Të Vlefshme	Jo	1222	91.6
	Po	112	8.4
	Total	1334	100.0

– Nga shkelje e te drejtës së autorit dhe pronësisë industriale e ndjejnë veten të cenuar 8.4% e të anketuarve.

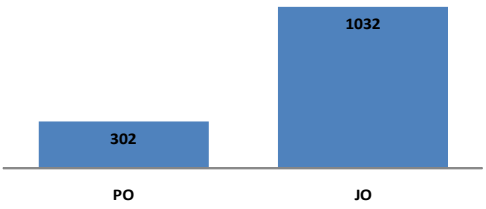
A keni ndjerë veten të cenuar nga forma të tjera të ndërhyrjes kompjuterike			
		Frekuenca	Përqindja
Të Vlefshme	Jo	998	74.8
	Po	336	25.2
	Total	1334	100.0

– Nga forma të tjera, të pa listuara më lart, e ndjejnë veten të cenuar 25.2% e të anketuarve.

Nga analiza e gjetjeve të mësipërme mund të arrijmë në përfundimin se të anketuarit e ndjejnë vetëm më shumë të kërcënuar nga sulmet me viruse, vjedhjet e identitetit dhe mashtrimet kompjuterike.

- Përgjigjet e të anketuarve lidhur me pyetjen nëse kanë përjetuar ndonjëherë pasoja të krimeve kibernetike, në paraqitje tabelore dhe grafike është si më poshtë:

A keni përjetuar ndonjëherë pasoja të krimeve kibernetike?			
		Frekuenca	%
Të Vlefshme	PO	302	22.6
	JO	1032	77.4
	Total	1334	100.0



Nga analiza e përgjigjeve të mësipërme gjejmë se 22.6% e të anketuarve kanë përjetuar pasoja të krimeve kibernetike, shifër kjo relativisht e lartë.

4.2 Llojet e pasojave të krimeve kibernetike që kanë përjetuar të anketuarit

A keni përjetuar ndonjëherë pasoja financiare nga krimet kibernetike?			
		Frekuenca	Përqindja
Të Vlefshme	Jo	1270	95.2
	Po	64	4.8
	Total	1334	100.0

– Nga krimet kibernetike kanë përjetuar pasoja financiare 4.8% e të anketuarve.

A keni përjetuar ndonjëherë humbjene të dhënave kompjuterike si pasoja të krimeve kibernetike?			
		Frekuenca	Përqindja
Të Vlefshme	Jo	1019	76.4
	Po	315	23.6
	Total	1334	100.0

– Humbje të të dhënave kompjuterike si pasojë e krimeve kibernetike kanë përjetuar 23.6% e të anketuarve.

A keni përjetuar ndonjëherë vjedhje të identitetit *online* si pasoje e krimeve kibernetike			
		Frekuenca	Përqindja
Të Vlefshme	Jo	1094	82.0
	Po	240	18.0
	Total	1334	100.0

– Vjedhje të identitetit *online* kanë përjetuar 18% e të anketuarve.

A keni përjetuar ndonjëherë pasoja të tjera përveç sa me sipër nga krimet kibernetike?		Frekuenca	Përqindja
Të Vlefshme	Jo	535	40.1
	Po	799	59.9
	Total	1334	100.0

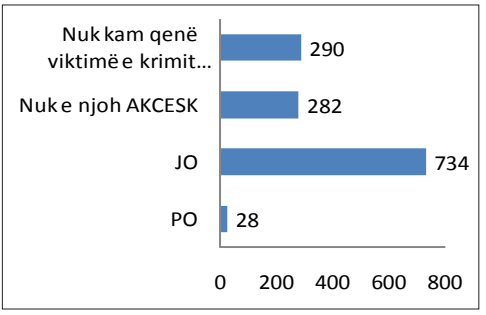
– Pasoja të tjera nga krimet kibernetike, përveç listimit të mësipërm, kanë përjetuar 59.9% e të anketuarve.

Nga analiza e gjetjeve të mësipërme mund të arrijmë në përfundimin se 22.6%e të anketuarve kanë qenë të paktën një herë viktimë e krimit kibernetik, ndërkohë që pasojat kanë qenë më shumë në formën e humbjes së të dhënave kompjuterike (23.6%), vjedhje të identitetit (18%) si dhe forma të tjera të pasojave (59.9%).

- Përgjigjet e të anketuarve lidhur me pyetjen nëse kanë raportuar apo kërkuar asistencë në Autoritetin Kombëtar për Sigurinë Kibernetike (AKCESK), në paraqitje tabelore dhe grafike janë si më poshtë:

A keni raportuar dhe kërkuar asistencë në Autoritetin Kombëtar për Sigurinë Kibernetike (AKCESK)?

A keni raportuar dhe kërkuar asistencë në Autoritetin Kombëtar për Sigurinë Kibernetike (AKCESK)?		Frekuenca	%
Të Vlefshme	PO	28	2.1
	JO	734	55.0
	NUK E NJOH AKCESK	282	21.1
	Nuk kam qenë viktimë e krimit kibernetik.	290	21.7
	Total	1334	100.0

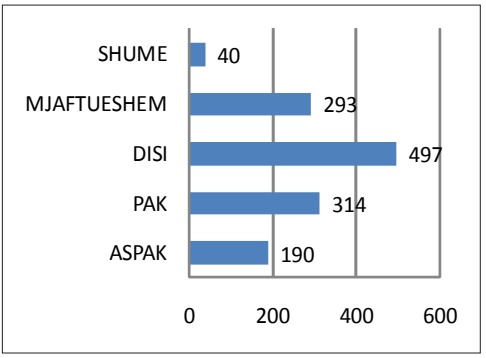


Nga analiza e gjetjeve të mësipërme të arrijmë në përfundimin se të anketuarit nuk kanë kërkuar asistencë pranë autoritetit kryesor kombëtar të sigurisë kibernetike në rastet e përjetimit të pasojave nga krimet kibernetike. Gjithashtu, konsiderohet jo i vogël edhe numri i të anketuarve që nuk e njohin fare atë institucion.

- Përgjigjet e të anketuarve për pyetjen se sa të sigurt ndjehen ata në aktivitetet specifike në hapësirën kibernetike, në paraqitje tabelore dhe grafike janë si më poshtë. Nga kjo paraqitje gjejmë se:

- Në aktivitetet *online* në rrjetet sociale, të anketuarit ndjehen "disi", "mjaftueshëm" dhe "shumë" të sigurt përkatësisht me 37.3%, 22% dhe 3%.

Sa të sigurt ndjeheni në aktivitetet *online* në rrjetet sociale?		Frekuenca	%
Të Vlefshme	ASPAK	190	14.2
	PAK	314	23.5
	DISI	497	37.3
	MJAFTUESHEM	293	22.0
	SHUME	40	3.0
	Total	1334	100.0

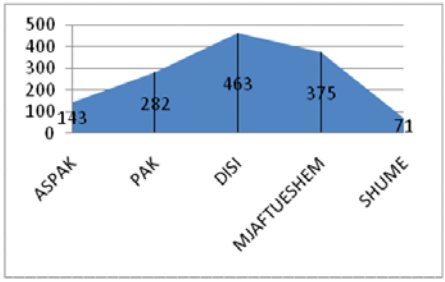


– Në postën elektronike, të anketuarit ndjehen "disi", "mjaftueshëm" dhe "shumë" të sigurt përkatësisht me 32.6%, 34.3% dhe 6.4%.

Sa të sigurt ndjeheni në aktivitetin tuaj me postën elektronike?			
		Frekuenca	Përqindja
Të Vlefshme	ASPAK	110	8.2
	PAK	245	18.4
	DISI	435	32.6
	MJAFTUESHEM	458	34.3
	SHUME	86	6.4
	Total	1334	100.0

- Në komunikimin *online* të anketuarit ndjehen "disi", "mjaftueshëm" dhe "shumë" të sigurt përkatësisht me 34.7%, 28.1% dhe 5.3%.

Sa të sigurt ndjeheni në komunikimin *online*?			
		Frekuenca	%
Të Vlefshme	ASPAK	143	10.7
	PAK	282	21.1
	DISI	463	34.7
	MJAFTUESHEM	375	28.1
	SHUME	71	5.3
	Total	1334	100.0

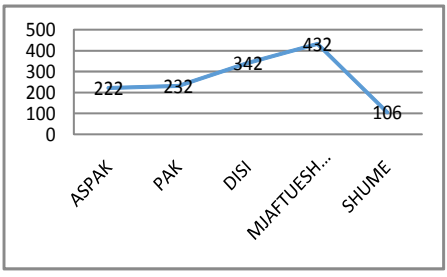


- Në blerjet *online* të anketuarit ndjehen "disi", "mjaftueshëm" dhe "shumë" të sigurt përkatësisht me 30%, 23.2% dhe 4.3%.

Sa të sigurt ndjeheni në blerjet *online*?			
		Frekuenca	%
Të Vlefshme	ASPAK	253	19.0
	PAK	314	23.5
	DISI	400	30.0
	MJAFTUESHEM	309	23.2
	SHUME	58	4.3
	Total	1334	100.0

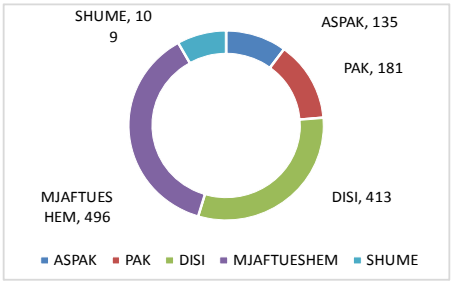
- Në veprimet bankare *online* të anketuarit ndjehen "disi", "mjaftueshëm" dhe "shumë" të sigurt përkatësisht me 25.6%, 32.4% dhe 7.9%.

Sa të sigurt ndjeheni në veprimet bankare onlinë			
		Frekuenca	%
Të Vlefshme	ASPAK	222	16.6
	PAK	232	17.4
	DISI	342	25.6
	MJAFTUESHEM	432	32.4
	SHUME	106	7.9
	Total	1334	100.0



- Gjatë punës në kompjuterin në zyrë të anketuarit ndjehen "disi", "mjaftueshëm" dhe "shumë" të sigurt përkatësisht me 31%, 37.2% dhe 8.2%.

Sa të sigurt ndjeheni gjatë punës në kompjuterin në zyrë?			
		Frekuenca	%
Të Vlefshme	ASPAK	135	10.1
	PAK	181	13.6
	DISI	413	31.0
	MJAFTUESHEM	496	37.2
	SHUME	109	8.2
	Total	1334	100.0



- Gjatë punës me kompjuterin në shtëpi të anketuarit ndjehen "disi", "mjaftueshëm" dhe "shumë" të sigurt përkatësisht me 32.5%, 38.1% dhe 8.2%.

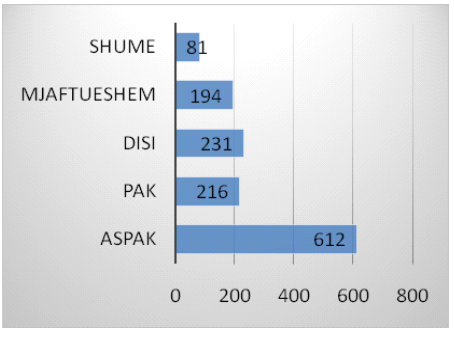
Sa të sigurt ndjeheni gjatë punës në kompjuterin në shtëpi			
		Frekuenca	Përqindja
Të Vlefshme	ASPAK	93	7.0
	PAK	189	14.2
	DISI	434	32.5
	MJAFTUESHEM	508	38.1
	SHUME	110	8.2
	Total	1334	100.0

- Në shkeljen e etikës në komunikim *online* të anketuarit ndjehen "disi", "mjaftueshëm" dhe "shumë" të sigurt përkatësisht 34.4%, 36.7% dhe 10%.

Sa të sigurt ndjeheni nga shkelja e etikës në komunikim *online* në hapësirën kibernetike?			
		Frekuenca	Përqindja
Të Vlefshme	ASPAK	73	5.5
	PAK	178	13.3
	DISI	459	34.4
	MJAFTUESHEM	490	36.7
	SHUME	134	10.0
	Total	1334	100.0

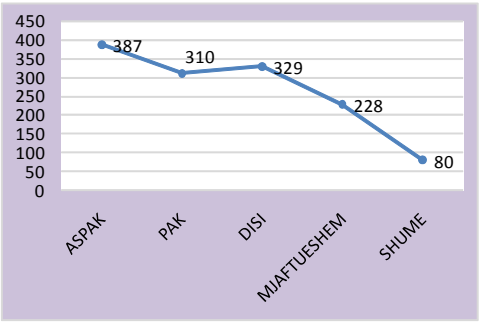
- Gjatë ndarjes së *password*-it (fjalëkalimit) me të tjerët të anketuarit ndjehen "disi", "mjaftueshëm" dhe "shumë" të sigurt përkatësisht me 17.3%; 14.5% dhe 6.1%.

Sa të sigurt ndjeheni gjatë ndarjes së *password*-it (fjalëkalimit) me të tjerët			
		Frekuenca	%
Të Vlefshme	ASPAK	612	45.9
	PAK	216	16.2
	DISI	231	17.3
	MJAFTUESHEM	194	14.5
	SHUME	81	6.1
	Total	1334	100.0



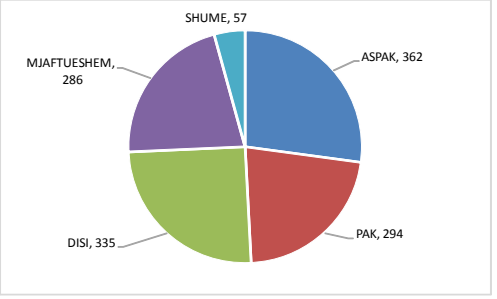
- Në përdorimin vetëm të një *password*-i në të gjitha shërbimet *online* të anketuarit ndjehen "disi", "mjaftueshëm" dhe "shumë" të sigurt përkatësisht me 24.7%,17.1% dhe 6%.

Sa të sigurt ndjeheni në përdorimin e vetëm të një *password*-i në të gjitha shërbimet *online*.			
		Frekuenca	%
Të Vlefshme	ASPAK	387	29.0
	PAK	310	23.2
	DISI	329	24.7
	MJAFTUESHEM	228	17.1
	SHUME	80	6.0
	Total	1334	100.0



- Në përdorimin e kartave të kreditit *online* të anketuarit ndjehen "disi", "mjaftueshëm" dhe "shumë" të sigurt përkatësisht me 25.1%,21.4% dhe 4.3%.

Sa të sigurt ndjeheni në secilin prej aktiviteteve dhe veprimeve të mëposhtme në hapësirën kibernetike? *Përdorimi i kartave të kreditit online*			
		Frekuenca	%
Të Vlefshme	ASPAK	362	27.1
	PAK	294	22.0
	DISI	335	25.1
	MJAFTUESHEM	286	21.4
	SHUME	57	4.3
	Total	1334	100.0



- Në përdorimin e shërbimeve publike online të anketuarit ndjehen "disi", "mjaftueshëm" dhe "shumë" të sigurt përkatësisht me 34.2%, 26.9% dhe 4.5%

Sa të sigurt ndjeheni në përdorimin e shërbimeve publike online			
		Frekuenca	Përqindja
Të Vlefshme	ASPAK	176	13.2
	PAK	283	21.2
	DISI	456	34.2
	MJAFTUESHEM	359	26.9
	SHUME	60	4.5
	Total	1334	100.0

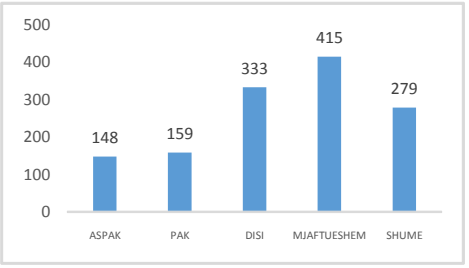
Nga analiza e gjetjeve të përgjigjeve të anketuarve për pyetjen se sa të sigurt ndjehen ata në aktivitetet e tyre specifike në hapësirën kibernetike mund të arrijmë në përfundimin se të anketuarit nuk ndjehen të sigurt në aktivitetet e tyre në hapësirën kibernetike në masën nga 18.8% deri në 62.1%.

Konkretisht ndjehen në masën 37.7% "aspak" dhe "pak" të sigurt në aktivitetet *online* në rrjetet sociale; 26.6% në postën elektronike; 31.8% në komunikimin *online*; 42.5% në blerjet *online*; 34% në veprimet bankare; 23.7% gjatë punës me kompjuter

në zyrë; 21.2% gjatë punës me kompjuterin në shtëpi; 18.8% në shkeljen e etikës në komunikim *online*; 62.1% gjatë ndarjes së *password*-it (fjalëkalimit) me të tjerët; 52.2% në përdorimi vetëm të një *password*-i në të gjitha shërbimet *online*; 47.1% në përdorimin e kartave të kreditit *online* dhe 34.4% në përdorimin e shërbimeve publike *online*.

- Përgjigjet e të anketuarve për pyetjen se a ndjeni përgjegjësi për sigurinë kibernetike në vendin e tuaj të punës, në paraqitje tabelore dhe grafike janë si më poshtë:

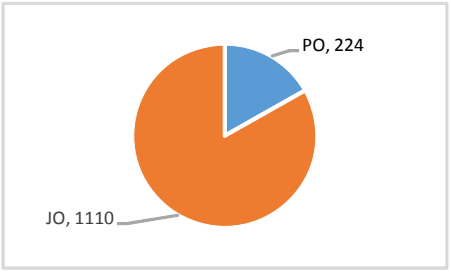
A ndjeni përgjegjësi për sigurinë kibernetike në vendin tuaj të punës?			
		Frekuenca	%
Të Vlefshme	ASPAK	148	11.1
	PAK	159	11.9
	DISI	333	25.0
	MJAFTUESHEM	415	31.1
	SHUME	279	20.9
	Total	1334	100.0



Nga analiza e gjetjeve të mësipërme mund të arrijmë në përfundimin se të anketuarit që nuk ndjejnë "aspak" përgjegjësi apo që ndjejnë "pak" dhe "disi" përgjegjësi për sigurinë kibernetike në vendin e tyre të punës përbëjnë 47 % të numrit total të intervistuarve shifër kjo mjaft e lartë. Kjo na obligon për rritjen e përgjegjshmërisë për sigurinë kibernetike të punonjësve në qendrën e tyre të punës.

- Përgjigjet e të anketuarve për pyetjen nëse janë trajnuar për sigurinë kibernetike në vendin e tuaj të punës, në paraqitje tabelore dhe grafike janë si më poshtë.

A jeni i trajnuar për sigurinë kibernetike në vendin tuaj të punës?			
		Frekuenca	%
Të Vlefshme	PO	224	16.8
	JO	1110	83.2
	Total	1334	100.0



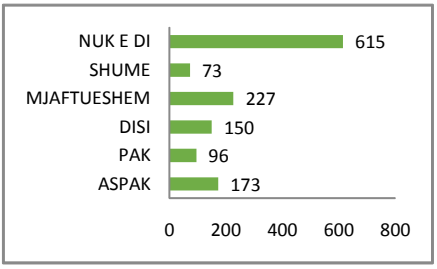
Nga këto të dhëna rezulton se 83% e të anketuarve përgjigjen se nuk janë trajnuar për sigurinë kibernetike në vendin e tyre të punës.

Ky tregues, relativisht i lartë tregon se vetë organizatat punuese nuk e vlerësojnë sigurinë kibernetike. Duke marrë parasysh se shumica e të anketuarve i përkasin sektorit publik arrijmë në përfundime, për mangësi në angazhimin e strukturave shtetërore për trajnimin e punonjësve të tyre për sigurinë kibernetike në vendin e punës. Kjo shpjegon dhe përgjigjen e të anketuarve në pyetjen e mësipërme ku 47% e të anketuarve nuk ndjejnë "aspak" përgjegjësi apo që ndjejnë "pak" dhe "disi" përgjegjësi për sigurinë kibernetike në vendin e tyre të punës.

- Gjetjet lidhur me përgjigjet e të anketuarve për pyetjen se "Nëse jeni trajnuar për sigurinë kibernetike, sa e ndjeni veten më të sigurt pas trajnimit", në paraqitje

tabelore e grafike janë si më poshtë:

Nëse po, sa e ndjeni veten më të sigurt pas trajnimit?			
		Frekuenca	%
Të Vlefshme	ASPAK	173	13.0
	PAK	96	7.2
	DISI	150	11.2
	MJAFTUESHEM	227	17.0
	SHUME	73	5.5
	NUK E DI	615	46.1
	Total	1334	100.0

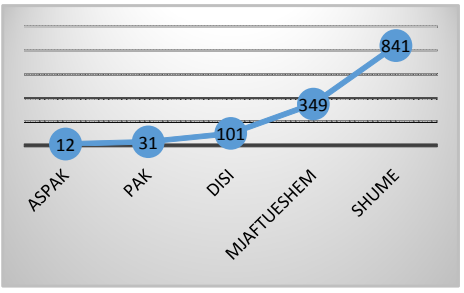


Nga analizat e gjetjeve të mësipërme statistikore mund të arrijmë në përfundimin se vetëm 22.5% e të anketuarve që janë trajnuar, kanë përfituar nga ky trajnim për sigurinë kibernetike dhe e ndjejnë veten (mjaftueshëm dhe shumë) të sigurt pas trajnimit, ndërkohë që 46.1% nuk e dinë nëse kanë përfituar apo jo. Këto të dhëna tregojnë se, edhe kur janë bërë trajnime në vendin e punës, lidhur me sigurinë kibernetike, ato nuk kanë qenë të frytshme.

- Gjetjet lidhur me përgjigjet e të anketuarve për fushat ku duhet investuar më shumë për të përmirësuar sigurinë kibernetike, në paraqitje tabelore dhe grafike janë si më poshtë, në vijim.

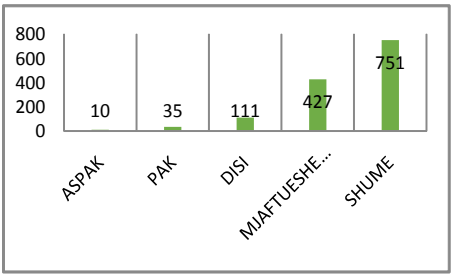
- Për edukimin që në shkollë për parandalimin e krimit në internet, si fushë ku duhet investuar për të përmirësuar sigurinë kibernetike, të anketuarit shprehen "mjaftueshëm" dhe "shumë"përkatësisht në masën 26.2% dhe 63%.

Sipas jush, për të përmirësuar sigurinë kibernetike, sa duhet investuar në edukimin që në shkollë për parandalimin e krimit në internet.			
		Frekuenca	%
Të Vlefshme	ASPAK	12	0.9
	PAK	31	2.3
	DISI	101	7.6
	MJAFTUESHEM	349	26.2
	SHUME	841	63.0
	Total	1334	100.0



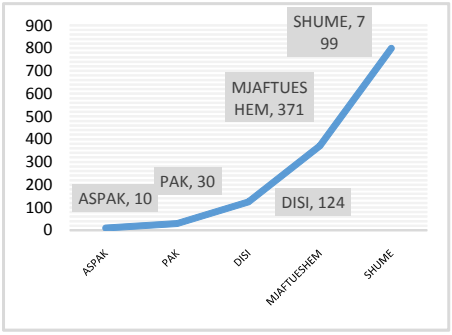
- Për investimin në menaxhimin e sigurisë kibernetike për të përmirësuar sigurinë kibernetike, të anketuarit shprehen "mjaftueshëm" dhe "shumë"përkatësisht në masën 32% dhe 56.3%.

Sipas jush, për të përmirësuar sigurinë kibernetike, sa duhet investuar në menaxhimin e sigurisë kibernetike.			
		Frekuenca	%
Të Vlefshme	ASPAK	10	0.7
	PAK	35	2.6
	DISI	111	8.3
	MJAFTUESHEM	427	32.0
	SHUME	751	56.3
	Total	1334	100.0



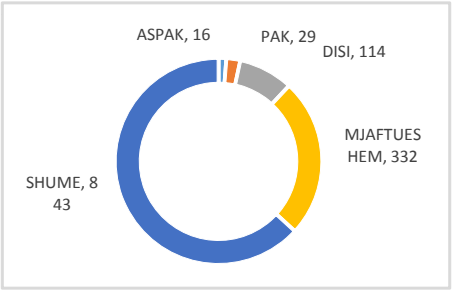
- Për investimin në rritjen e ndërgjegjësimit të publikut të gjerë, për të përmirësuar sigurinë kibernetike, të anketuarit shprehen "mjaftueshëm" dhe "shumë"përkatësisht në masën 27.8% dhe 59.9%.

Sipas jush, për të përmirësuar sigurinë kibernetike, sa duhet investuar në rritjen e ndërgjegjësimit të publikut të gjerë.			
		Frekuenca	%
Të Vlefshme	ASPAK	10	0.7
	PAK	30	2.2
	DISI	124	9.3
	MJAFTUES HEM	371	27.8
	SHUME	799	59.9
	Total	1334	100.0



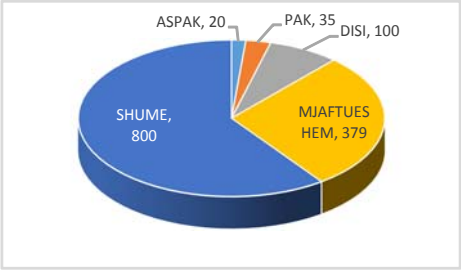
- Për investimin në ligjet dhe politikat mbi krimin kibernetik si fushë për të përmirësuar sigurinë kibernetike, të anketuarit shprehen "mjaftueshëm" dhe "shumë"përkatësisht në masën 24.9% dhe 63.2%.

Sipas jush, për të përmirësuar sigurinë kibernetike, sa duhet investuar në ligjet dhe politikat mbi krimin kibernetik.			
		Frekuenca	%
Të Vlefshme	ASPAK	16	1.2
	PAK	29	2.2
	DISI	114	8.5
	MJAFTUES HEM	332	24.9
	SHUME	843	63.2
	Total	1334	100.0



- Për investimin në rreziqet dhe efektet e krimit kibernetik si fushë për të përmirësuar sigurinë kibernetike, të anketuarit shprehen "mjaftueshëm" dhe "shumë"përkatësisht në masën 28.4% dhe 60%.

Sipas jush, për të përmirësuar sigurinë kibernetike, sa duhet investuar në rreziqet dhe efektet e krimit kibernetik.			
		Frekuenca	%
Të Vlefshme	ASPAK	20	1.5
	PAK	35	2.6
	DISI	100	7.5
	MJAFTUES HEM	379	28.4
	SHUME	800	60.0
	Total	1334	100.0

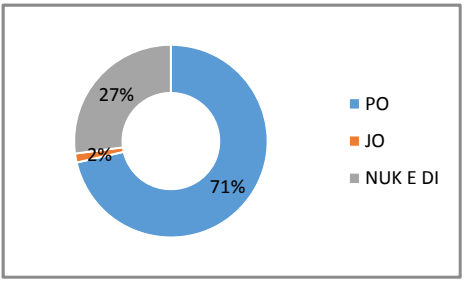


Nga analiza e gjetjeve të mësipërme, mund të arrijmë në përfundimin se të anketuarit besojnë mjaftueshëm dhe shumë, në masën 87 deri 89% se fushat ku duhet investuar për të përmirësuar sigurinë kibernetike janë edukimin që në shkollë për parandalimin e krimit në internet; në menaxhimin e sigurisë kibernetike; në rritjen e ndërgjegjësimit të

publikut të gjerë; në ligjet dhe politikat mbi krimin kibernetik dhe në rreziqet dhe efektet e krimit kibernetik.

- Gjetjet për përgjigjen të anketuarve për pyetjen se nëse do të hasnit një rast të krimit kibernetik, a do ta raportonit, në paraqitje tabelore dhe grafike janë si më poshtë:

Nëse do të hasnit një rast të krimit kibernetik, a do ta raportonit?			
		Frekuenca	%
Të Vlefshme	PO	953	71.4
	JO	20	1.5
	NUK E DI	361	27.1
	Total	1334	100.0

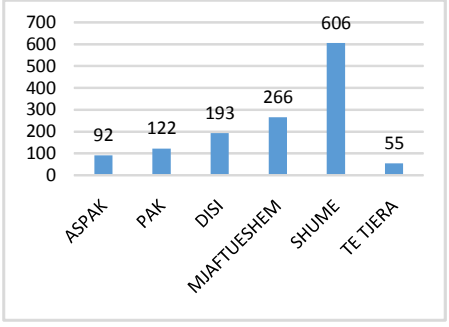


Nga analiza e gjetjeve të përgjigjeve të anketuarve për pyetjen se nëse do të hasnit një rast të krimit kibernetik, a do ta raportonit, mund të arrijmë në përfundimin se shumica e të anketuarve (71.4) do ta raportonin nëse do të hasnin një rast të krimit kibernetik, përkundrejt 1.5% që nuk do ta raportonin një rast të tillë. Ndërkohë, mund të konsiderohet përsëri e lartë (27.1) shifra e atyre që janë të pavendosur për ta raportuar një rast të tillë. Për këtë rekomandohet që të gjenden mënyrat për ndërgjegjësimin edhe të kësaj kategorie për të raportuar raste e hasura të krimit kibernetik.

- Gjetjet lidhur me përgjigjet e të anketuarve për pyetjen sa do ta raportonit një rast të krimit kibernetik në secilën nga agjencitë e mëposhtme në paraqitje tabelore dhe grafike janë si më poshtë:

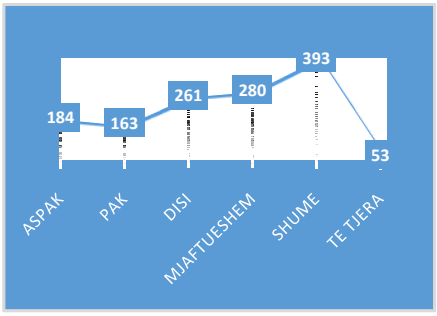
- Në Policinë e Shtetit të anketuarit do ta raportonin "disi", "mjaftueshëm" dhe "shumë " një rast të krimit kibernetik përkatësisht me 14.5%, 19.9% dhe 45.4%.

Sa do ta raportonit një rast të krimit kibernetik në Policinë e Shtetit			
		Frekuenca	%
Të Vlefshme	ASPAK	92	6.9
	PAK	122	9.1
	DISI	193	14.5
	MJAFTUESHEM	266	19.9
	SHUME	606	45.4
	TE TJERA	55	4.1
	Total	1334	100.0



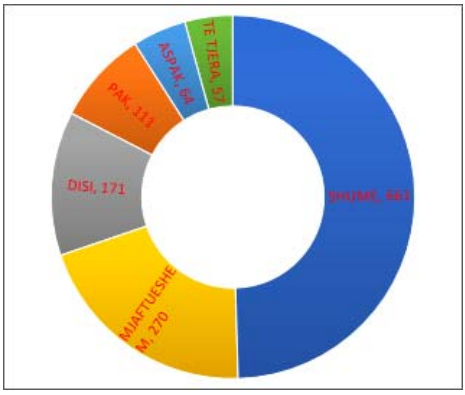
- Në Prokurori të anketuarit do ta raportonin “disi”, “mjaftueshëm” dhe “shumë” një rast të krimit kibernetik përkatësisht me 19.6%,21% dhe 29.5%.

Sa do ta raportonit një rast të krimit kibernetik në Prokurori			
		Frekuenca	%
Të Vlefshme	ASPAK	184	13.8
	PAK	163	12.2
	DISI	261	19.6
	MJAFTUESHEM	280	21.0
	SHUME	393	29.5
	TE TJERA	53	4.0
	Total	1334	100.0



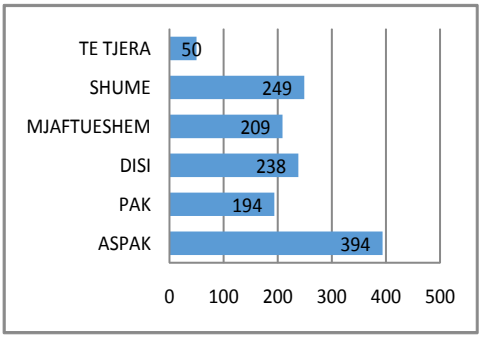
- Në *Autoritetin për Sigurinë Kibernetike* të anketuarit do ta raportonin “disi”, “mjaftueshëm” dhe “shumë “ një rast të krimit kibernetik përkatësisht me 12.8%, 20.2% dhe 49.6%.

Sa do ta raportonit një rast të krimit kibernetik në Autoritetin për Sigurinë Kibernetike			
		Frekuenca	%
Të Vlefshme	ASPAK	64	4.8
	PAK	111	8.3
	DISI	171	12.8
	MJAFTUESHEM	270	20.2
	SHUME	661	49.6
	TE TJERA	57	4.3
	Total	1334	100.0



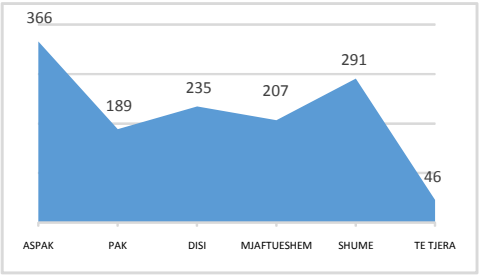
- Në SHISH të anketuarit do ta raportonin “disi”, “mjaftueshëm” dhe “shumë”një rast të krimit kibernetik përkatësisht me 17.8%, 15.7% dhe 18.7%.

Sa do ta raportonit një rast të krimit kibernetik në SHISH			
		Frekuenca	%
Të Vlefshme	ASPAK	394	29.5
	PAK	194	14.5
	DISI	238	17.8
	MJAFTUESHEM	209	15.7
	SHUME	249	18.7
	TE TJERA	50	3.7
	Total	1334	100.0



- Në institucionin e Avokatit të Popullit, të anketuarit do ta raportonin "disi", "mjaftueshëm" dhe "shumë" një rast të krimit kibernetik përkatësisht me 17.6%, 15.5% dhe 21.8%.

Sa do ta raportonit një rast të krimit kibernetik në Avokatin e Popullit			
		Frekuenca	%
Të Vlefshme	ASPAK	366	27.4
	PAK	189	14.2
	DISI	235	17.6
	MJAFTUESHEM	207	15.5
	SHUME	291	21.8
	TE TJERA	46	3.4
	Total	1334	100.0



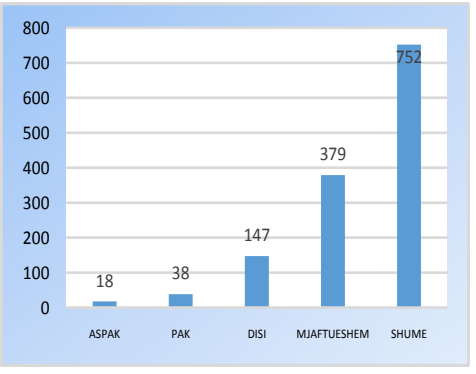
Nga gjetjet e mësipërme rezulton që nivelin më të lartë të besimit për të raportuar një rast të krimit kibernetik të anketuarit e kanë tek Policia e Shtetit me 79.8%(14.5%(disi) + 19.9%(mjaftueshëm) + 45.4% (shumë)); Autoriteti Për Sigurinë Kibernetike me 82.6% (12.8%+20.2%+49.6%) dhe, më pas renditen, Prokuroria me 70.1%; Avokati i Popullit me 54.9% dhe SHISH me 52.2%.

Vlen të theksohet se ka rritje të besimit tek Autoritetit Për Sigurinë Kibernetike pas marrjes së informacionit të duhur gjatë procesit të anketimit. Kjo pasi në fillim të pyetësorit pyetjes nëse kanë raportuar apo kërkuar asistencë në Autoritetin Kombëtar për Sigurinë Kibernetike (AKCESK) i janë përgjigjur pozitivisht vetëm 2.1%, ndërkohë që 55% nuk kanë raportuar e kërkuar asistencë, 21.1% nuk e njohin fare atë institucion.

- Gjetjet lidhur me përgjigjet e të anketuarve për pyetjen lidhur me alternativat që ata i vlerësojnë si hapa të domosdoshëm për të parandaluar rritjen e rasteve të krimit kibernetik (pra, në rritjen e sigurisë kibernetike) në paraqitje tabelore dhe grafike janë si më poshtë, në vijim.

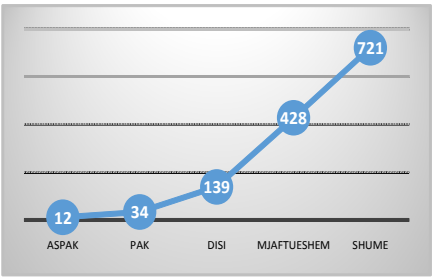
- Trajnimi i duhur i oficerëve të zbatimit të ligjit vlerësohet disi, mjaftueshëm dhe shumë si hap i domosdoshëm për të parandaluar rritjen e rasteve të krimit kibernetik përkatësisht në masën 11%,28.4% dhe 56.4%.

Sa e vlerësoni ofrimin e trajnimit të duhur të oficerëve të zbatimit të ligjit që punojnë në fushën e krimit kibernetik si hap i domosdoshme për të parandaluar rritjen e rasteve të krimit kibernetik?			
		Frekuenca	%
Të Vlefshme	ASPAK	18	1.3
	PAK	38	2.8
	DISI	147	11.0
	MJAFTUESHEM	379	28.4
	SHUME	752	56.4
	Total	1334	100.0



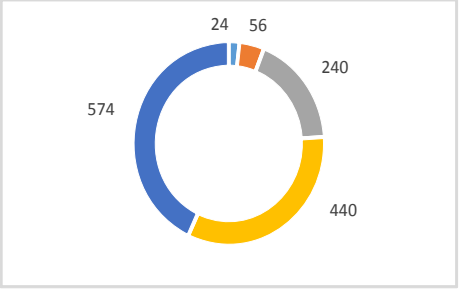
- Rritja e ndërgjegjësimit të publikut të gjerë vlerësohet disi, mjaftueshëm dhe shumë, si hap i domosdoshëm për të parandaluar rritjen e rasteve të krimit kibernetik përkatësisht në masën 10.4%, 42% dhe 54%.

Sa i vlerësoni alternativën e rritjes së ndërgjegjësimit të publikut të gjerë si hap i domosdoshëm për të parandaluar rritjen e rasteve të krimit kibernetik?			
		Frekuenca	%
Të Vlefshme	ASPAK	12	.9
	PAK	34	2.5
	DISI	139	10.4
	MJAFTUESHEM	428	32.1
	SHUME	721	54.0
	Total	1334	100.0



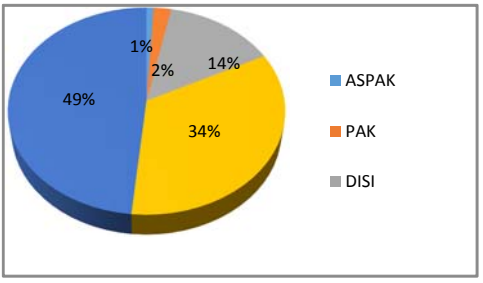
- Shtimi i numrit të oficerëve të zbatimit të ligjit vlerësohet disi, mjaftueshëm dhe shumë, si hap i domosdoshëm për të parandaluar rritjen e rasteve të krimit kibernetik përkatësisht në masën 18%, 33% dhe 43%.

Sa e vlerësoni alternativën e shtimit të numrit të oficerëve të zbatimit të ligjit si hap i domosdoshëm për të parandaluar rritjen e rasteve të krimit kibernetik?			
		Frekuenca	%
Të Vlefshme	ASPAK	24	1.8
	PAK	56	4.2
	DISI	240	18.0
	MJAFTUESHEM	440	33.0
	SHUME	574	43.0
	Total	1334	100.0



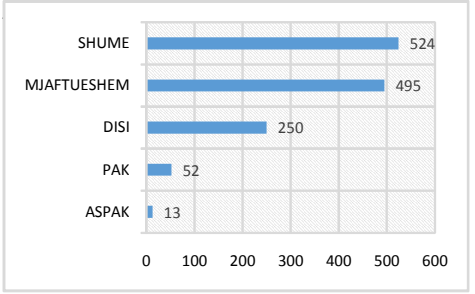
- Ndryshimet e duhura ligjore vlerësohet disi, mjaftueshëm dhe shumë, si hap i domosdoshëm për të parandaluar rritjen e rasteve të krimit kibernetik përkatësisht në masën 14%, 34.1% dhe 48.4%.

Sa e vlerësoni alternativën e ndryshimeve të duhura ligjore si hap i domosdoshëm për të parandaluar rritjen e rasteve të krimit kibernetik?			
		Frekuenca	%
Të Vlefshme	ASPAK	12	.9
	PAK	30	2.2
	DISI	191	14.3
	MJAFTUESHEM	455	34.1
	SHUME	646	48.4
	Total	1334	100.0



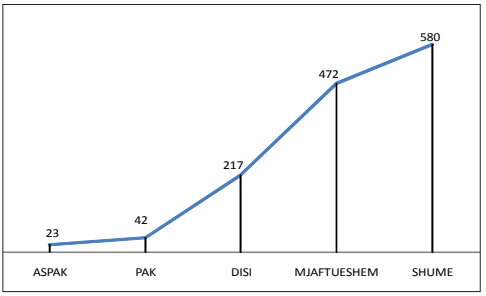
- Ndryshimet e duhura strukturore vlerësohet disi, mjaftueshëm dhe shumë, si hap i domosdoshëm për të parandaluar rritjen e rasteve të krimit kibernetik përkatësisht në masën 18.7%, 37.1% dhe 39.3%.

Sa e vlerësoni alternativën e ndryshimeve të duhura strukturore si hap i domosdoshëm për të parandaluar rritjen e rasteve të krimit kibernetik?			
		Frekuenca	%
Të Vlefshme	ASPAK	13	1.0
	PAK	52	3.9
	DISI	250	18.7
	MJAFTUESHEM	495	37.1
	SHUME	524	39.3
	Total	1334	100.0



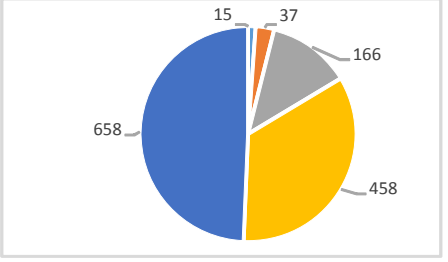
- Bashkëpunimi publik-privat në fushën e luftës kundër krimit kibernetik vlerësohet disi, mjaftueshëm dhe shumë, si hap i domosdoshëm për të parandaluar rritjen e rasteve të krimit kibernetik përkatësisht në masën 16.3%, 35.4% dhe 43.5%.

Sa e vlerësoni alternativën e rritjes së bashkëpunimit publik-privat në këtë fushë si hap të domosdoshëm për të parandaluar rritjen e rasteve të krimit kibernetik?			
		Frekuenca	%
Të Vlefshme	ASPAK	23	1.7
	PAK	42	3.1
	DISI	217	16.3
	MJAFTUESHEM	472	35.4
	SHUME	580	43.5
	Total	1334	100.0



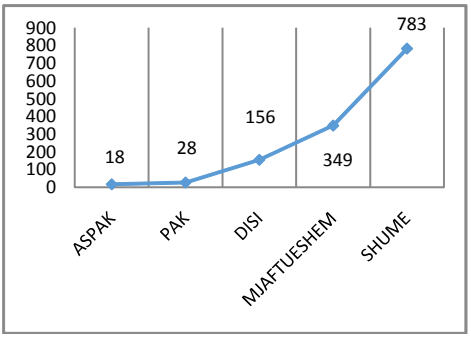
- Përfshirjes së njohurive mbi veprat penale kompjuterike në programet shkollore vlerësohet disi, mjaftueshëm dhe shumë, si hap i domosdoshëm për të parandaluar rritjen e rasteve të krimit kibernetik përkatësisht në masën 12.4%, 34.3% dhe 49.3%.

Sa e vlerësoni alternativën e përfshirjes së njohurive mbi veprat penale kompjuterike në programet shkollore si hap i domosdoshëm për të parandaluar rritjen e rasteve të krimit kibernetik?			
		Frekuenca	%
Të Vlefshme	ASPAK	15	1.1
	PAK	37	2.8
	DISI	166	12.4
	MJAFTUESHEM	458	34.3
	SHUME	658	49.3
	Total	1334	100.0



- Ashpërsimi i dënimeve ndaj autorëve te veprave penale kompjuterike vlerësohet disi, mjaftueshëm dhe shumë, si hap i domosdoshëm për të parandaluar rritjen e rasteve të krimit kibernetik përkatësisht në masën 11.7%, 26.2% dhe 58.7%.

Sa e vlerësoni alternativën e ashpërsimit të dënimeve ndaj autorëve te veprave penale kompjuterike si hap i domosdoshme për të parandaluar rritjen e rasteve të krimit kibernetik?			
		Frekuenca	%
Të Vlefshme	ASPAK	18	1.3
	PAK	28	2.1
	DISI	156	11.7
	MJAFTUESHEM	349	26.2
	SHUME	783	58.7
	Total	1334	100.0



Nga analiza e gjetjeve të mësipërme mund të arrijmë në përfundimin se, të anketuarit i vlerësojnë si hapa të domosdoshëm për të parandaluar rritjen e rasteve të krimeve kibernetike alternativat e mësipërme në masën mbi 94% dhe konkretisht ofrimin e trajnimit të duhur të oficerëve të zbatimit të ligjit që punojnë në fushën e krimit në masën 96.6% (11% (disi) + 28.4% (mjaftueshëm) + 56.4% (shumë); rritjen e ndërgjegjësimit të publikut të gjerë në masën 96.5%; shtimin e numrit të oficerëve të zbatimit të ligjit që punojnë në fushën e krimit kibernetik në masën 94%; ndryshimet e duhura ligjore në masën 96.8%; ndryshimet e duhura strukturore ne masën 95.1%; rritjen e bashkëpunimit publik-privat në këtë fushë në masën 95.%; përfshirjen e njohurive mbi veprat penale kompjuterike në programet shkollore në masën 96% dhe ashpërsimin e dënimeve ndaj autorëve të këtyre veprave penale në masën 96.6%. Nga alternativat e cituara më sipër rritjen e ndërgjegjësimit të publikut të gjerë në masën 96.5%.

5. Përfundimet dhe rekomandimet kryesore

Në përfundim të këtij punimi, është e rëndësishme të theksohet se zhvillimi i teknologjisë së sotme të informacionit dhe komunikimit, po luan një luan rol gjithnjë e më të rëndësishëm në të gjithë aspektet e jetës, por tendenca për të orientuar zhvillimin ekonomik drejt teknologjive të avancuara, rrit në mënyrë të pakthyeshme varësinë nga teknologjia, e cila, tashmë, në terrenin e fituar, kërkon një qasje bashkëpunuese për të arritur shmangien e përdorimit të teknologjisë, në kundërshtim me qëllimin kryesor. Punimi evidenton qartë pasigurinë e qytetarëve për veprimet në hapësirën kibernetike, referuar kjo rrezikut që është prezent nga veprimet e jashtëligjshme që synojnë individin, biznesin, industrinë dhe institucionet publike.

Ndërkohë niveli i vlerësimit të riskut nga individi, shoqëria dhe institucionet nuk është në shkallën me të cilin zhvillohet teknologjia dhe qasja e individit/shoqërisë ndaj saj. Kjo vjen edhe si pasojë e mungesës së duhur të informacionit, sensibilizimit, ndërgjegjësimit dhe trajnimeve në këtë fushë. Për këtë, rekomandohet që fushatat sensibilizuese dhe trajnimet për kërcënimin dhe sigurinë kibernetike duhet të jenë periodike, intensive si edhe të përgatitura për të qenë të asimilueshme nga audienca të ndryshme dhe nëpër mjete te ndryshme të komunikimit, nisur kjo nga shkalla e përdorimit të teknologjisë nga këto kategori.

Më poshtë paraqiten përfundimet dhe rekomandimet kryesore nga ky punim.

- Në anketim kanë marrë pjesë nga të gjithë grupmoshat të cilave iu është adresuar

pyetësori. Grupmosha 27-45 vjeç dhe 46-60 vjeç kanë qenë më të përfaqësuara në këtë anketim dhe kanë pasur më shumë interes për fushën e krimeve dhe sigurisë kibernetike. Kështu, 97.7% e kampioneve ka një nivel të lartë arsimor (*bachelor*, master dhe doktoraturë).

- Të anketuarit femra kanë qenë më të interesuara dhe më të ndjeshme për tematikën e anketimit, me një përgjegjshmëri më të madhe sociale se meshkujt si dhe më të sakta në plotësimin e pyetësorit nga fillimi në fund.

- Kampioni ka një përfaqësim e larmi profesionale ku numrin më të madh e përbëjnë arsimtarët (70.8%) dhe punonjësit e policisë (10%) ndërsa më pak nga bota e biznesit dhe punëtorët. Arsimtarët, si profesion, në raport me gjyqtarët, prokurorët dhe punonjësit e policisë, tregojnë një nivel përgjegjësie më të madhe sociale, duke u angazhuar në anketime në probleme kaq të rëndësishme për shoqërinë shqiptare, siç është krimi kompjuterik dhe siguria kibernetike.

- Shumica e të anketuarve mendojnë se zhvillimi i teknologjisë së sotme të informacionit dhe komunikimit luan rol të rëndësishëm në të gjithë aspektet e jetës duke përfshirë biznesin, komunikimin dhe edukimin, aksesin në informacion e shërbime publike dhe në fushën e privatësisë. Për shumicën e të anketuarve ky zhvillim teknologjik, cenon privatësinë ndërkohë që për një pjesë të konsiderueshme të anketuarve (31.7%) komunikimi nëpërmjet kësaj teknologjie nuk është aspak i sigurt ose është pak i sigurt.

- Sulmet me viruse, vjedhjet e identitetit dhe mashtrimet kompjuterike janë kërcënimet më të përhapura ndaj të anketuarve.

- Një numër i konsiderueshëm i të anketuarve (22.6%) kanë përjetuar pasoja të krimeve kibernetike më shumë në formën e humbjes së të dhënave kompjuterike (23.6%), vjedhje të identitetit (18%) si dhe forma të tjera të pasojave (59.9%).

- Të anketuarit nuk kanë kërkuar asistencë pranë autoritetit kryesor kombëtar të sigurisë kibernetike në rastet e përjetimit të pasojave nga krimet kibernetike. Gjithashtu, konsiderohet jo i vogël edhe numri i të anketuarve që nuk e njohin fare atë institucion.

- Të anketuarit nuk ndjehen të sigurt në aktivitetet e tyre të ndryshme në hapësirën kibernetike, në masën nga 21.2% deri në 47.1%.

- Ndarja e fjalëkalimit me të tjerët si dhe përdorimi i vetëm një fjalëkalimi në të gjitha shërbimet *online* vlerësohet nga të anketuarit si kërcënim për sigurinë e aktiviteteve të tyre në hapësirën kibernetike.

- Në një numër të konsiderueshëm (47%) të anketuarit nuk ndjejnë "aspak" përgjegjësi apo ndjejnë "pak" dhe "disi" përgjegjësi për sigurinë kibernetike në vendin e tyre të punës.

- 83% e të anketuarve nuk janë trajnuar për sigurinë kibernetike në vendin e tyre të punës dhe vetëm 22.5% e të anketuarve që janë trajnuar, kanë përfituar nga ky trajnim për sigurinë kibernetike. Ky tregues, relativisht i lartë tregon se vetë organizatat punuese nuk e vlerësojnë sigurinë kibernetike.

- Duke marrë parasysh se shumica e të anketuarve i përkasin sektorit publik, arrijmë në përfundime, për mangësi në angazhimin e strukturave shtetërore për trajnimin e punonjësve të tyre për sigurinë kibernetike në vendin e punës si dhe për cilësinë e këtyre trajnimeve. Për këtë rekomandohet fillimi i trajnimit të punonjësve për sigurinë kibernetike në vendin e tyre të punës.

- Sipas të anketuarve fushat ku duhet investuar për të përmirësuar sigurinë kibernetike janë edukimin që në shkollë për parandalimin e krimit në internet; në menaxhimin e sigurisë kibernetike; në rritjen e ndërgjegjësimit të publikut të gjerë; në ligjet dhe politikat

mbi krimin kibernetik dhe në rreziqet dhe efektet e krimit kibernetik.

- Shumica e të anketuarve (71.4) do ta raportonin nëse do të hasnin një rast të krimit kibernetik. Ndërkohë mund të konsiderohet përsëri e lartë (27.1) shifra e atyre që janë të pavendosur për ta raportuar një rast të tillë. Për këtë rekomandohet që të gjenden mënyrat për ndërgjegjësimin edhe të kësaj kategorie për të raportuar raste e hasura të krimit kibernetik.

- Të anketuarit do ta raportonin një rast të krimit kibernetik më shumë në Policinë e Shtetit me 79.8%(14.5%(disi) + 19.9%(mjaftueshëm) + 45.4% (shumë)); Autoriteti Për Sigurinë Kibernetike me 82.6% (12.8%+20.2%+49.6%) dhe më pas në Prokurori me 70.1%; Avokati i Popullit me 54.9% dhe SHISH me 52.2%.

- Vlen të theksohet se, pas marrjes së informacionit të duhur gjatë procesit të anketimit, ka rritje të besimit tek Autoritetit Për Sigurinë Kibernetike. Kjo pasi në fillim të pyetësorit pyetjes nëse kanë raportuar apo kërkuar asistencë në këtë institucion i janë përgjigjur pozitivisht vetëm 2.1%, ndërkohë që 55% nuk kanë raportuar e kërkuar asistencë, 21.1% nuk e njohin fare atë institucion.

- Të anketuarit i vlerësojnë si hapa të domosdoshëm për të parandaluar rritjen e rasteve të krimeve kibernetike në masën mbi 94% ofrimin e trajnimit të duhur të oficerëve të zbatimit të ligjit që punojnë në fushën e krimit kibernetik; rritjen e ndërgjegjësimit të publikut të gjerë; shtimin e numrit të oficerëve të zbatimit të ligjit që punojnë në fushën e krimit kibernetik; ndryshimet e duhura ligjore; ndryshimet e duhura strukturore; rritjen e bashkëpunimit publik-privat në këtë fushë; përfshirjen e njohurive mbi veprat penale kompjuterike në programet shkollore si dhe ashpërsimin e dënimeve ndaj autorëve të këtyre veprave penale.

- Është e nevojshme që të studiohen dhe gjenden format e metodat e duhura për të nxitur pjesëmarrjen e punonjësve të policisë dhe me gjere në anketime të ndryshme për probleme të luftës kundër krimit, çështjeve të sigurisë dhe jo vetëm, si një shprehje e rritjes së përgjegjësisë së tyre sociale për pjesëmarrje në procesin e hartimit të politikave për këto probleme.

Literatura

1. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels, 7.2.2013.
2. Informacion përmbledhës i analizave të Sektorit për Hetimin e Krimeve Kompjuterike, për vitet 2016 2018, dinamika e punës, prioritetet, kërkesat.
3. Dokumenti i Politikave për Sigurinë Kibernetike 2015-2017, miratuar me VKM nr. 973, datë 2.12.2015.
4. Dokumenti për Rishikimin e Strategjisë së Mbrojtjes së Republikës së Shqipërisë. Miratuar me VKM nr. 269, datë 3.04. 2013. Fletore Zyrtare Nr. 58, 19 prill 2013.
5. Strategjia e Sigurisë Kombëtare të Republikës së Shqipërisë, miratuar me Ligjin nr. 103/2014.
6. Strategjia Shtetërore për Sigurinë Kibernetike dhe Plani i Veprimit 2016-2019. Republika e Kosovës, Qeveria e Kosovës, Ministria e Punëve të Brendshme. dhjetor 2015.
7. Gjetjet e anketimit të realizuar *online* për periudhën 7-14 shtator 2018, me programin "Enalyzer", në adresën: https://surveys.enalyzer.com/?pid=f2q2s5r7.

Rëndësia e mbrojtjes së infrastrukturave kritike të informacionit – rasti i Shqipërisë

Dr. Vilma TOMÇO
Drejtoreshë e Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike
vilma.tomco@cesk.gov.al

MSc. Klorenta PASHAJ
Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike
klorenta.janushi@cesk.gov.al

Abstrakt

Mbrojtja e infrastrukturave kritike të informacionit është fushë prioritare, që nga krijimi i Internetit deri në ditët e sotme, kur sulmet kundrejt sistemeve kritike të informacionit prekin çdo sektor kritik. Funksionimi i sistemeve kritike lidhet në mënyrë të ngushtë me infrastrukturën e informacionit, ndaj shkëputja e funksionimit të kësaj të fundit do të pengonte funksionimin e vetë sistemit. Vendet e zhvilluara, kanë arritur të zbatojnë masat për mbrojtjen e infrastrukturave kritike të informacionit, por këto zgjidhje nuk janë gjithmonë të përshtatshme për vendet në zhvillim, apo për vende si Shqipëria. Me miratimin e listës së infrastrukturave kritike dhe të rëndësishme, të informacionit, lind nevoja e hartimit të një dokumenti, i cili përmban masat për mbrojtjen e sistemeve dhe sigurimin e vazhdimësisë së punës, pas sulmeve kibernetike që mund të evidentohen. Mbrojtja e infrastrukturave kritike të informacionit është përgjegjësi e përbashkët e sektorëve publikë e private. Megjithëse nuk ka një strategji të miratuar e publikuar për mbrojtjen e infrastrukturave kritike të informacionit, hartimi i rregulloreve dhe ndjekja e praktikave më të mira ul faktorët kërcënues dhe redukton rrezikun nga sulme kibernetike. Skuadrat CERT kombëtare/shtetërore dhe sektoriale janë organizma koordinues, në mbrojtjen e infrastrukturave kritike të informacionit, duke marrë masa për parandalimin e sulmeve, si dhe duke vepruar në mënyrë reaktive në trajtimin e incidenteve. Pas ndodhjes së një sulmi kibernetik, rekomandohet një bashkëveprim ndërmjet CERT-eve sektorialë dhe CERT-eve kombëtarë, për menaxhimin sa më efektiv të krizës. Në Shqipëri, Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK) vepron në cilësinë e CERT-it kombëtar. Gjithashtu, bashkëpunimi me organizma të tjerë në nivel ndërkombëtar dhe programet ndërgjegjësuese/trajnuese mund të reduktojnë në masë kërcënimet ndaj infrastrukturave kritike të informacionit. Ky artikull shtron nevojën e mbrojtjes së infrastrukturave kritike të informacionit dhe zhvillimin e praktikave të mbrojtjes së tyre, duke nënvizuar kërkesat në rastin e Shqipërisë, sipas sektorëve kritikë, në zbatim të kuadrit rregullator kombëtar dhe europian, të fushës së sigurisë kibernetike. Në fund të këtij punimi, janë paraqitur konkluzionet e nxjerra dhe disa rekomandime, për një qasje sa më të mirë të strategjive për mbrojtjen e infrastrukturave kritike të informacionit, të arritura, si rezultat i konstatimeve të nxjerra gjatë përgatitjes së punimit.

Fjalëkyçe:
infrastrukturë kritike informacioni, sisteme kritike, masa mbrojtëse, sektor kritik, CERT.

"If you close your eyes to facts, you will learn through incidents"
- Proverbë

1. Hyrje

Rrjetet e komunikimit dhe sistemet e informacionit janë bërë një faktor thelbësor në zhvillimin ekonomik dhe social. Informatika dhe rrjetëzimi, tani janë shërbime të domosdoshme, po aq të nevojshme, sa edhe furnizimi me energji elektrike apo ujë. Prandaj, siguria e rrjeteve të komunikimit dhe e sistemeve të informacionit, dhe disponueshmëria e tyre në veçanti, është një shqetësim në rritje për shoqërinë, për shkak të kompleksitetit të sistemeve, aksidenteve, gabimeve dhe sulmeve ndaj infrastrukturave fizike që ofrojnë shërbime kritike për mirëqenien e qytetarëve.

Zhvillimi i teknologjisë me hapa shumë të shpejtë e kompleksë, ka nxjerrë në pah domosdoshmërinë për përcaktimin e infrastrukturave kritike dhe të rëndësishme. Të gjitha vendet dhe qeveritë kërkojnë një mbështetje shumë të madhe nga strukturat e sigurisë, për të kuptuar rreziqet që lidhen me futjen e këtyre teknologjive. Në fakt, përballimi i këtyre rreziqeve është përgjegjësi e përbashkët që shtrihet si në strukturat ndërkombëtare, ashtu edhe në ato kombëtare. Përgjegjësia e përbashkët brenda vendit (kombëtare) përfshin industrinë private (e cila zotëron dhe operon infrastruktura shumë kritike), administratën dhe qytetarët.

Për sa më sipër, krijimi dhe funksionimi i një strukture për menaxhimin e incidenteve të sigurisë kompjuterike është një komponent shumë i vlefshëm për të ndihmuar në menaxhimin e këtyre fenomeneve të reja me pasoja në aktivitetet e biznesit, administratës apo jetës së qytetarëve. Kjo strukturë mund të jetë e organizuar në formate të ndryshme, por tashmë njihen si CIRT-e. Kjo strukturë, përveç përgjigjes ndaj incidenteve të sigurisë

kompjuterike, do të mundësojë aftësimin e strukturave qeverisëse, për të kuptuar dhe për t'iu përgjigjur kërcënimeve kibernetike, nëpërmjet një menaxhim të fuqishëm të incidenteve.

1.2 Konteksti i punimit

Rreziqet që lidhen me sulmet kibernetike, janë gjithnjë e në rritje dhe kërcënimet nga burimet e panjohura, evoluojnë vazhdimisht. Më shpesh se kurrë më parë, raporteve mbi incidente serioze të sigurisë, po u jepet përparësi në media, duke ilustruar një nevojë në rritje për menaxhimin efektiv dhe efikas të sigurisë kibernetike.

Si pasojë, çdo vend që ka qasje në internet, ka një interes në zbatimin e strategjive, për t'iu përgjigjur në mënyrë efektive dhe efikase incidenteve të sigurisë kibernetike, dhe për të mbrojtur këto funksione thelbësore, nga perspektiva e sigurisë kombëtare. *Ekipet e reagimit të emergjencave kompjuterike* (CERT) po luajnë një rol gjithnjë e më të rëndësishëm në këtë drejtim, pasi ata janë përgjegjës, për mbledhjen e informacionit dhe koordinimin e reagimit ndaj incidenteve të sigurisë kibernetike.

2.2 Qëllimi i përgjithshëm i punimit

Punimi, ka si qëllim kryesor që të evidentojë praktikat më të mira, për mbrojtjen e infrastrukturave kritike të informacionit, dhe të krahasojë përpjekjet e shtetit shqiptar, në kuadër të këtij qëllimi. Për realizimin e qëllimit, parashtrohen objektivat e mëposhtme:

- të identifikohen praktikat dhe strategjitë më të mira për mbrojtjen e infrastrukturave kritike të informacionit;
- të evidentohet rëndësia e skuadrave CERT, në mbrojtjen e infrastrukturave kritike të informacionit;
- të analizohet trajtimi i infrastrukturave kritike të informacionit në Shqipëri;
- të nxirren konkluzione për përmirësimin e përpjekjeve në kuadër të mbrojtjes së infrastrukturave kritike të informacionit.

2.3 Metodologjia

Kërkimet e kryera për këtë punim janë bazuar në një qasje deduktive, pra duke interpretuar artikuj shkencorë dhe praktikat më të mira të rekomanduara nga Bashkimi Evropian, në fushën e sigurisë kibernetike.

Duke qenë se studimi ka si qëllim edhe analizimin e situatës aktuale të legjislacionit shqiptar dhe të huaj, të organizmave të specializuara, në lidhje me sigurinë kibernetike, kërkimi është i bazuar në literaturën e huaj dhe atë shqiptare, ku përfshihen jo vetëm akte ligjore në fushën kibernetike, por edhe, strategji, rregullore, metodologji etj.

Trajtimi i infrastrukturave kritike të informacionit në legjislacionin shqiptar sjell nevojën e përdorimit të një qasjeje krahasuese. Të gjitha çështjet e trajtuara projektohen edhe në kontekstin shqiptar.

2.4 Struktura e punimit

Punimi është i organizuar në tri pjesë kryesore.

Pjesët 1 dhe 2, trajtojnë teorikisht konceptin e infrastrukturave kritike të informacionit, rëndësinë e tyre në nivel kombëtar dhe ndërkombëtar dhe nevojën për të hartuar politika për mbrojtjen e tyre.

Pjesa 3, është tërësisht e fokusuar në trajtimin e skuadrave CERT, si një ndër praktikat më të mira për mbrojtjen e infrastrukturave kritike të informacionit.

2. Vështrim i përgjithshëm mbi kuptimin e infrastrukturave kritike të informacionit

2.1 Çfarë janë infrastrukturat kritike të informacionit

Përkufizimi fillestar i CII u formulua rreth vitit 2001, nga disa profesorë dhe kërkues zviceranë, të cilët i përcaktuan infrastrukturat kritike të informacionit si "komponentë si, telekomunikacioni, kompjuterë/softuerë, internet, satelitë, fibra optike etj., si dhe tërësinë e kompjuterëve dhe rrjeteve të ndërlidhura, dhe rrjedhën e informacionit kritik ndërmjet tyre"[1].

G8-a, në vitin 2003, në një udhëzues mbi "Principet e mbrojtjes së infrastrukturave kritike të informacionit"[2], dha nocionin e saj, ndonëse, dokumenti fokusohej më shumë në dhënien e sugjerimeve për praktikat më të mira sesa në dhënien e një përkufizimi të qartë. Kjo nismë mori formë më konkrete, kur në vitin 2005, në *Dokumentin e Gjelbër* për një Program Evropian për Mbrojtjen e Infrastrukturave Kritike (EPCIP), Komisioni Evropian i përkufizoi CII-të si të gjithë "sistemet TIK, që janë vetë infrastruktura kritike ose, që janë thelbësore, për funksionimin e infrastrukturave kritike (telekomunikacion, / *softwar*e, Internet, satelitë, etj.)"[3] dhe, pas saj, shumë shtete formuluan nocionet e tyre për CII. Disa përkufizime të CII nga e gjithë bota janë:

"Infrastruktura kritike e Cyber/TIK do të thotë infrastruktura kibernetike që është esenciale për shërbimet e sigurisë publike, stabilitetit ekonomik, sigurisë kombëtare, stabilitetit ndërkombëtar dhe qëndrueshmërisë dhe restaurimit të hapësirës kibernetike kritike" (Bashkimi Afrikan)[4].

"Komponenti TIK i infrastrukturës kritike, quhet infrastrukturë kritike informacioni" (Viktoria)[5].

"Infrastrukturat kritike të informacionit janë nëngrupet e aseteve të informacionit që ndikojnë drejtpërdrejt në arritjen dhe vazhdimësinë e misionit shtetëror dhe sigurinë e shoqërisë " (Brazil)[6].

"Një infrastrukturë kritike informacioni, mund t'u referohet të gjitha sistemeve të teknologjisë së informacionit, që mbështesin asetet dhe shërbimet kryesore brenda infrastrukturës kombëtare" (Mbretëria e Bashkuar)[7].

"Infrastrukturë kritike e informacionit" është tërësia e rrjeteve dhe sistemeve të informacionit, cenimi apo shkatërrimi i të cilave do të kishte impakt serioz në shëndetin, sigurinë dhe/ose mirëqenien ekonomike të qytetarëve dhe/ose funksionimin efektiv të ekonomisë në Republikën e Shqipërisë" (Republika e Shqipërisë)[8].

Megjithëse nuk ka përkufizim të përbashkët global të infrastrukturave kritike të informacionit (CII), ai që mbetet gjerësisht i pranueshëm është përkufizimi i dhënë nga

[1] S. Bruno and M. Dunn, Critical Information Infrastructure Protection: An Inventory of Protection Policies in Eight Countries, ETH, Zürich, Switzerland, 2002.
[2] G8, G8 Principles for Protecting Critical Information Infrastructures, 2003.
[3] Commission Of The European Communities, 17 November 2005, Green Paper on a European Programme or Critical Infrastructure Protection.
[4] African Union, African Union Convention on Cyber Security and Personal Data Protection, LC12490.
[5] Victorian Government CIO Council, Critical Information Infrastructure Risk Management, Victoria, Australia, 2012.
[6] Guia de referência para a segurança das infraestruturas críticas da Informação Versão 01 (Nov. 2010).
[7] Cyber Security in the UK, Postnote Number 389, September 2017.
[8] Metodologji për identifikimin dhe klasifikimin e infrastrukturave kritike dhe infrastrukturave të rëndësishme të informacionit.

Organizata për Bashkëpunim dhe Zhvillim Ekonomik (OECD) në vitin 2008. Në mbështetje të dhënies së një kuptimi sa më të qartë të infrastrukturave kritike të informacionit, është e nevojshme të bëhet dallimi me infrastrukturat kritike dhe mbrojtjen e infrastrukturave kritike të informacionit:

Infrastruktura kritike (CI) nënkupton një aset, sistem ose pjesë të tij të vendosur në një shtet, që është thelbësor për ruajtjen e funksioneve jetësore shoqërore, shëndetin, sigurinë, mbrojtjen, mirëqenien ekonomike ose sociale të njerëzve dhe prishja ose shkatërrimi i të cilave do të kishte një ndikim të rëndësishëm në një shtet si rezultat i dështimit në ruajtjen e këtyre funksioneve[9].

Infrastruktura kritike e informacionit (CII): "Të gjitha ato sisteme dhe rrjete të ndërlidhura informacioni, ndërprerja apo shkatërrimi i të cilave do të kishte një ndikim serioz në shëndetin, sigurinë, mbrojtjen ose mirëqenien ekonomike të qytetarëve, ose në funksionimin efektiv të qeverisë ose ekonomisë " (OECD)[10].

Mbrojtja e infrastrukturës kritike të informacionit (CIIP) është derivat i përkufizimit të CII dhe përfshin: "Të gjitha aktivitetet që synojnë të sigurojnë funksionalitetin, vazhdimësinë dhe integritetin e CII, në mënyrë që të pengojnë, zbutin dhe neutralizojnë kërcënimin, rrezikun ose cenueshmërinë ose minimizojnë ndikimin e një incidenti"[11].

2.2 Identifikimi i infrastrukturave kritike të informacionit

Operatorët publikë, gjysmëpublikë dhe privatë të CI-së, ofrojnë mallra dhe shërbime. Është lloji i mallrave dhe shërbimeve të ofruara nga këta operatorë dhe mënyra e përdorimit nga klientët e tyre që përcakton nëse një shërbim infrastrukture është kritik. Tabela 1 jep shembuj të sektorëve të CI[12].

Sektorët e Infrastrukturave Kritike
Shërbimi bankar dhe financa
Qeverisja qendrore/shërbimet qeveritare
Telekomunikacioni /sektori i teknologjisë së informacionit dhe komunikimit
Shërbimet e emergjencës dhe shpëtimit
Shërbimi i furnizimit me energji elektrike
Shërbimi shëndetësor
Transporti/logjistika/furnizimi
Shërbimi i furnizimit me ujë
Ushqimi
Mbrojtja mjedisore

Tabela 1: Sektorët e infrastrukturave kritike

[9] Wenger A, Metsger J, Dunn M, International CIIP Handbook – Critical Information Infrastructure Protection.
[10] OECD ICCP Committee and the Working Party on Information Security and Privacy, OECD Recommendation on the Protection of Critical Information Infrastructures.
[11] Po aty.
[12] CIPedia©: a common international reference point for CIP and CIIP concepts and definitions.

Identifikimi i infrastrukturave kritike të informacionit, shpesh, është më kompleks se identifikimi i infrastrukturave kritike. Sipas OECD, infrastrukturat kritike të informacionit, zakonisht, përfshijnë një ose më shumë nga:

- komponentët e informacionit që mbështesin CI;
- dhe/ose, infrastrukturat e informacionit që mbështesin komponentët thelbësorë të shërbimit qeveritar;
- dhe/ose, infrastrukturat e informacionit thelbësor për ekonominë kombëtare[13].

Siç shfaqet në figurën 1[14], CII përfshin si infrastrukturën kritike të informacionit dhe komunikimit (p.sh. shërbimet e telekomunikacionit celular) dhe infrastrukturën kritike të informacionit dhe komunikimit brenda secilit prej CI, të tilla si sistemet kritike kibernetike dhe sistemet kryesore administrative.

Shembuj të CII-së, janë shërbimet e informacionit midis bankave, për të shlyer llogaritë, dhe aksesi në infrastrukturë, për të përdorur shërbimet globale të internetit.

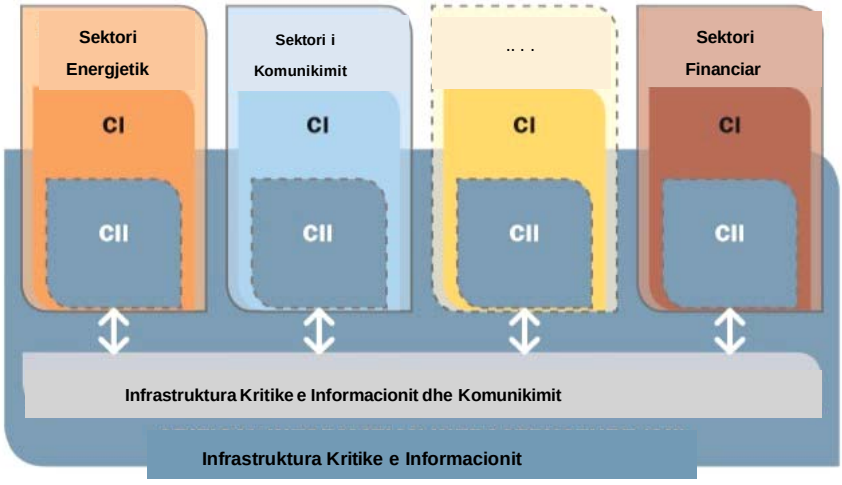


Figura 1: Ndërtimi i infrastrukturave kritike të informacionit

Sipas ENISA[15], kriteret dhe faktorët për identifikimin dhe klasifikimin e infrastrukturave të informacionit mund të listohen si më poshtë:

Kriteret	Faktorët
Ndikimi ekonomik	Efekti financiar
Ndikimi polik/qeveritar	Efekti në kohë
Ndikimi industrial/mjedisor	Shpërndarja gjeografike
Ndikimi shëndetësor	

Tabela 2: Kriteret dhe faktorët për identifikimin e CII

[13] OECD ICCP Committee and the Working Party on Information Security and Privacy, OECD. Recommendation on the Protection of Critical Information Infrastructures.
[14] CSIRT Maturity Kit: A step-by-step guide towards enhancing CSIRT Maturity, NCSC, The Hague, Netherlands.
[15] GFCE-Meridian, Good Practice Guide on Critical Information Infrastructure Protection-for governmental policy-makers.

Faktorët që duhet të aplikohen për të identifikuar infrastrukturat kritike dhe të rëndësishme janë:

1. efekti financiar: ndikimi financiar që shkaktohet kur infrastruktura është jashtë funksionimit;

2. shpërndarja gjeografike: numri i individëve që mund të ndikohet nga mosfunksionimi i infrastrukturës;

3. efekti i kohës: përcaktohet në orë, ditë, muaj dhe vite, i cili tregon ndikimin që një shërbim do ketë, në humbje, kur është jashtë funksionimit.

Në Shqipëri, Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike

(AKCESK), në dokumentin "Metodologji për identifikimin dhe klasifikimin e infrastrukturave kritike dhe infrastrukturave të rëndësishme të informacionit"[16], mbështetur në praktikat europiane më të mira, përcakton se mosfunksionimi i sistemit/rrjetit ka ndikim kritik në sektorin ku operon institucioni, nëse:

- ndikimi financiar është më shumë se 3.3 milionë lekë, dhe/ose,
- më shumë se 39000 individë, ndikohen nga mosfunksionimi i infrastrukturës, dhe/ose,
- shkëputja ndodh për intervale më të gjata se 24 orë.

Në bazë të ligjit nr. 2/2017 për "Sigurinë kibernetike", neni 6, pika 2, Këshilli i Ministrave miraton listën e infrastrukturave kritike të informacionit, e cila përditësohet, të paktën një herë në dy vjet[17]. Lista e infrastrukturave kritike të informacionit u miratua më 26 prill 2018[18].

2.3 Identifikimi i kërcënimeve ndaj infrastrukturave kritike të informacionit

Për shkak të rëndësisë së infrastrukturave kritike të informacionit, sistemet gjenden vazhdimisht nën kërcënimin e sulmeve ndaj tyre dhe të pasojave të mundshme, që sjell një CII e dobët ose e sulmuar.

Kërcënimet ndaj CII-së përfshijnë:

- hyrje të paautorizuar në informacione të ndjeshme ose konfidenciale;
- shkatërrimin, modifikimin ose zëvendësimin e softuerit të përdorur nga infrastruktura kritike;
- hyrje e kufizuar për agjentët, për të parandaluar ose zbutur rezultatet e sulmeve.

Pasojat e mundshme të sulmeve ndaj infrastrukturave kritike të informacionit përfshijnë:

- bllokimin e transportit, të furnizimit me energji elektrike dhe ujë, të komunikimit, të transmetimit së të dhënave, të centraleve bërthamore, të kontrollit të trafikut ajror;
- falimentimin e strukturave tregtare dhe të sistemeve financiare, dështimin e transaksioneve ndërkombëtare të biznesit, destabilizimin e tregjeve dhe institucioneve financiare, vjedhjen e parave dhe të informacionit;
- humbjen e pronësisë intelektuale ose të reputacionit (për shkak të një sulmi me *worms*, kompania për pagesat *online PayPal* u përball me një rrezik falimentimi në vitin 2002);
- viktimat njerëzore ose humbjet materiale, të shkaktuara nga përdorimi shkatërrues i elementeve të infrastrukturës kritike (sabotimi kibernetik në industrinë ushqimore, në

[16] ENISA, Methodologies for the identification of Critical Information Infrastructure assets and services, December 2014.

[17] Metodologji për identifikimin dhe klasifikimin e infrastrukturave kritike dhe infrastrukturave të rëndësishme të informacionit.

[18] ENISA, po aty.

trafikun ajror ose atë hekurudhor);

- hyrjen te informacioni personal, dhe/ose modifikimin e paautorizuar të tij;

- mundësinë për të nxitur akte terroriste në një shtet/qeveri tjetër dhe përkeqësimin e tensioneve në marrëdhëniet ndërkombëtare[19].

Ndërsa rimëkëmbja pas një sulmi ndaj një CII-je, mund të jetë, në disa raste, një detyrë e shpejtë dhe e lehtë, efektet indirekte të sulmit mund të ndjehen për një kohë të gjatë. Sulmet ndaj CII-ve mund të dëmtojnë seriozisht besimin e publikut dhe të biznesit, në tregtinë elektronike dhe iniciativat qeveritare. Shpenzimet njerëzore dhe ekonomike të lidhura, me strategjitë e rimëkëmbjes ose zbutjes, janë të mëdha. Humbjet e biznesit dhe produktivitetit maten në miliarda dollarë nga secili sulm në mbarë botën, dhe madje, edhe shitësit më të mëdhenj të softuerëve, janë nën presionin për të vazhduar me përmirësimin e masave të sigurisë.

Incidentet e ndodhura në Estoni, në vitin 2007, dhe Gjeorgji në 2008-ën, kanë treguar pamundësinë e shteteve për të funksionuar efektivisht, kur sulmet kibernetike prekin infrastrukturat e informacionit. Natyra ndërlidhëse e sistemeve, falë internetit, mundëson që sulmet të realizohen nga çdo vend i botës. Si rezultat i zhvillimit më të madh të teknologjisë, shtetet e zhvilluara kanë qenë iniciatorët e këtyre sulmeve.

Të shumta janë edhe rastet e sistemeve, që janë sulmuar dhe kompromentuar në Lindjen e Largët. Shumica e sulmeve kanë qenë të motivuar politikisht. Përgjatë tensioneve politike mes shteteve, është vërejtur një rritje e sulmeve kibernetike. Shembujt janë të shumtë, mjafton të përmendim këtu konfliktin midis Indisë dhe Pakistanit në territorin e Kashmirit. Pakistani arriti të sulmonte faqen e Parlamentit, sistemin e Institutit të Shkencave, qendrën kërkimore *Bhabha Atomic Research Center*, nga e cila u morën informacione sensitive. Konflikti Izrael-Palestinë, ka sjellë gjithashtu, shumë sulme kibernetike që lidhen me pasoja reale etj. Cenimi i sigurisë, ka ndodhur edhe për shkak të mungesës së politikave të sigurisë kibernetike dhe standardeve, për mbrojtjen e CII-ve.

2.4 Nevoja për mbrojtjen e infrastrukturave kritike të informacionit

Sistemi shëndetësor, siguria, mirëqenia ekonomike e qytetarëve, funksionimi efektiv i qeverisë, dhe ndoshta edhe mbijetesa e botës së industrializuar, mbështetet shumë në sistemet kritike të ndërlidhura. Një vend mund të përjetojë kaos, madje mund të përjetojë humbje të jetëve njerëzore, nëse këto sisteme bëhen të paoperueshme. Besueshmëria, stabiliteti dhe mbrojtja e ndërlidhjes së infrastrukturave të informacionit, janë bërë çelës për funksionimin e sistemeve kritike të një vendi.

Mbrojtja e infrastrukturave kritike të informacionit (CIIP) është një temë komplekse, por e rëndësishme për kombet. Kombet e mëdha, në mënyrë kritike, varen nga shërbimet e infrastrukturës kritike (CI) si: furnizimi me energji, telekomunikacioni, sistemet financiare, uji i pijshëm dhe shërbimet qeveritare.

Siguria Kibernetike
Figura 2: Lidhja ndërmjet CIP, CIIP dhe Sigurisë Kibernetike

[19] VKM nr. 222, datë 26.4.2017, "Për miratimin e listës së infrastrukturave kritike të informacionit dhe të listës së infrastrukturave të rëndësishme të informacionit".

Mbrojtja e infrastrukturave kritike të informacionit dhe siguria kibernetike *(Cyber Security*) janë terma që, shpesh, plotësojnë njëra-tjetrën në çështjet që kanë të bëjnë me sigurinë e infrastrukturave dhe të informacionit. Megjithatë, siguria kibernetike nuk është iniciativë e njëjtë me CIIP-in. CIIP-i është pjesë integrale e mbrojtjes së infrastrukturave kritike (CIP). Në kahun tjetër, CIIP-i është bërthama e sigurisë kibernetike dhe qëllimi më i rëndësishëm i saj, por nuk është i barabartë me sigurinë kibernetike dhe përjashton krimin kibernetik të zakonshëm, çështjet e privatësisë dhe të drejtave të njeriut, si dhe çështjet e kibernetikës ekonomike[20].

Siguria kibernetike: "Siguria Kibernetike është koleksioni i mjeteve, politikave, koncepteve të sigurisë, masave të sigurisë, udhëzimeve, politikave të menaxhimit të rrezikut, veprimeve, trajnimit, praktikave më të mira, sigurimit dhe teknologjive që mund të përdoren për të mbrojtur mjedisin kibernetik dhe asetet e përdoruesve dhe organizatës"[21].

Sot, ndërprerja fizike (apo edhe shkatërrimi) i elementeve kritike të CI-së nuk është i vetmi faktor që kërcënon funksionimin korrekt të CI-së. Shërbimet e bazuara në teknologjitë e informacionit dhe të komunikimit (ICT), po bëhen gjithnjë e më të rëndësishme për funksionimin e CI-së. Ndërprerja e infrastrukturës së informacionit është e aftë të shkaktojë ndikim të madh te një komb. Kjo çon në konceptin e infrastrukturës kritike të informacionit (CII) i cili përfshin infrastrukturën e informacionit kritik dhe telekomunikimit (p.sh. shërbimet e telefonisë mobile dhe të qasjes në internet), dhe sistemet e kontrollit të TIK-ut e proceseve, të cilat janë një pjesë kritike e ofrimit të shërbimit CI-së (shih *Figurën 1*).

CII-ja është gjithnjë e më tepër pjesë kritike e CI-së dhe po bëhet globalisht e ndërlidhur. Në të njëjtën kohë, CII-ja e një vendi mund të jetë objektiv për *malware*-t, hakerat, haktivistët, si dhe një mjet për të sulmuar CII-të e një kombi tjetër. Një CII i kompromentuar ose i dobët, mund të rrezikojë sigurinë dhe stabilitetin kombëtar, rritjen ekonomike, prosperitetin e qytetarëve dhe jetën e përditshme, dhe mund të ketë ndikim të gjerë në vende të tjera, për shkak të ndërlidhjes globale të CII-së. Nevoja për strategjitë, politikat dhe aktivitetet për një CIIP efektive, kësisoj, bëhet gjithnjë e më e rëndësishme në shumicën e vendeve.

3. Mbrojtja e infrastrukturave kritike të informacionit

3.1 Strategjitë për mbrojtjen e infrastrukturave kritike të informacionit

Për shkak të ndërlidhjes ndërsektoriale, mbrojtja e infrastrukturave kritike të informacionit (CIIP) është përgjegjësi e përbashkët e sektorit publik dhe privat. Ashtu si për çdo infrastrukturë informacioni, edhe në drejtim të mbrojtjes së CII, nuk ekziston asnjë strategji plotësisht efektive. Qëllimi është që të krijohen masa sigurie për të reduktuar në maksimum mundësitë për sulme ndaj CII-ve. Si një udhëzues i përgjithshëm, parimet e mëposhtme duhet të jenë qendrore, në drejtim të sigurimit të një programi efektiv të sigurisë së CII-së[22]:

- mënyra më efektive për të siguruar një biznes/institucion është kombinimi i informacioneve me shtresa sigurie, përveç masave të sigurisë njerëzore;

[20] CSIRT Maturity Kit: A step-by-step guide towards enhancing CSIRT Maturity, NCSC, The Hague.
[21] Nickolov E, Critical Information Infrastructure Protection: Analysis, Evaluation and Expectations.
[22] ITU Security in Telecommunications and Information Technology: An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications, ITU-T, Geneva.

- masat duhet të jenë proporcionale me kërcënimin e pritur dhe me profilin e rrezikut të organizatës, si dhe me industrinë dhe vendndodhjen specifike të operacioneve;

- nuk është e mundur që të mbrohen të gjitha asetet në çdo kohë; nevojitet që t'u jepet përparësi fushave kryesore, për t'u mbrojtur së pari;

- siguria është kosto efektive kur përfshihet në planifikimin afatgjatë.

Pasi përcaktohen parimet brenda një sektori kritik, nevojitet të vendosen qëllime ndërsektoriale me fokus mbrojtjen e infrastrukturave kritike të informacionit. Këto qëllime përfshijnë:

- lehtësimin për zhvillimin e një strategjie kombëtare për mbrojtjen e infrastrukturës kritike të informacionit (CIIP);

- asistimin e sektorëve, nënsektorëve dhe operatorëve të infrastrukturës kritike, si të qeverisë ashtu edhe të subjekteve të sektorit privat për të zbutur rrezikun ndaj informacionit;

- identifikimin e informacionit kritik të sektorit dhe varësisë ndërsektoriale;

- bashkëpunimin me organizatat ndërkombëtare CIP/CIIP për të krijuar zgjidhje rajonale dhe/ose ndërkombëtare.

Tri shtyllat në të cilat mbështetet një program CIIP-i efektiv janë:

- *Udhëheqja dhe qeverisja:* të krijohet udhëheqje dhe qeverisje e qartë në menaxhimin e rrezikut të sigurisë së informacionit, në nivel kombëtar dhe në nivel organizatash.

- *Zbutja e rrezikut:* vendosja e politikave të detyrueshme të menaxhimit të rrezikut të sigurisë së informacionit, për operatorët e sektorit kritik, për t'i mbrojtur nga kërcënimet e sigurisë kibernetike.

- *Ndërgjegjësimi dhe parandalimi:* promovimi i praktikave më të mira të sigurisë së informacionit dhe një kulture të sigurisë kibernetike, brenda sektorëve kritikë[23].

3.2 Praktikat më të mira për zhvillimin e politikave për mbrojtjen e infrastrukturave kritike të informacionit

Megjithëse ka shumë mënyra për të parandaluar ngjarjet shkatërruese, nuk ka asnjë mënyrë, që parandalimi të mund të eliminojë të gjitha rreziqet që lidhen me CII, për kombet dhe qytetarët e tyre. Menaxhimi kombëtar i krizave organizon dhe menaxhon të gjitha rolet, përgjegjësitë dhe burimet për t'u marrë me incidentet serioze, emergjencat dhe krizat në nivel kombëtar. Menaxhimi i mirë i krizave në nivel kombëtar, si dhe në nivel ndërkombëtar dhe rajonal, merr CII si pjesë të përgatitjes së tij, të reagimit dhe fazave të rimëkëmbjes, mbi bazën e mëposhtme:

- Pasojat e një ndërprerje të CII-ve mund të jenë të rënda. Parandalimi i ndërprerjes së CII-ve dhe menaxhimi i duhur i incidenteve është një detyrë parësore e operatorit të CII. Ushtrimet e përbashkëta ndërsektoriale mund të rrisin gatishmërinë e operatorëve administrues të CII-ve në një masë të madhe.

- Për organizatat e reagimit ndaj incidenteve, vazhdimësia e shërbimeve CII mund të jetë vendimtare për efektivitetin e operacioneve të tyre.

Është e qartë se menaxhimi efektiv i incidenteve kibernetike kërkon njohuri të thella mbi CII-të, operacionet e tyre dhe varësitë e tyre. Bashkëpunimi i ndërsjellë i operatorëve CI / CII është ndër hapat më të rëndësishëm për planifikimin e reagimit ndaj incidenteve, përgatitjes së emergjencave (p.sh. trajnimet e përbashkëta dhe iniciativat

[23] Wolfpack Information Risk, 2016, South Africa – Critical Information Infrastructure Protection Report.

ndërsektoriale), reagimin ndaj krizave dhe rimëkëmbjen. Një organ koordinues për CIIP i modernizon përpjekjet.

Praktikat më të mira për mbrojtjen e infrastrukturave kritike të informacionit përfshijnë:

- përfshirjen e ekspertizës CII me funksion mbështetjeje për menaxhimin kombëtar të krizave;
- krijimin e një organi koordinues për CIIP – skuadrat CERT /CIRT;
- iniciativën e përbashkët për menaxhimin e krizave publiko-private, duke përfshirë sektorët/operatorët CII.

4. CERT, si struktura kryesore për mbrojtjen e infrastrukturave kritike të informacionit

4.1 Nivelet e planifikimit të mbrojtjes

Përpjekjet për mbrojtjen e infrastrukturave kritike të informacionit mund të mbështeten nga një mekanizëm i përbashkët koordinues. Një organ i tillë mund të veprojë në nivel strategjik ose taktik, por edhe në nivel teknik/operacional[24]. Ka disa përfitime në kombinimin e disa prej këtyre niveleve në lidhje me CIIP.

Nivelet taktike dhe strategjike: kryesisht të iniciuara nga vullneti politik, ato mund të jenë për shembull, aktive në hartimin e strategjive të CIIP-ve, në krijimin e lidhjeve ndërkombëtare (në nivel strategjik, taktik, operacional/teknik), dhe për të nxitur dialogët ndërkombëtarë me rrjetet publike dhe palët e interesuara private CII/CIIP.

Niveli operacional/teknik: në CIIP mund të jenë *ekipet e reagimit të emergjencave kompjuterike* (CERT) publike dhe private, të njohura edhe si *ekipet e reagimit të incidenteve të sigurisë kompjuterike* (CSIRT). CERT-ët shpesh kanë një rol të rëndësishëm në zhvillimin e aftësisë teknike të reagimit ndaj incidentit për CII-të. Për ta bërë këtë, CERT monitoron, paralajmëron dhe jep mbështetje gjatë incidenteve kibernetike nën juridiksionin e tyre. Një CERT mund të ketë lidhje të forta me një entitet që koordinon CIIP në nivelin taktik.

Në rastin e privatizimit, operatorët CI/CII mund të krijojnë CERT-e brenda secilit sektor, për të ruajtur sigurinë e CII-së. Në raste të tilla, rekomandohet që organet publike ose CERT-ët kombëtarë të ndërveprojnë ose të formojnë një aleancë me CERT-ët privatë.

Vitet e fundit, disa vende kanë krijuar qendra kombëtare të sigurisë kibernetike (NCSC) në të cilën skuadrat CSIRT/CERT janë elemente thelbësore. Një qendër e tillë mund të kombinojë dhe të koordinojë përpjekjet e aktorëve publikë, në lidhje me CIIP (identifikimi CI / CII, vlerësimi i rrezikut, monitorimi dhe bashkëpunimi ndërkombëtar). Nga një vëzhgim i NCSC-ve, në mbarë botën, është identifikuar se ato janë organe koordinuese, që përfshijnë aktivisht palët e interesuara, në CIIP. Disa NCSC ofrojnë shërbimet e tyre për palët publike dhe private. Ata mund të veprojnë si ndërmjetës të besuar (pa model biznesi). Krijimi i një NCSC-je nuk është i përshtatshëm gjatë hapave të parë të CIIP-it, por mund të jetë shumë i dobishëm në ndërmarrjen e hapave të mëtejshëm.

Funksionet dhe kompetencat që kanë këto organizma, ndryshojnë në varësi të shteteve. Në rastet kur ekziston *qendra kombëtare e sigurisë kibernetike*, një CSIRT/

[24] Usmani KA, Incident response and its role in protecting critical infrastrukture.

CERT kombëtar ose një iniciativë e ngjashme, kjo organizatë mund të marrë rolin udhëheqës në këtë përpjekje, por gjithmonë do të ketë nevojë, për kontributin e operatorëve CI/CII, për të vlerësuar ndikimin e mundshëm në CI, dhe për një rrjet ndërkombëtar publik, privat dhe akademik, për të fituar njohuritë më të fundit.

4.2 Llojet e skuadrave CERT

Në këtë seksion sqarohen disa nocione kryesore lidhur me CERT-ët kombëtarë, qeveritare dhe sektoriale[25].

CERT/CSIRT: *ekipi i reagimit të emergjencave kompjuterike* (CERT) është një organizatë shërbimi përgjegjëse për një zonë zgjedhore të përcaktuar për t'iu përgjigjur incidenteve të sigurisë kibernetike. Ai siguron shërbimet e nevojshme për trajtimin e incidenteve dhe mbështet rimëkëmbjen e proceseve. Për të zbutur rreziqet dhe për të minimizuar numrin e sulmeve, shumica e CERT-ëve gjithashtu ofrojnë shërbime parandaluese dhe edukative për zonat e tyre zgjedhore. Zona zgjedhore (një term i vendosur për bazën e konsumatorëve) e një CERT-i zakonisht i takon një sektori specifik, si akademia, kompanitë, qeveria apo ushtria. Termi CSIRT (*ekipi i reagimit ndaj incidenteve të sigurisë kompjuterike*) është një sinonim më modern që ilustron faktin se CERT-ët zhvillohen me kalimin e kohës, nga vetëm forca reaktive, në ofrues universalë të shërbimeve të sigurisë.

CERT kombëtar: një CERT kombëtar vepron si një pikë kontakti kombëtare (PoC) për bashkëpunimin dhe shkëmbimin e informacionit (siç janë, raportet e incidenteve dhe informacion mbi dobësitë) me CERT-ët e tjerë kombëtarë në mbarë botën. CERT-i kombëtar gjithashtu mund të konsiderohet si CERT-i i fundit-resort për domenin kombëtar, i cili është një pikë unike kombëtare e kontaktit me një rol koordinues. Në shumë raste, një CERT kombëtar vepron gjithashtu si CERT qeveritar. Duhet të theksohet se përkufizimet mund të ndryshojnë në varësi të shteteve.

CERT ' de facto' kombëtar: një CERT 'de facto' kombëtar vepron si një PoC në vendet ku ende nuk është themeluar ndonjë CERT zyrtar kombëtar nga qeveria. Zakonisht CERT-i i parë i krijuar në një vend perceptohet si CERT 'de facto' kombëtar nga ekipet e vendeve të tjera. CERT-ët "de facto' kombëtarë janë të domosdoshëm për menaxhimin e incidenteve ndërkufitare derisa të krijohet një CERT zyrtar kombëtar ose CERT-i 'de facto' kombëtar mandatohet nga qeveria.

CERT qeveritar: një CERT qeveritar është përgjegjës për mbrojtjen e rrjeteve qeveritare dhe të administratës publike. Pra, juridiksioni i një CERT-i qeveritar është qeveria dhe organet e tjera publike. Duhet të theksohet se, në shumë raste, CERT-ët ushtarakë konsiderohen veçmas për shkak të përgjegjësisë së tyre të veçantë. Praktikat aktuale ilustrojnë se në shumë raste CERT-ët qeveritarë gjithashtu veprojnë si CERT-ë kombëtarë.

CSIRT sektorial: ekipi/personi përgjegjës ndaj incidenteve të sigurisë kibernetike, në strukturën e një operatori që administron infrastrukturat kritike dhe të rëndësishme të informacionit.

4.3 Detyrat e skuadrave CERT për mbrojtjen e infrastrukturave kritike të informacionit

Përveç shërbimeve që një CERT ofron në varësi të shtrirjes së kompetencave të tij (kombëtar, qeveritar apo sektorial), shërbimet që ofron një CERT/CSIRT janë në varësi

[25] ENISA, Baseline capabilities of national/governmental CERTs, Part 2: Policy Recommendations.

edhe të nivelit të maturitetit të skuadrës, të cilat variojnë nga shërbimet reaktive deri në implementimin e shërbimeve proaktive dhe menaxhimit të cilësisë. Shërbimet reaktive synojnë trajtimin e incidenteve dhe minimizimin e dëmit, ndërsa shërbimet proaktive synojnë parandalimin e incidenteve përmes ndërgjegjësimit dhe trajnimit. Shërbimet e menaxhimit të cilësisë së sigurisë, janë shërbime me qëllime afatgjata dhe përfshijnë masa këshilluese dhe edukative[26].

Niveli i maturitetit	Përshkrimi
1. Fillestar	CERT/CSIRT-i ekziston si pikë kontakti për koordinimin dhe zgjidhjen e incidenteve. Gjithashtu janë krijuar rregulloret dhe politikat për koordinimin me autoritetet e tjera përgjegjëse.
2. Bazik	Përveç cilësive të nivelit të parë, në këtë nivel CERT/CSIRT-i ka të implementuar një proces për trajtimin e kërcënimeve të reja. Për raportimin e incidenteve përdoret një sistem i dedikuar, si p.sh. RTIR.
3. Aktiv	Përveç cilësive të nivelit të dytë, në këtë nivel CERT/CSIRT-i ka të implementuar *tools*-e për të analizuar kërcënimet dhe ekzistojnë procedura për klasifikimin dhe shkëmbimin e informacionit.
4. Proaktiv	Përveç cilësive të nivelit të tretë, në këtë nivel CERT/CSIRT-i realizon rregullisht kontrolle për të ruajtur statusin e sigurisë dhe ka planifikuar trajnimin e vazhdueshëm të anëtarëve të ekipit.
5. I avancuar	Përveç cilësive të nivelit të katërt, në këtë nivel CERT/CSIRT-i monitoron në kohë reale incidentet dhe kërcënimet. Udhëzimet për kërcënimet e reja dhe parandalimin e incidenteve hartohen dhe ndahen brenda dhe jashtë organizatës me qëllim rritjen e ndërgjegjësimit.

Figura 3: Nivelet e maturitetit të skuadrave CERT/CSIRT

Roli i një CERT-i kombëtar/qeveritar në strategjinë e mbrojtjes së infrastrukturave kritike të informacionit, nuk është standard. Disa shërbime, mund të ofrohen krahas shërbimit të trajtimit të incidentit. Shembuj të tillë përfshijnë analizën e rrezikut, konsultimet për sigurinë, vlerësimin e sigurisë, shërbimet e zbulimit të ndërhyrjeve dhe shumë shërbime të tjera. Roli i saktë i CERT-it kombëtar/qeveritar varet shumë nga strategjia kombëtare për CIIP.

Në kontekstin e CIIP, përveç shërbimeve të renditura më lart, këshillohet që CERT-ët kombëtarë/qeveritarë të ofrojnë shërbime shtesë si:

- njoftime të karakterit informues për sektorët/operatorët e CI-ve rreth zhvillimeve të reja me ndikim afatmesëm dhe afatgjatë, siç janë dobësitë e reja;
- shpërndarje të informacioneve lidhur me sigurinë, të cilat u japin sektorëve/operatorëve, një koleksion gjithëpërfshirës informacionesh dhe udhëzimesh të dobishme për përmirësimin e sigurisë;
- alarme dhe paralajmërime që përfshijnë shpërndarjen e një informacioni të detajuar që përshkruan një sulm nga një ndërhyrje, sigurinë e dobët, alarme në rastin e një ndërhyrjeje, virusin kompjuterik ose mashtrimin etj., dhe siguron një kurs veprimi të rekomanduar afatshkurtër për trajtimin e problemit që rezulton;
- shpërndarje informacionesh dhe udhëzimesh për përshtatje më të mirë me praktikat e sigurisë dhe politikat e sigurisë organizative.

Këto shërbime i japin vlerë të shtuar dhe kosto-efektivitet CERT-ëve, pasi

informacioni i nevojshëm për të ofruar këto shërbime bazë mund të përdoret për shumë sektorë njëkohësisht. Përveç kësaj, njoftimet e sigurisë dhe informacione të tjera për palët e interesuara e përmirësojnë imazhin e një CERT-i kombëtar/qeveritar dhe lehtësojnë ndërtimin e besimit në aftësitë e skuadrës.

Shumica e CERT-ëve kombëtarë/shtetërorë ofrojnë shërbime "falas" (siç janë njoftimet dhe paralajmërimet) për publikun, por ofrojnë shërbime shtesë (përgjigje ndaj incidentit, trajtim dobësish, analiza, etj.) vetëm ndaj qeverisë, institucioneve publike dhe njësive të CII-ve.

4.4 Procesi i trajtimit të incidenteve

Sulmet klasifikohen si incidente, nëse: janë të drejtuara kundër aseteve të informacionit; kanë një shans real për sukses; mund të kërcënojë konfidencialitetin, integritetin ose disponueshmërinë e burimeve të informacionit. Pasi një incident ndodh, fillon zbatimi i strategjisë së vazhdimësisë (CP) e cila përbëhet nga tri planet e mëposhtme:

1. *Plani i përgjigjes ndaj incidenteve (IRP)* – fokusohet në përgjigje të menjëhershme; nëse sulmi përshkallëzohet apo është katastrofik, procesi ndryshon në DRP dhe BCP.

2. *Plani i rimëkëmbjes nga fatkeqësitë (DRP)* – zakonisht fokusohet në rikthimin e sistemeve pasi fatkeqësia të ndodhë; si i tillë, është i lidhur ngushtë me BCP.

3. *Plani i vazhdimësisë së biznesit (BCP)* – ndodh njëkohësisht me DRP kur dëmi është i madh apo afatgjatë, që kërkon më shumë se rikthimin e thjeshtë të informacionit dhe të burimeve të informacionit. (Shih *Figurën 4*)

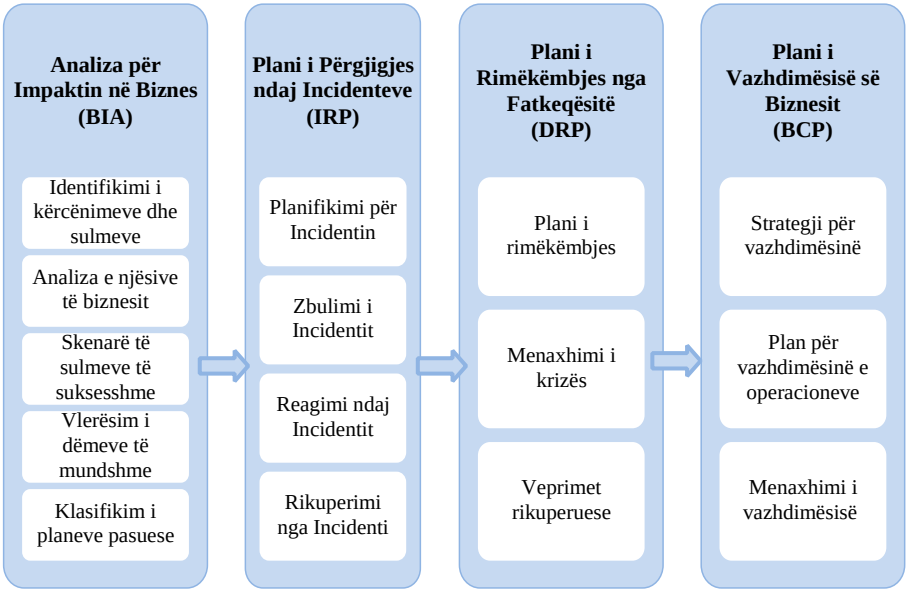


Figura 4: Hapat e trajtimit të incidenteve nga CERT

Analiza për impaktin në biznes (BIA), është faza fillestare e përgatitjes së strategjisë e cila nuk ka ndikim të drejtpërdrejtë në trajtimin e incidentit, por është shumë e rëndësishme në vlerësimin e aseteve të informacionit në një sektor. BIA investigon dhe vlerëson ndikimin që sulme të ndryshme mund të kenë në organizatë, duke supozuar se kontrollet e sigurisë janë anashkaluar, kanë dështuar, ose janë joefektive dhe sulmi ka pasur sukses.

4.5 Ndërveprimi, CERT sektorial – CERT kombëtar

Struktura e një CERT-i sektorial është e lidhur ngushtë me strukturën e organizatës/sektorit ku bën pjesë CERT-i. Një CERT sektorial efektiv është proaktiv dhe ka të paktën tre role kryesore për të ndihmuar në zgjidhjen e incidentit të sigurisë[27].

1. *Ekipi i reagimit ndaj incidenteve të sigurisë kompjuterike* (skuadra operacionale teknike) që posedon njohuritë dhe ekspertizën e nevojshme teknike për të zbutur dëmet e incidentit, kryen riparimet e nevojshme, auditime të rregullta, *patch*-e dhe trajton incidentet.

2. *Një ekspert ligjor,* i cili harton politikat e nevojshme, këshillon ekipin menaxhues për veprimet e nevojshme ligjore dhe kryen detyra të sigurimit të cilësisë, për të siguruar që pozita ligjore e një organizate të jetë e mbrojtur në rastin e një incidenti të sigurisë.

3. *Një ekspert komunikimi,* i cili ndihmon organizatën që të komunikojë siç duhet, mbi incidentin e sigurisë, me publikun dhe kanalet e tjera relevante, për të demonstruar besim edhe në momente krize, si dhe për të lehtësuar komunikimin e hapur dhe adekuat, me qëllim mbrojtjen e reputacionit të organizatës.

Në dokumentin "Udhëzim për metodologjinë e organizimit dhe funksionimit të CSIRT-ëve në nivel kombëtar", AKCESK thekson bashkëpunimin dhe koordinimin e CERT-ëve sektorialë me CERT-ët kombëtarë, në strategjitë për mbrojtjen e infrastrukturave kritike të informacionit. Në këtë rast, CERT-ët sektorialë veprojnë më së shumti në nivel teknik/operacional ose hartojnë strategji, vetëm për sektorin për të cilin kanë përgjegjësi, ndërsa CERT-ët kombëtarë, veprojnë kryesisht në nivel strategjik/taktik, duke kryer rolin e koordinatorit dhe monitoruesit, të politikave të përgjithshme të sigurisë të zbatueshme, për të gjithë sektorët. Në raste specifike, kur cenohet një CII, CERT-i kombëtar vepron edhe në rolin e CERT-it sektorial, duke asistuar me ndihmë në trajtimin e incidenteve. Ndërmjetësimi i CERT-ëve bëhet nëpërmjet qendrave kombëtare të sigurisë së informacionit (NCSC), nëse ka.

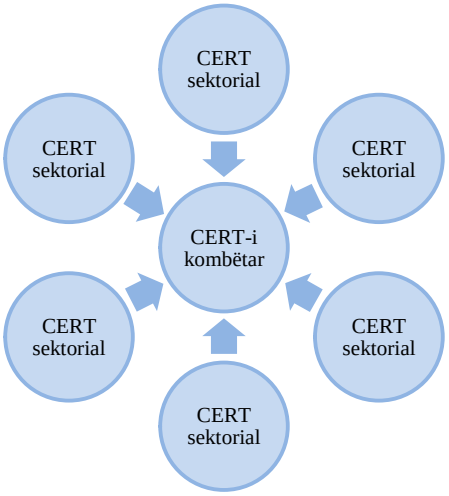


Figura 5: Diagrami e paraqitjes dhe raportimit të CERT-ëve

[27] Udhëzim për metodologjinë e organizimit dhe funksionimit të CSIRT-ve në nivel kombëtar.

Detyrat e CERT-ëve sektorialë:

1. monitoron sistemet e infrastrukturave kritike dhe/apo të rëndësishme të informacionit mbi incidente dhe/apo sulme të mundshme kibernetike;

2. siguron *back up* të të dhënave të sistemeve që disponon;

3. kontrollon dhe menaxhon incidentet kibernetike;

4. identifikon dhe kategorizon incidentet kibernetike;

5. vlerëson shtrirjen e incidentit dhe dëmin e shkaktuar;

6. heton në kohë dhe vlerëson ndikimin e incidentit;

7. njofton në kohë për incidentet, që kanë ndikim tek administratorët e operatorët e CII;

8. siguron analizë dinamike të rrezikut dhe incidentit dhe realizon kontroll për përmbajtjen e tij;

9. mban dhe ruan kronologjinë e të gjitha provave të incidentit, sipas legjislacionit në fuqi për ruajtjen e konfidencialitetit;

10. njofton CERT-in kombëtar/shtetëror menjëherë pasi identifikon incidentin;

11. ndjek me rigorozitet masat paralajmëruese të CERT-it kombëtar dhe/ose njofton NCSC në rastin e zgjidhjes së shpejtë të incidentit;

12. përgatit dhe dërgon pranë CERT-it kombëtar raportet e incidenteve, sipas formatit të miratuar nga NCSC;

13. parandalon incidente të ngjashme në të ardhmen duke marrë masa parandaluese.

14. rikuperon të dhënat dhe kthen në normalitet sistemin e prekur brenda kohës së përcaktuar sipas rregullores për klasifikimin e incidentit, të miratuar nga AKCESK;

15. duhet të sigurojë rritjen e kapaciteteve të stafit, nëpërmjet trajnimeve dhe certifikimeve periodike.

Detyrat e CERT-it kombëtar:

1. CERT-i kombëtar organizon dhe koordinon punën me të gjithë operatorët e infrastrukturave kritike të informacionit;

2. CERT-i kombëtar mbledh në mënyrë periodike CERT-ët sektorialë, me qëllim evidentimin e problematikave të ndryshme të fushës dhe rritjen e bashkëpunimit;

3. menaxhon dhe trajton çdo kërkesë të paraqitur nga CERT-ët sektorialë në lidhje me incidentet kibernetike të mundshme;

4. jep asistencë në kohë reale pranë CERT-ëve sektorialë, sipas kërkesave të tyre;

5. siguron paralajmërim të hershëm dhe shpërndan informacionin e nevojshëm për marrjen e masave parandaluese, tek operatorët në lidhje me rreziqet dhe incidentet kibernetike;

6. kërkon raporte të detajuara nga CERT-ët sektorialë, për çdo procedurë incidenti kibernetik;

7. përveç rolit si CERT-i kombëtar, luan edhe rolin e CERT-it sektorial në rastin e disponimit të infrastrukturave kritike të informacionit;

8. promovon dhe miraton standarde për procedurat e trajtimit të incidenteve dhe masat për parandalimin e tyre;

9. zhvillon dhe përditëson skemën e klasifikimit të incidenteve;

10. publikon statistika vjetore të incidenteve të raportuara;

11. NCSC monitoron përmbushjen e detyrave të CERT-ëve sektorialë të përcaktuara në këtë udhëzim;

12. organizon dhe koordinon trajnime kualifikuese, periodike për rritjen e

kapaciteteve të ekipeve të CERT-ëve, në fushën e sigurisë kibernetike.

CERT-i kombëtar, në bashkëpunim edhe me organizmat ndërkombëtarë, organizon stërvitje periodike, që simulon një incident të sigurisë kibernetike, me qëllim testimin dhe përditësimin e aftësive mbrojtëse të sistemeve si dhe trajnimin e punonjësve të CERT-it, për menaxhim sa me profesional të incidenteve kibernetike. Në përfundim të stërvitjes, përgjegjësi/punonjësi pjesëmarrës i CERT-it përgatit një raport të shkurtër për administratorin e operatorëve CII mbi përfitimet e marra nga stërvitja.

Në Shqipëri, Autoriteti Përgjegjës për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK) vepron në cilësinë e CSIRT-it kombëtar[28]. Autoriteti ka këto kompetenca në fushën e sigurisë kibernetike:

a) përcakton masat e sigurisë kibernetike;

b) vepron si pikë qendrore kontakti në nivel kombëtar, për operatorët përgjegjës në fushën e sigurisë kibernetike dhe bashkërendon punën, për zgjidhjen e incidenteve të sigurisë kibernetike;

c) administron raportet e incidenteve në fushën e sigurisë kibernetike dhe siguron ruajtjen e regjistrimin e tyre;

d) siguron ndihmë dhe mbështetje metodike, për operatorët përgjegjës në fushën e sigurisë kibernetike;

e) kryen analiza për dobësitë e konstatuara në fushën e sigurisë në internet;

f) kryen aktivitete ndërgjegjësimi dhe edukimi në fushën e sigurisë kibernetike.

Autoriteti koordinon veprimtaritë e tij me institucionet e sigurisë dhe të mbrojtjes, dhe bashkëpunon me CSIRT-et sektoriale dhe autoritetet ndërkombëtare, në fushën e sigurisë kibernetike, nëpërmjet marrëveshjeve të përbashkëta, në përputhje me legjislacionin në fuqi. Ekipet e përgjigjes ndaj incidenteve të sigurisë kompjuterike (CSIRT) përbëhen nga specialistë të fushës së sigurisë kompjuterike, pranë çdo operatori që administron infrastrukturën kritike të informacionit.

Operatorët e infrastrukturës kritike të informacionit janë të detyruar të zbatojnë masat e sigurisë, si dhe të dokumentojnë zbatimin e tyre.

5. Konkluzione dhe rekomandime

5.1 Konkluzione

Sulmet në infrastrukturat kritike të informacionit, në rang vendi, mund të kenë pasoja të rënda në funksionalitetin e tyre, duke shkaktuar edhe humbje të mëdha financiare, prandaj lind nevoja që së pari ato të identifikohen e më pas, të merren masa të forta sigurie, për ta mbajtur në nivel sa më të lartë sigurinë e këtyre infrastrukturave jetike, për funksionimin e shoqërisë. Në Shqipëri lista e CII-ve mund të përditësohet të paktën një herë në 2 vjet, me vendim të Këshillit të Ministrave. Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK) monitoron zbatimin e masave të sigurisë nga operatorët e CII-ve.

Në këtë punim argumentohet rëndësia e krijimit të skuadrave CERT sektoriale dhe kombëtare, si një ndër përpjekjet kryesore në kuadër të strategjive për mbrojtjen e infrastrukturave kritike të informacionit. Skuadrat CERT identifikojnë operacionet kritike të sektorëve, kërcënimet e mundshme kibernetike dhe hartojnë plane për trajtimin e incidenteve dhe rimëkëmbjen e sistemeve kritike në raste sulmesh. Në

[28] Ligj nr. 2/2017, datë 26.1.2017, "Për sigurinë kibernetike".

Shqipëri, AKCESK vepron në cilësinë e CERT-it kombëtar.

Punimi është bazuar mbi rregullore, vendime e udhëzues të miratuar në nivel kombëtar e sektorial, çka thekson rëndësinë e kuadrit ligjor si një bazë për mbrojtjen e infrastrukturave kritike të informacionit. Në Shqipëri, ky objektiv është realizuar me hyrjen në fuqi të ligjit "Për sigurinë kibernetike". Gjithashtu trajnimi dhe edukimi i personelit që përdor dhe administron CII-të, është një faktor kyç për parandalimin e incidenteve kibernetike.

5.2 Rekomandime

Bazuar në faktet e përmendura më sipër, për mbrojtjen e infrastrukturave kritike të informacionit nevojitet të ndërmerren disa hapa, në nivel kombëtar dhe europian, si më poshtë:

- metodologji konsistente për të identifikuar CII-të kombëtare;
- zhvillimi i procedurave të unifikuara për zbulimin e cenueshmërisë;
- zhvillimi i metodologjive për adresimin e rrezikut, ose adoptimi i metodologjive ekzistuese;
- krijimi i një sistemi alarmi dhe trajtimi kombëtar në rast incidentesh;
- krijimi i një manuali me masa për mbrojtjen e infrastrukturave kritike të informacionit;
- zhvillimi i një sistemi europian trajnimi dhe edukimi.

Bibliografia

1. African Union, *African Union Convention on Cyber Security and Personal Data Protection*, LC12490, 27th June2014.
   On-line:
   http://pages.au.int/sites/default/files/en_AU%20Convention%20on% 20CyberSecurity%20Pers% 20Data%20 Protec%20AUCyC%20adopted% 20Malabo.pdf
2. AKCESK, *Metodologji për identifikimin dhe klasifikimin e infrastrukturave kritike dhe infrastrukturave të rëndësishme të informacionit*.
   On-line: http://www.cesk.gov.al/urdher/infrastruktura.pdf
3. AKCESK, *Udhëzim për Metodologjinë e Organizimit dhe Funksionimit të CSIRT-ëve në Nivel Kombëtar*.
   On-line:
   http://www.cesk.gov.al/legjislacioni/Udh%C3%ABzim% 20p%C3% ABr% 20Metodologjin%C3% AB%20% 20e%20pun% C3 %ABs,%20 det yrat%20q %C3%AB%20 duhet%20t% C3%AB% 20zbatojn%C3% AB%20CS IRT-et%20n%C3% AB%20nivel%20Komb% C3%ABtar.pdf
4. CIPedia©: *A common international reference point for CIP and CIIP concepts and definitions*. On-line: http://www.cipedia.eu
   https://publicwiki-01.fraunhofer. de/CIPedia/index.php/CIPedia%C2%A9_Main_Page
5. CSIRT Maturity Kit: *A step-by-step guide towards enhancing CSIRT Maturity*, NCSC, The Hague, Netherlands, 2015. On-line: https://check.ncsc.nl/static/ CSIRT_MK_guide.pdf
6. Commission of The European Communities, 17 November 2005, *Green Paper on a European Programme for Critical Infrastructure Protection*.
   https://eur-lex.europa.eu/legalcontent/EN/TXT/HTML/?uri=CELEX:52005DC0576&from=BG
7. Cyber Security in the UK, Postnote Number 389, September 201.
   On-line: http:// www.parliament.uk/documents/post/postpn389_cyber-security-in-the-UK.pdf
8. ENISA, *Methodologies for the identification of Critical Information Infrastructure assets and services*, December 2014.
   On-line:https://www.enisa.europa.eu/publications/methodologies-for-the-identificationof-ciis
9. ENISA, *Baseline capabilities of national/governmental CERTs, Part 2: Policy Recommendations*. On-line: https://www.enisa.europa.eu/publications/baseline-capabilities-of-national-governmental-certs-policyrecommendations/at_download/fullReport

10. ITU *Security in Telecommunications and Information Technology: An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications*, ITU-T, Geneva (2012) - ITU-T X.1205. On-line: http://www. itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx
11. GFCE-Meridian, *Good Practice Guide on Critical Information Infrastructure Protection-for governmental policy-makers.* On-line: https://www.meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf
12. G8, *G8 Principles for Protecting Critical Information Infrastructure*s, 2003. Online: http://www.cybersecuritycooperation.org/documents/G8_CIIP_Principles.pdf
13. LigjNr. 2/2017, date 26.012017, "*Për sigurinë kibernetike*". On-line: http://www.cesk.gov.al/wpcontent/uploads /2016/04/Ligji%20_ Per_Sigurine_ Kibernetike_Nr_ 2_Date_26.1.2017.pdf
14. Meridian Process website, https://www.meridianprocess.org Nickolov E, *Critical Information Infrastructure Protection: Analysis, Evaluation and Expectation*s. On-line:http://www.comw.org/tct/fulltext/05nickolov.pdf
15. OECD ICCP Committee and the Working Party on Information Security and Privacy, OECD *Recommendation on the Protection of Critical Information Infrastructure*s [C(2008)35], 2008, OECD. Online: http://www.oecd.org/ sti/40825404.pdf
16. S. Bruno and M. Dunn, *Critical Information Infrastructure Protection: An Inventory of Protection Policies in Eight Countries, ETH*, Zürich, Switzerland, 2002. On-line: http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-forsecuritiesstudies/pdfs/CIIP_Handbook_2002.pdf
17. Victorian Government CIO Council, *Critical Information Infrastructure Risk Management,* Victoria, Australia, 2012. On-line: http://www.digital.vic.gov.au/ wp-content/uploads/2014/07/SEC-STD-02-CriticalInformation-InfrastructureRisk-Management1.pdf
18. VKM Nr. 222, date 26.04.2017, *"Për miratimin e listës së Infrastrukturave Kritike të Informacionit dhe të listës së Infrastrukturave të Rëndësishme të Informacionit"*.On-line: http://www.akce.gov.al/wpcontent/uploads/2016/04/vkm_infrastrukturat.pdf
19. Usmani KA, *Incident response and its role in protecting critical infrastructure*. On-line: http://certmu.govmu.org/English/Documents/tc/CERT-MU%20Presentation.pdf
20. Wenger A, Metsger J, Dunn M, International CIIP Handbook – *Critical Information Infrastructure Protection.* On-line: https://www. emsec. rub.de /media/crypto/attachments/files /2011/03/ciip_handbook _2004_ethz.pdf
21. Wolfpack Information Risk, 2016, South Africa – *Critical Information Infrastructure Protection Report.* On-line: https://www.wolfpackrisk.com/assets/docs/ciip_full_report_final.pdf
22. Whitman ME, Mattord HJ, 2012, *Principles of Information Security, 4th edition*. On-line: http://bedfordcomputing.co.uk/learning/wp-content/uploads/2016/08/Principles-of-Information-Security-4th-ed.-Michael-E.-Whitman.pdf


AKADEMIA E SIGURISË
AS
1971

Krimi kompjuterik dhe kërcënimet kibernetike, cenojnë sigurinë kombëtare

■**Dr. Bajram IBRAJ**
Drejtor i komanduar/Rektor
Kolegji ISPE, Prishtinë
bajramibraj@yahoo.com

Abstrakt

Bota ka arritur në një zhvillim shumë të shpejtë të komunikimit masiv në hapësirën kibernetike (virtuale), si rezultat i zhvillimit të shpejtë që ka sjellë teknologjia. Krimet kompjuterike janë evidentuar në ditët e sotme si format më të reja e nga më të përhapurat të kriminalitetit. Kjo formë e re e krimit është e vështirë për t'u dokumentuar dhe për t'u hetuar, dhe si rrjedhojë, shkalla e zbulueshmërisë dhe e ndëshkueshmërisë është e ulët. Siguria kibernetike është një ndër synimet strategjike dhe pjesë e rëndësishme e sigurisë kombëtare e Shqipërisë. Studimi synon të trajtojë aspektin ligjor, procedurën penale të hetimit dhe gjykimit të krimit kompjuterik, evidentimin e problematikave dhe sfidave kryesore në luftimin e krimit kibernetik në Shqipëri, format e krimeve kompjuterike e kërcënimeve kibernetike dhe cenimet e sigurisë kombëtare. Modeli analitik dhe metodologjia e këtij studimi, janë në përputhje të plotë me qëllimin përfundimtar të kërkimit. Studimi gërsheton dimensione teorike, juridike e profesionale, dhe metodologjia e përdorur për t'i dhënë përgjigje pyetjes kërkimore e për të përmbushur qëllimin e studimit, është metodologjia analitike e bazuar te Shqipëria, duke kombinuar qasjen cilësore me atë sasiore. Modeli i hulumtimit mbi të cilin mbështetet studimi, është analiza teorike dhe krahasuese, e fokusuar në kontekstin rajonal, te Shqipëria. Ky studim, nëpërmjet analizimit dhe ballafaqimit të literaturës, aspekteve ligjore e të dhënave statistikore, strategjive kombëtare të sigurisë kibernetike dhe sigurisë kombëtare, synon të rrisë ndërgjegjësimin e institucioneve shtetërore mbi rëndësinë e mbrojtjes së sigurisë kombëtare të shtetit dhe shtetasve shqiptarë, nga rreziqet që shfaq krimi kibernetik. Ai arrin të gjejë disa aspekte kryesore të fushës së krimeve kibernetike, si dhe nxjerrjen e përfundimeve dhe rekomandimeve, mbi masat që duhen marrë për një luftim më efikas të kriminalitetit kibernetik në Shqipëri.

Fjalëkyçe:
hapësira kibernetike, krimi kompjuterik, kërcënimet kompjuterike, siguria kombëtare, strategjia e krimit kibernetik.

1. Hyrje

Studimi është i fokusuar te krimet kompjuterike, kërcënimet kibernetike dhe siguria kombëtare. Studimi nëpërmjet pyetjes kërkimore dhe hipotezës synon të provojë gjendjen e aspekteve ligjore, të ndjekjes penale të hetimit të krimeve kompjuterike dhe kërcënimeve kibernetike, si dhe, të ndikimit të tyre në sigurinë kombëtare. Objektivat kryesore të studimit janë fokusuar në identifikimin dhe analizën e këtyre aspekteve: zhvillimi i hapësirës kibernetike, dhe ndikimi i saj në kryerjen e krimeve kompjuterike; vështrim i përgjithshëm mbi kuptimin e krimit kibernetik; mënyrat e shfrytëzimit të kompjuterit si mjet për kryerjen e krimit, baza ligjore dhe ndryshimet e bëra në fushën e krimit kibernetik; procedura penale e hetimit dhe gjykimit të krimit kibernetik; parandalimi dhe goditja e krimit të organizuar kibernetik në Shqipëri, për periudhën 2008-2015; dhe, krimi kibernetik dhe kërcënimet kibernetike si cenim për sigurinë kombëtare. Studimi është bazuar në metoda cilësore, të cilat mbështeten në literaturën e huaj dhe atë shqiptare, dokumente të rëndësishme ku përfshihen aktet ligjore në fushën kibernetike, si: *Konventa për Krimin Kibernetik*; *Strategjia Kombëtare e Sigurisë së Republikës së Shqipërisë*, 2014; *Dokumenti i Politikave për Sigurinë Kibernetike*, 2015-2017; statistikat për veprat penale të krimit të organizuar, terrorizmit dhe korrupsionit dhe krimeve kompjuterike në vitet 2008-2015; libra, etj.

Pyetja kërkimore bazë që ngre studimi është: Cilat janë veprimtaritë kriminale, të organizuara, në fushën e krimeve kompjuterike dhe kibernetike, dhe cili është, niveli i tyre në raport me veprimtaritë e tjera kriminale të organizuara, si dhe, ndikimi i tyre në sigurinë kombëtare. Studimi synon t'i japë përgjigje kësaj hipoteze: siguria kombëtare mbetet e kushtëzuar nga parandalimi, goditja dhe lufta kundër krimit kompjuterik dhe kërcënimeve kibernetike.

2. Zhvillimi i hapësirës kibernetike dhe ndikimi i tyre për kryerjen e krimeve kompjuterike

Bota ka arritur në një zhvillim shumë të shpejtë të komunikimit masiv në hapësirën kibernetike (virtuale), si rezultat i zhvillimit të shpejtë që ka sjellë teknologjia. Me zhvillimet e shpejta të teknologjisë së informacionit dhe komunikimit, me shtrirjen e përdorimit të saj pothuajse në të gjitha fushat e veprimtarisë së shoqërisë, bëhet evidente kërkesa për shërbime të sigurta dhe të besueshme[1]. Sipas Statistikave Botërore të Internetit (*Internet World Stats*) për popullsinë botërore 7 634 758 428 banorë, me datën 31 dhjetor 2017 janë evidentuar 4 156 932 140 përdorues të internetit në botë, ose 54.4 % e popullsisë botërore, nga të cilat 704,833,752 përdorues të internetit në Europë ose 85.2 %[2]. Ndërkohë, në vendet e Bashkimit Evropian për çdo 100 banorë, 68 janë shfrytëzues të internetit, në një kohë kur në Ballkan ky tregues është shumë më i ulët (50 nga 100 banorë)[3].

Numri i përdoruesve të internetit është një tregues shumë i rëndësishëm sepse tregon popullaritetin dhe përdorimin e teknologjisë në një vend, si dhe shkëmbimin e informacionit në nivel vendi. Kështu, përqindja e përdoruesve të internetit në Shqipëri, në vitin 2000 ka qenë 0,1%, 2001-03%, 2002-04%, 2003-1% për të vijuar me vitin 2004-2.4%, 2005-6%, 2006-9.6%, 2007 -15%, 2008 -23.9%, 2009- 41.2%, 2010-43.5%, (ose 1.34 milion), 2011-49%, 2012-54.7%, 2013-57.2%, 2014-60.1%, 2015-62%, 2016-62.8%[4]. Ndërsa, sipas studimit të botuar nga Universiteti i Oksfordit, Shqipëria, renditet në vendet ku interneti përdoret nga 60-80 % të popullsisë[5]. Përdoruesit e internetit në Shqipëri në muajin korrik 2016 janë evidentuar gjithsej: 2 016 516 persona ose 66.4% e popullsisë[6]. Pra, për 17 vjet përqindja e përdoruesve të internetit është rritur në 66.4%. Shqipëria krahasuar me popullsinë botërore është 12% mbi mesataren e përdorimit të internetit, ndërsa me vendet e Bashkimit Evropian është 1.6% nën mesataren e përdorimit të internetit. Shënim: (Shifrat për Shqipërinë janë evidentuar deri në muajin korrik 2016, ndërsa për vendet e Botës e BE-së deri me 31 dhjetor 2017). Ndërsa, "Penetrimi i Internetit në Kosovë është 76.6%, shkallë kjo, shumë e ngjashme me mesataren e Bashkimit Evropian, derisa edhe sjelljet e qytetarëve të Kosovës në Internet duket të jenë të ngjashme me trendet globale[7].

Sipas të dhënave të publikuara nga Bashkimi Ndërkombëtar i Telekomunikacionit, penetrimi i Internetit në Shqipëri, në dhjetë vitet e fundit, është rritur nga 0.97%, në vitin 2003, në mbi 60%, në vitin 2013[8]. Sipas *Gartner Inc.*,deri më 2020 do të ketë afërsisht 26 miliardë pajisje në Internet. Me këtë përdorim të madh të Internetit, si platformë kryesore e punës, shkencës dhe komunikimit social të qytetarit modern, siguria dhe privatësia e tij kthehen në brenga kryesore[9]. Por, krahas këtij zhvillimi të

[1] Vendim nr. 973, datë 2.12.2015,"Për miratimin e dokumentit të politikave për sigurinë kibernetike 2015 - 2017".
[2] https://www.internetworldstats.com/stats.htm,/aksesuar me 14 korrik 2018.
[3] http://open.data.al/en/lajme/lajm/id/214/Number-of-internet-users-in-Albania,/aksesuar me 14 korrik 2018.
[4] http://open.data.al/en/lajme/lajm/id/214/Number-of-internet-users-in-Albania,/aksesuar me 14 korrik 2018.
[5] http://www.balkaneu.com/albania-internet-users-italy-greece-world-bank,/aksesuar me 14 korrik 2018.
[6] https://www.indexmundi.com/albania/internet_users.html,/aksesuar me 14 korrik 2018.
[7] Strategjia Shtetërore për Sigurinë Kibernetike dhe Plani i Veprimit,2016-2019 të Republikës së Kosovës, dhjetor 2015.
[8] Dokumenti i Politikave për Sigurinë Kibernetike 2015-2017, faqe 12.
[9] Strategjia Shtetërore për Sigurinë Kibernetike dhe Plani i Veprimit 2016-2019,të Republikës së Kosovës, dhjetor 2015.

vrullshëm të përdorimit të internetit, është treguar se ka edhe një anë të errët, ku janë evidentuar edhe rënie të lirive të së drejtave të njeriut në internet. Kështu, nga gjetjet e raportit të fundit "Liria në Internet 2017", të organizatës "Freedom House", e cila vëzhgon nivelin e demokracisë dhe lirisë në mbarë botën, për periudhën qershor 2016-maj 2017, rreth gjysma e 65 vendeve të vlerësuara, që përfaqëson rreth 87 për qind të së gjithë njerëzve me qasje në internet në mbarë globin, panë një rënie të lirive të tyre në internet[10].

Hapësira kibernetike, sot është bërë një nga sfidat më të mëdha, ligjore dhe të sigurisë. Kjo hapësirë kibernetike, duke shfrytëzuar mundësitë që ka krijuar ky mjedis i ri, për sjellje kriminale gjatë përdorimit të kompjuterëve, dhe celularëve përmes internetit, ka nxitur edhe format e metodat e reja të krimit kompjuterik e të kërcënimit kibernetik, si dhe, ka çuar në rritjen e ndjeshme të kriminalitetit, e të kërcënimeve kombëtare dhe ndërkombëtare. Sot, ne jemi në një epokë globalizimi, dhe pas energjisë, siguria kibernetike është bërë një prej synimeve kryesore strategjike të secilit vend.

Krimi kompjuterik, edhe në botë, konsiderohet si kriminalitet i organizuar, i evidentuar vetëm në gjysmën e dytë të shekullit të kaluar, edhe sepse pas futjes në përdorim të kompjuterëve, dhe aplikimit të gjerë të tyre në fushat e ndryshme të jetës,"*filluan keqpërdorimet e para me ndihmën e kompjuterëve*"[11]. Statistikat e para mbi kriminalitetin kompjuterik janë mbajtur që nga viti 1958. Këto të dhëna janë përpiluar nga Instituti i Stanfordit (IKS). Rasti i parë, i paraqitur, i keqpërdorimit kompjuterik, është shënuar në vitin 1958, ndërsa në vitin 1966, është shënuar rasti i parë që kompjuteri është shfrytëzuar si mjet për kryerjen e vjedhjes në një bankë në Minesota (SHBA)[12].

M. E. Kabay, në librin "*A Brief History of Computer Crime"* shprehet se: "Dëmtimi fizik i sistemeve kompjuterike ishte një kërcënim i shquar deri në vitet '80; Programuesit në vitet 1980 filluan të shkruanin softuer të dëmshëm, duke përfshirë vetëpërsëritje të programeve, për të ndërhyrë në kompjuterët personalë; në vitet 1990 përparoi krimi financiar, duke përdorur depërtimin, dhe, përmbysja e kompjuterëve të sistemeve u rrit. Ndërsa, aplikacionet e paligjshme të postës elektronike u rritën me shpejtësi nga mesi i viteve 1990, duke gjeneruar *torrents* dhe "e-mail"-ë të pakërkuar, tregtie dhe mashtrues[13].

Zhvillimi i madh dhe i shpejtë në fushën teknologjike në botë, në rreth 50 vitet e fundit, u shoqërua edhe me një përdorim masiv të përdoruesve, dhe kjo solli edhe zhvillimin e shpejtë të krimit kompjuterik, apo krimit kibernetik, si dhe të kërcënimeve kibernetike. Por, gjithashtu, krimi kompjuterik apo krimi kibernetik, është një formë e veçantë e krimit të organizuar dhe i përket kryesisht kriminalitetit të organizuar, veçanërisht krimit të "*jakave të bardha*". Duke zhvilluar shumë krimin e organizuar kibernetik, nëpërmjet përdorimit të kompjuterëve, "*sot sistemet kompjuterike ofrojnë mundësi të reja dhe më të sofistikuara për shkeljen e ligjit*"[14]. Mirëpo, "Strategjia ndërsektoriale për shoqërinë e informacionit 2008-2013" (SNSHI) e miratuar me VKM nr. 59 datë 21.1.2009, përveçse përbën dokumentin strategjik që përcaktonte drejtimet

[10] https://freedomhouse.org/.https://www.zeriamerikes.com/a/4114767.html,/aksesuar me 14 korrik 2018.
[11] D. Krapac: Kompjutorski kriminalitet, Zagreb, 1992, faqe 15, sipas D.Dragiçeviç, cituar po aty. (Marrë nga Dr.sc.Veton Vula "Kriminaliteti i Organizuar", Prishtinë, 2013, faqe 137).
[12] J. Sumida: Computer crime, marrë nga internet: http:www.webnerds.com/ computercrime/main.html (Marrë nga Dr.sc.Veton Vula "Kriminaliteti i Organizuar", Prishtinë, 2013, faqe 137).
[13] M. E. Kabay,"*A Brief History of Computer Crime"*,botuar në vitin 2008, faqe 3-4.
[14] Dr. sc. Veton Vula "Kriminaliteti i Organizuar", Prishtinë, 2013, faqe 138.

kryesore dhe objektivat e zhvillimit në fushën e shoqërisë së informacionit, për periudhën 2008-2013, ishte edhe dokumenti i vetëm, ku përmendej shkurtimisht *siguria kibernetike,* si një nga fushat që duhej konsideruar me prioritet për shkak të vizionit të qeverisë shqiptare, për të rritur e zhvilluar qeverisjen përmes ofrimit të e-shërbimeve[15].

3. Vështrim i përgjithshëm mbi kuptimin e krimit kibernetik dhe mënyrat e shfrytëzimit të kompjuterit si mjet për kryerjen e krimit.

Në nivel Evropian dhe ndërkombëtar, nuk ka ndonjë përkufizim të harmonizuar të termave dhe nocioneve "kibernetikë" dhe "siguri kibernetike". Kuptimi i sigurisë kibernetike dhe termave të tjerë të rëndësishëm dallojnë në shtete të ndryshme. Ndërkohë, akoma nuk ekziston një përkufizim ndërkombëtar i njohur dhe pranuar për krimin e organizuar kibernetik. Megjithatë, autorë të ndryshëm, kanë dhënë përkufizime të ndryshme. Kështu, Interpoli, në vitin 1981, ka dhënë këtë përkufizim: "Kriminalitet kompjuterik, është çdo akt ilegal, ku për kryerjen e suksesshme të tij, hetimin, ndjekjen ose dënimin, nevojitet njohje esenciale e teknologjisë kompjuterike"[16]. Ndërsa, Policia Federale Gjermane, në vitin 1983, jep këtë përkufizim: "Kriminaliteti kompjuterik, përmban mashtrimin kompjuterik, spiunazhin kompjuterik si dhe keqpërdorimin kompjuterik"[17].

Dokumenti i Politikave për Sigurinë Kibernetike 2015-2017, të Republikës së Shqipërisë, përcakton përkufizimet e mëposhtme:

Krim kibernetik, konsiderohet ndërhyrja e paautorizuar, drejt dhe/ose, përmes përdorimit të TIK, penalizimi për të cilin rregullohet në Kodin Penal të Republikës së Shqipërisë[18].

Kërcënim/sulm kibernetik, konsiderohet çdo përpjekje e drejtuar/qëllimshme për të marrë akses, manipuluar, ndërhyrë ose dëmtuar integritetin, konfidencialitetin, sigurinë, dhe/ose, disponibilitetin e të dhënave, të një aplikimi ose së të dhënave të sistemit kompjuterik, pa pasur autoritet ligjor për ta bërë këtë.

Strategjia Shtetërore për Sigurinë Kibernetike dhe Plani i Veprimit, 2016–2019, i Republikës së Kosovës, përcakton përkufizimet e mëposhtme:

Kibernetika (cyber) përkufizohet si: *"çdo gjë që ka të bëjë me, apo që përfshin, kompjuterët apo rrjetet kompjuterike (si Interneti)".* Sipas Organizatës Ndërkombëtare për Standardizim (ISO), "cyber" është *"mjedis kompleks që lind nga ndërveprimi i njerëzve, i programeve dhe i shërbimeve në Internet, me anë të pajisjeve e rrjeteve teknologjike që lidhen në të, që nuk ekziston në formë fizike".*

Siguria kibernetike. Në Strategjinë e Sigurisë Kibernetike të Bashkimit Evropian

[15] Strategjia Ndërsektoriale për Shoqërinë e Informacionit, 2008-2013 (SNSHI) e miratuar me VKM nr.59 datë 21.1.2009, faqe 11.

[16] Tenhuen M."Combating Computer Crime", Interpol Review, nr. 147, 1989.

[17] Mohr K. Polizeiliches Lagebild der Computer Kriminalitet "Die Policai no.2 Bremen, 1987, faqe 41.

[18] Ligj nr.9859, datë 21.1.2008 "Për disa shtesa dhe ndryshime në ligjin nr.7895, datë 27.1.1995 "Kodi penal i Republikës së Shqipërisë", të ndryshuar.
Ligj nr.10023, datë 27.11.2008 "Për disa shtesa dhe ndryshime në ligjin nr.7895,datë 27.1.1995 "Kodi penal i Republikës së Shqipërisë", të ndryshuar.
Ligj nr.10054, datë 29.12.2008 "Për disa shtesa dhe ndryshime në ligjin nr.7905,datë 21.3.1995 "Kodi i procedurës penale i Republikës së Shqipërisë", të ndryshuar.
Ligj nr. 144/2013"Për disa shtesa dhe ndryshime në ligjin nr.7895,datë 27.1.1995 "Kodi Penal i Republikës së Shqipërisë", të ndryshuar.

(Hapësirë kibernetike e hapur, e sigurt dhe e mbrojtur)[19], *"siguria kibernetike, përgjithësisht iu referohet masave mbrojtëse, dhe veprimeve që mund të ndërmerren për të mbrojtur domenin kibernetik, edhe në fushën civile edhe atë ushtarake, nga ato kërcënime që ndërlidhen me to, apo që mund të dëmtojnë rrjetet dhe infrastrukturën komunikuese të ndërvarur. Siguria kibernetike përpiqet të ruajë disponueshmërinë dhe integritetin e rrjeteve dhe infrastrukturës, si dhe, fshehtësinë e informatave që mbahen në to"*. Organizata Ndërkombëtare e Standardizimit (ISO), përkufizon sigurinë kibernetike si: *"ruajtje të konfidencialitetit, integritetit dhe disponueshmërisë së informatave në hapësirën kibernetike"*.

Kriminaliteti kibernetik. Sipas Strategjisë së Sigurisë Kibernetike të Bashkimit Evropian, *"kriminaliteti kibernetik i referohet përgjithësisht një spektri të gjerë veprimtarish kriminale të ndryshme, ku kompjuterët dhe sistemet informative angazhohen ose si vegël primare ose si shënjestër primare.* Krimi kibernetik, *përfshin veprat penale tradicionale (p.sh. mashtrimi, falsifikimi dhe thyerja e identitetit), veprat në lidhje me përmbajtjen (p.sh. shpërndarja në Internet e pornografisë së fëmijëve, apo nxitja e urrejtjes racore), si dhe, veprat që janë unike, për kompjuterë dhe sisteme informative (p.sh. sulmet ndaj sistemeve informative, mohimi i shërbimit dhe "maluer" (malware))"*.

Kërcënimet kibernetike, vijnë nga mundësitë dhe qëllimet e një armiku, që fillon një sulm kibernetik mbi Sistemet e Komunikimit dhe të Informacionit. Ekzistojnë pesë lloje sulmesh kibernetike, të motivuara nga:

1. *Hakmarrja, kurioziteti*, të kryera nga stafi brenda organizatës, ose ish-të punësuar (të larguar nga puna), dhe nga të ashtuquajtur "script-kiddies" (të rinj që përdorin *skripte* të gatshme për sulme).

2. *Përfitime monetare:* të kryera nga krimi i organizuar.

3. *Spiunimi, aktivizmi:* sulmet kibernetike që kanë të bëjnë me ndërhyrjen e pavërejtur të një pale të tretë brenda Sistemeve të Komunikimit dhe të Informacionit, duke lexuar, ndryshuar, shlyer apo edhe shtuar informata. Ndërhyrjet e tilla mund të përdoren edhe për të keqpërdorur sistemet e sulmuara të komunikimit dhe të informacionit, dhe për të sulmuar sisteme të tjera.

4. Siguria kombëtare: të kryera nga aktorë të sponsorizuar shtetërorë.

5. *Terrorizmi kibernetik*: Ka të bëjë me përpjekje me shënjestra të nivelit të lartë, që bëhen me qëllime terroriste, i cili është një kërcënim në zhvillim e sipër dhe ka potencial të shkaktojë dëme të mëdha. Përderisa terrorizmi shpesh ndërlidhet me humbjen e jetës, nuk mund t'i anashkalojmë pasojat e rëndësishme, si: frikësimi, apo shtytja, që mund të shkaktohen nga terrorizmi kibernetik[20].

Mënyrat e shfrytëzimit të kompjuterëve janë të shumta, ndërkohë që edhe mjetet për kryerjen e krimit dhe krimit të organizuar janë mjaft të gjera. Sipas autorit A. Bequaj, në punimin e tij, "How to prevent computer crime", shfrytëzimi i kompjuterit në fushën kriminale bëhet në pesë mënyra themelore: 1. kompjuteri si objekt sulmi; 2. kompjuteri si subjekt sulmi, - mjet i kryerjes (*modus operandi*); 3. kompjuteri si mjet për planifikim, fshehje ose udhëheqje me kriminalitetin; 4. kompjuteri si simbol për mashtrim; 5. kompjuteri si mjet për ndalimin, sqarimin dhe të provuarin e veprave

[19] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52013JC0001.

[20] Strategjia Shtetërore për Sigurinë Kibernetike dhe Plani i Veprimit 2016-2019,i Republikës së Kosovës, dhjetor 2015, faqe 7-9.

penale apo veprimit kriminal[21].

4. Baza ligjore dhe ndryshimet e bëra në fushën e luftimit të krimit kompjuterik dhe kibernetik.

Republika e Shqipërisë ka ratifikuar Konventën "Për Krimin në Fushën e Kibernetikës"[22], në prill të vitit 2002, dhe legjislacioni shqiptar për implementimin e konventës, ka pësuar ndryshimin, e:

1. Kodit Penal të Republikës së Shqipërisë,[23] në drejtim të shtimit të neneve që përcaktojnë veprat penale në fushën kibernetike, lidhur me përdorimin e të miturve për prodhimin e materialeve pornografike, dhe shpërndarjen e tyre në internet;

2. Ligjit nr. 10023, datë 27.11.2008, "Për disa shtesa dhe ndryshime në ligjin nr. 7895 datë 27.01.1995 Kodi Penal i Republikës së Shqipërisë i ndryshuar", në të cilin janë parashikuar 11 vepra penale lidhur me shpërndarjen e materialeve pro gjenocidit dhe krimeve kundër njerëzimit, raciste, ksenofobe, mashtrimin kompjuterik, falsifikimin kompjuterik, ndërhyrjen në sisteme kompjuterike, keqpërdorimin e pajisjeve kompjuterike etj.;

3. Kodit të Procedurës Penale së Republikës së Shqipërisë, i cili ka pësuar ndryshime[24] në drejtim të shtimit të neneve që përcaktojnë procedura specifike për sekuestrimin dhe ruajtjen e përshpejtuar së të dhënave kompjuterike.

Krimi kompjuterik dhe kërcënimet kibernetike në Shqipëri, janë një ndër veprat penale të përcaktuara në Kodin Penal të Republikës së Shqipërisë, si dhe, një ndër veprimtaritë kriminale të organizuara vonë, sepse lidhet me zhvillimin e vonshëm të teknologjisë së kompjuterëve elektronik digjital. Duke qenë se përballja me këto krime përbënte një sfidë të re dhe të vështirë, në Strategjinë e Policisë së Shtetit 2007-2013[25], është parashikuar ngritja e një strukture të specializuar për luftën ndaj krimit kibernetik. Në departamentin kundër krimit të organizuar dhe krimeve të rënda, pranë drejtorisë kundër krimit financiar, është krijuar sektori kundër krimeve kompjuterike, i miratuar me urdhrin e Ministrit të Brendshëm nr. 372 datë 8.6.2009,[26] ndërsa me urdhrin nr. 200, datë 16.6.2010,[27] të ndryshuar, janë fuqizuar kapacitetet për hetimin e krimeve kompjuterike dhe ekzaminimin e provave kompjuterike, konkretisht në sektorin kundër

---

[21] August Bequaj"How to Prevent Computer Crime",John Walley & Sons, Inc, 1983, faqe 164; Carter L.D."Computer Crime Categories:How Techno-criminals Operate" FBI Law Enforcement Bulletin. http://www.nsi.org/Library.Compsec/crimecom.html cituar sipas S.Petroviq, faqe 36-37,(marrë nga https: // arditmuca. files. wordpress.com/2010/07/kriminaliteti-kompjuterik.pdf).

[22] Ligj nr.8888 datë 25.04.2002,"Për Ratifikimin e Konventës për Krimin Kibernetik",fletore zyrtare nr.18 datë 17.05.2002, faqe 553.
Ligj nr.9262 i datës 29.07.2004 "Për Ratifikimin e Protokollit shtesë të Konventës për krimin kibernetik, për penalizimin e akteve me natyrë raciste dhe ksenofobe të kryera nëpërmjet sistemeve kompjuterike".

[23] Ligj nr. 9859 datë 21.01.2008 "Për disa shtesa dhe ndryshime në ligjin nr.7895 datë 27.01.1995 (Kodi Penal i Republikës së Shqipërisë) i ndryshuar.

[24] Ligj nr.10054 datë 29.12.2009, "Për disa shtesa e ndryshime në ligjin nr.7905 datë 21.03.1995 (Kodi i Procedurës Penale të Republikës së Shqipërisë) i ndryshuar .

[25] Vendim i Këshillit të Ministrave nr. 14 datë 9.1.2008,"Për miratimin e Strategjisë së Policisë së Shtetit 2007-2013".

[26] Urdhër nr. 372 datë 08.06.2009 i Ministrit të Brendshëm,"Për miratimin e strukturës dhe limitit të Organikës së Drejtorisë së Përgjithshme të Policisë së Shtetit".

[27] Urdhër nr. 200 datë 16.06.2010 i Ministrit të Brendshëm,"Për disa ndryshime në Urdhrin nr. 372, datë 08.06.2009, të Ministrit të Brendshëm"Për miratimin e strukturës dhe limitit të organikës së Drejtorisë së Përgjithshme të Policisë së Shtetit".

krimeve kompjuterike në Drejtorinë e Përgjithshme të Policisë së Shtetit janë 5 funksione. Gjithashtu, në të njëjtën kohë, në Institutin e Policisë Shkencore është ngritur një strukturë e policisë shkencore, e cila emërtohet, sektori i ekzaminimeve të provave kompjuterike, me 6 specialistë, e që ka për detyrë ekzaminimin e pajisjeve kompjuterike me qëllim kërkimin dhe nxjerrjen e provave kompjuterike. Ndërkohë, që përpara krijimit të kësaj strukture, çështjet në lidhje me kriminalitetin kompjuterik apo kibernetik, kryheshin nga strukturat e antikrimit,policisë kriminale dhe nga drejtoria e luftës kundër krimit të organizuar, krijuar në vitin 2004.

Kuadri ligjor që merret me sigurinë dhe krimin kibernetik në Shqipëri, përfshin gjithsej katërmbëdhjetë struktura qeveritare dhe konkretisht: Agjencia Kombëtare për Sigurinë Kompjuterike (ALCIRT); Drejtoria e Sigurimit të Informacionit të Klasifikuar (DSIK); Autoriteti Kombëtar për Certifikimin Elektronik (AKCE); Agjencia Kombëtare e Shoqërisë së Informacionit (AKSHI); Policia e Shtetit; Prokuroria e Përgjithshme; Shërbimi Informativ i Shtetit (SHISH); Ministria e Mbrojtjes; Shtabi i Përgjithshëm i Forcave të Armatosura të Republikës së Shqipërisë; Drejtoria e Shifrës (DSH); Agjencia e Inteligjencës së Mbrojtjes dhe Sigurisë (AISM); Banka e Shqipërisë (BSH); Autoriteti i Komunikimeve Elektronike dhe Postare (AKEP) dhe Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale (IDP). Por, në këtë punim, do të trajtojmë në mënyrë më specifike përgjegjësitë dhe detyrat e Sektorit kundër Krimeve Kompjuterike në Drejtorinë e Policisë së Shtetit.

4. Procedura penale e hetimit dhe gjykimit të krimit kibernetik

Në bazë të ndryshimeve të rëndësishme ligjore, sektori kundër krimeve kompjuterike në Drejtorinë e Policisë së Shtetit, policia gjyqësore, prokuroria dhe gjykata, kanë përgjegjësi dhe detyrë, ndjekjen dhe hetimin e gjykimin, e veprave penale të mëposhtme.

1. *Vepra penale në fushën e teknologjisë së informacionit janë:* mashtrimi kompjuterik (neni 143/b); falsifikimi kompjuterik (neni 186/a); hyrja e paautorizuar kompjuterike (neni 192/b); përgjimi i paligjshëm i të dhënave kompjuterike (neni 293/a); ndërhyrja në të dhënat kompjuterike (neni 293/b); ndërhyrja në sistemet kompjuterike (neni 293/c); keqpërdorimi i pajisjeve (neni 293/ç).

2. *Vepra Penale të kryera nëpërmjet sistemit kompjuterik janë***:** shpërndarja kompjuterike e materialeve pro gjenocidit dhe krime ndaj njerëzimit (neni 74/a); kanosja me motive raciste dhe ksenofobe nëpërmjet sistemit kompjuterik,(neni 84/a); shpërndarja e materialeve raciste ose ksenofobike nëpër sistemit kompjuterik, (neni 119/a); fyerja me motive raciste ose ksenofobe nëpërmjet sistemit kompjuterik, (neni 119/b); pornografia (nëpërmjet sistemit kompjuterik) (neni 117 paragrafi i dytë), neni 117, paragrafi i dytë; përdorimi i të miturit për prodhimin e materialeve pornografike, neni 74/a; shpërndarja kompjuterike e materialeve pro gjenocidit ose krimeve kundër njerëzimit, neni 84/a; kanosja me motive racizmi dhe ksenofobie nëpërmjet sistemit kompjuterik, neni 119/a; shpërndarja e materialeve raciste ose ksenofobike nëpërmjet sistemit kompjuterik, neni 119/b; fyerja me motive racizmi ose ksenofobie nëpërmjet sistemit kompjuterik, neni 143/b; mashtrimi kompjuterik, neni 186/a; falsifikimi kompjuterik, neni 192/b; hyrja e paautorizuar kompjuterike, neni 293/a; përgjimi i paligjshëm i të dhënave kompjuterike, neni 293/b; ndërhyrja në të dhënat kompjuterike, neni 293/c; ndërhyrja në sistemet kompjuterike, neni 293/ç; keqpërdorimi i pajisjeve, nëpërmjet ndryshimeve me ndryshimet e bëra në ligje të veçanta kanë krijuar bazën e

plotë procedurale e ligjore me qëllim parandalimin, zbulimin, dokumentimin dhe goditjen e veprimtarisë kriminale të organizuar në fushën kompjuterike apo krimi i organizuar kibernetik.

3. Format e krimeve kompjuterike. Format e krimeve kompjuterike janë të shumëllojshme dhe nëpërmjet tyre, krimi i organizuar nacional e transnacional, siguron qëllimin e tij: përfitimin material e financiar. Format e krimeve kompjuterike të konstatuara gjatë kësaj periudhe janë:

3.1 Mashtrimet nëpërmjet internetit. Nëpërmjet mashtrimeve, nëpërmjet internetit, sigurohet: Ndërhyrje të paligjshme në komunikimet elektronike midis dy subjekteve tregtare, për të ndryshuar destinacionin e transaksioneve bankare, me qëllim përfitimin e paligjshëm të tyre; krijimi dhe përdorimi i faqeve të internetit mashtruese, me qëllim marrjen e të dhënave personale dhe financiare të përdoruesve të internetit, për përfitim të paligjshëm, metoda "phishing"; përfitimi me mashtrim i shumave të parave, duke përdorur të dhëna kompjuterike të rreme, nëpërmjet përdorimit të faqeve të internetit mashtruese, duke u paraqitur si subjekt tregtar në një shtet të huaj; kryerja e transaksioneve të paautorizuara nga përdorues të paligjshëm, nëpërmjet vjedhjes së kredencialeve të aksesit; dërgimi i mesazheve elektronike nëpërmjet metodës "SPAM", me qëllim viktimizimin e sa më shumë përdoruesve, në skema mashtrimi si lotari fiktive, trashëgimi fiktive, etj.; krijimi i profileve mashtruese në rrjete sociale, në të cilat gjoja shiten ndeshje futbolli të paracaktuara.

3.2 Mashtrimet me karta bankare. Nëpërmjet mashtrimeve me karta bankare nga autorët e grupeve kriminale realizohet: Vjedhja apo kopjimi i të dhënave të kartave bankare nëpërmjet vendosjes së pajisjeve elektronike në ATM; përdorimi i të dhënave të kartave bankare të vjedhura, për blerjen e mallrave, produkteve apo shërbimeve në internet; përdorimi i kartave të klonuara për blerjen e mallrave, produkteve apo shërbimeve në subjekte apo qendra tregtare; përdorimi i të dhënave të kartave bankare, të vjedhura për prenotimin e biletave të udhëtimit, akomodimit në hotel, prenotimin për organizimin e ceremonive.

3.3 Falsifikimi kompjuterik. Nëpërmjet falsifikimit kompjuterik, realizohet fshirja dhe ndryshimi i dokumenteve kompjuterike, me qëllim ngritjen e të dhënave.

3.4 Ndërhyrjet e paligjshme kompjuterike. Nëpërmjet ndërhyrjes së paligjshme kompjuterike, realizohet: thyerja e paligjshme, e masave të sigurisë së llogarive, në rrjetet sociale në internet, me qëllim, kanosjen për publikim së të dhënave personale dhe shtrëngimin e poseduesit të llogarisë, për dhënien e pasurisë, në kundërshtim me vullnetin e tij; thyerja e masave të sigurisë së sistemeve, apo programeve kompjuterike, për vjedhjen e të dhënave personale dhe financiare; futja e paligjshme në faqet zyrtare të internetit, të subjekteve publike dhe private, me qëllim mosfunksionimin e tyre dhe prishjen e imazhit; hyrja e paligjshme në adresat e postës elektronike, apo profilet në rrjetet sociale të përdoruesve të internetit; dhe, thyerja e masave të sigurisë së sistemeve apo programeve kompjuterike, për vjedhjen e të dhënave personale dhe financiare.

3.5 Pornografia me të mitur në internet. Nëpërmjet pornografisë me të mitur, në internet, realizohet përdorimi i rrjeteve sociale, për të konsumuar materiale abuzive me të mitur.

3.6 Shkelje të së drejtës së autorit në internet. Nëpërmjet shkeljes të së drejtës së autorit në internet, arrihet: përdorimi i faqeve elektronike për të publikuar filma, dokumentare në shkelje të së drejtës së autorit, dhe vjedhja e programeve kompjuterike, duke i tregtuar ato si origjinale, në shkelje të së drejtës së autorit.

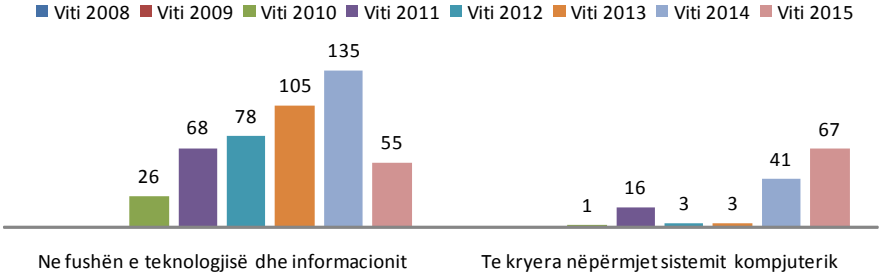
3.7 Shkelje të privatësisë, përndjekje, shpifje dhe fyerje. Nëpërmjet shkeljes të privatësisë, përndjekjes, shpifjes dhe fyerjes, realizohet: krijimi i profileve të rreme në rrjete sociale, me qëllimin për të publikuar të dhëna personale dhe private, si dhe, për të shpifur dhe fyer ndaj viktimës; dhe, përndjekja nëpërmjet teknologjisë së informacionit.

3.8 Terrorizmi kompjuterik. Përdorimi i paautorizuar dhe përhapja e informacionit të privilegjuar, dhe pastrimi i produkteve të krimit apo veprimtarisë kriminale lidhur me krimin kompjuterik.

5. Parandalimi dhe goditja e krimit të organizuar kibernetik në Shqipëri, për periudhën 2008-2015

Lufta e organizuar për parandalimin dhe goditjen e krimit të organizuar kompjuterik, apo krimit të organizuar kibernetik, fillon në çdo rast, minimalisht, kur krijohen strukturat përkatëse për parandalimin dhe luftën kundër këtij kriminaliteti. Pra, kjo luftë ka filluar pas gjysmës së dytë të vitit 2009. Siç do ta shohim edhe nga treguesit statistikorë, do të shohim se në vitet 2008 dhe 2009, shifrat e statistikave të Policisë së Shtetit, janë zero. Pra, askush nuk mund të mendojë se do të luftojë një lloj kriminaliteti të ri dhe të sofistikuar, pa ngritur, organizuar dhe funksionuar strukturat përkatëse dhe pa emëruar, trajnuar e motivuar, drejtues e punonjës të aftë me aftësi juridiko-policore dhe të përkushtuar në detyrë.

Më poshtë, paraqitet figura për krimet kibernetike në Shqipëri për periudhën 2008-2015.



Burimi: Shkresa nr. B-11/1, datë 04.03.2016 e Drejtorisë së Policisë së Shtetit, lënda, "Përgjigje Tuajës nr. B-11 Prot. datë 10.02.2016, "Informacion mbi statistikat për veprat penale të krimit të organizuar, terrorizmit dhe korrupsionit në vitet 2008-2015", drejtuar Bajram Ibraj. *Përpunim i Autorit (2016).*

Figura1. Krimet Kibernetike në Shqipëri, 2008-2015.

Në mënyrë tabelore, paraqitet figura për krimet kibernetike në Shqipëri, në fushën e teknologjisë dhe informacionit, dhe të kryera nëpërmjet sistemit kompjuterik për periudhën 2008-2015, ku evidentohen shifrat përkatëse sipas viteve. Kështu, krimet kibernetike në fushën e teknologjisë dhe informacionit, paraqiten në vitin 2010 me 26 vepra penale, në vitin 2011 me 68, në vitin 2012 me 78, në vitin 2013 me 105, në vitin 2014 me 135, dhe në vitin 2015 me 55 vepra penale. Viti 2014, ka evidentuar numrin më të lartë, me 135 vepra penale; viti 2010 me 26, dhe viti 2015 me 55 vepra penale, janë evidentuar vitet me numrin më të ulët të veprave penale. Ndërsa, vepra penale të

kryera nëpërmjet sistemit kompjuterik, janë evidentuar: në vitin 2010, 1 vepër penale; në vitin 2011, 16 vepra penale, në vitin 2012, 3 vepra penale, në vitin 2013, 3 vepra penale, në vitin 2014, 41 vepra penale dhe në vitin 2015 janë evidentuar 67 vepra penale. Viti 2015 ka evidentuar numrin më të lartë, me 67 vepra penale, dhe viti 2010, evidenton vitin me numrin më të ulët, me 1 vepër penale. Më poshtë, paraqiten veprat penale në fushën e krimit të organizuar, të evidentuara e zbuluara dhe, krahasimi me krimet kompjuterike sipas statistikave të Policisë së Shtetit, për periudhën 2008-2015.

Tabela 2. Veprat penale në fushën e krimit të organizuar të evidentuar e zbuluar dhe krahasimi me krimet kompjuterike sipas statistikave të Policisë së Shtetit, 2008-2015.

		VITI 2008		VITI 2009		VITI 2010		VITI 2011		VITI 2012		VITI 2013		VITI 2014		VITI 2015	
		Evidentuar	Zbuluar	Evidentuar	Zbuluar	Evidentuar	Zbuluar	Evidentuar	Zbuluar	Evidentuar	Zbuluar	Evidentuar	Zbuluar	Evidentuar	Zbuluar	Evidentuar	Zbuluar
A	Krime ne fushën e Akteve Terroriste	9	8	9	6	8	5	14	8	10	9	22	16	39	23	12	5
B	Krime ne fushën e trafiqeve te paligj.	517	500	400	392	457	440	465	462	509	506	387	371	444	433	432	364
C	Krime ne fushën e drogës	653	407	647	391	526	491	647	619	957	911	1105	1042	1243	1127	1021	975
D	Krime ekonomiko-financiare	1918	1874	1224	1191	1385	1362	1540	1497	1801	1733	2318	2262	1980	1913	2436	2326
E	Krime kundër korrupsionit	370	365	357	345	384	378	354	344	432	425	458	445	691	683	907	877
F	Krime kundër pastrimit te parasë	183	181	159	146	56	56	86	86	116	116	125	125	326	326	355	344
G	Kundër krimeve kompjuterike					27	17	84	62	81	57	108	63	176	75	122	33

Burimi: Shkresa nr. B-11/1, datë 04.3.2016 e Drejtorisë së Policisë së Shtetit, lënda, "Përgjigje Tuajës nr.B-11 Prot. datë 10.2.2016, "Informacion mbi statistikat për veprat penale të krimit të organizuar, terrorizmit dhe korrupsionit në vitet 2008-2015", drejtuar Bajram Ibraj. *Përpunim i Autorit (2016).*

Më poshtë paraqitet grafiku me të dhënat e veprimtarive kriminale të organizuara dhe krimi i organizuar kompjuterik, sipas statistikave të Policisë së Shtetit, 2008-2015.

Tabela 5. Të dhënat e krimit të organizuar kompjuterik sipas statistikave të Policisë së Shtetit për periudhën, 2008-2015.

Burimi: Shkresa nr. B-11/1, datë 4.3.2016 e Drejtorisë së Policisë së Shtetit, lënda, "Përgjigje Tuajës nr. B-11 Prot. datë 10.2.2016, "Informacion mbi statistikat për veprat penale të krimit të organizuar, terrorizmit dhe korrupsionit në vitet 2008-2015", drejtuar Bajram Ibraj. *Përpunim i Autorit (2016).*

Më poshtë paraqitet të dhënat e krimit të organizuar kompjuterik sipas statistikave të Policisë së Shtetit, 2008-2015.

Tabela 4. Të dhënat e krimit të organizuar kompjuterik sipas statistikave të Policisë së Shtetit, 2008-2015.

Viti	2008		2009		2010		2011		2012		2013		2014		2015	
	Evidentuar	Zbuluar	Evidentuar	Zbuluar	Evidentuar	Zbuluar	Evidentuar	Zbuluar	Evidentuar	Zbuluar	Evidentuar	Zbuluar	Evidentuar	Zbuluar	Evidentuar	Zbuluar
Krimi Organizuar Kompjuterik					27	17	84	62	81	57	108	63	176	75	122	33
Krimi Organizuar Kompjuterik (Zbulimi në %)						63%		74%		70.40%		58.30%		42.60%		27.00%

Burimi: Shkresa nr. B-11/1, datë 04.03.2016 e Drejtorisë së Policisë së Shtetit, lënda, "Përgjigje Tuajës nr.B-11 Prot. datë 10.2.2016, "Informacion mbi statistikat për veprat penale të krimit të organizuar, terrorizmit dhe korrupsionit në vitet 2008-2015", drejtuar Bajram Ibraj. *Përpunim i Autorit (2016).*

Në mënyrë tabelore paraqiten të dhënat e mëposhtme: krimi i organizuar kompjuterik gjatë vitit 2008 dhe 2009, nuk ka të evidentuar asnjë rast të krimit të organizuar kompjuterik. Në vitin 2010, fillojnë statistikat zyrtare me 26 vepra penale të evidentuara, zbuluar 17 ose 63%; në vitin 2011, janë evidentuar 84 dhe zbuluar 62 ose 74%; në vitin 2012, janë evidentuar 81 dhe janë zbuluar 57 ose 70.40%; në vitin 2013 janë evidentuar 108 dhe janë zbuluar 63 ose 58.30%; në vitin 2014 janë zbuluar 176 dhe janë zbuluar 75 ose 42.60% dhe, në vitin 2015, janë evidentuar 122 vepra penale dhe janë zbuluar 33 ose 27.00%. Në total, për periudhën 2010-2015, janë evidentuar gjithsej 598 vepra penale, dhe janë zbuluar 307 vepra penale ose 51.33%. Pra, 291 vepra penale ose 48.67%, janë krime të pazbuluara ose "*shifra të përhimëta*" të kriminalitetit. Kjo "*shifër e përhimët*" e kriminalitetit, në masën 48.67%, në pesë vite lë shumë për të dëshiruar. Siç e shpjeguam edhe më lart, krimi kompjuterik është formë e veçantë dhe shumë e rëndësishme dhe sidomos e rrezikshme e krimit të organizuar sidomos kriminalitetit të "*Jakave të Bardha*". Ndërkohë, në total, për shtatë fushat e veprimtarisë kriminale, të organizuar për periudhën 2008-2015 (Tabela nr. 2), janë evidentuar 31.092 vepra penale dhe janë zbuluar 29.398 vepra penale ose 51.33%. Pra, 1694 vepra penale ose 48.67% janë krime të pazbuluara, ose "*shifra të përhimëta*" të kriminalitetit, për shtatë veprimtaritë e krimit të organizuara në Shqipëri për periudhën 2008-2015.

Krimin kompjuterik, do ta konsideroja kriminalitetin "*on line*" dhe që nëpërmjet këtij kriminaliteti, zhvillohen, ndërmjetësohen, mbështetën dhe suportohen edhe krimet e tjera. Ndërkohë që, krimi kibernetik gjatë të së njëjtës periudhë, në raport me totalin e veprave penale, (31.092 vepra penale) janë evidentuar (totali 29.398 vepra penale) 598 vepra penale, ose vetëm 1.92 % vepra penale, dhe janë zbuluar 307, ose 1.04%, e tyre. Mendoj, se ky kriminalitet, nuk merr rëndësi nga shifrat e mësipërme, por nga

gjendja reale e ushtrimit të kriminalitetit kompjuterik, i cili përdoret gjerësisht edhe në format e tjera kriminale kryesor të organizuara. Le të kujtojmë vetëm faktin, që shteti "*on line*", ISIS, e zhvilloi aktivitetin e tij terrorist me pjesëmarrës nga 82 shtete të ndryshme të botës.

Kjo është "*fuqia negative*" e teknologjisë moderne, që krimi i organizuar transnacional dhe terrorizmi, e përdorin për të bërë terror, shantazh, për të vjedhur, mashtruar, për të kryer trafiqet e paligjshme së të gjitha llojeve dhe, për të pastruar paratë, nëpërmjet mënyrave të shfrytëzimit të kompjuterit, si mjet për kryerjen e krimit, si dhe nëpërmjet formave të krimeve kompjuterike si: mashtrimet nëpërmjet internetit, mashtrimet me karta bankare, falsifikimi kompjuterik, ndërhyrjet e paligjshme kompjuterike, shkelje e të drejtës së autorit në internet, shkelje të privatësisë, përndjekje, shpifje dhe fyerje, terrorizëm kompjuterik, përdorim i paautorizuar dhe përhapje e informacionit të privilegjuar dhe, pastrimi i produkteve të krimit, apo veprimtarisë kriminale lidhur me krimin kompjuterik. Prandaj, kërkohet që në të ardhmen, të bëhet një investim shumë më i madh dhe më serioz, për parandalimin, dokumentimin dhe goditjen e luftën kundër krimeve kompjuterike dhe kërcënimeve kibernetike në Shqipëri.

6. Krimi kompjuterik dhe kërcënimet kibernetike cenojnë sigurinë kombëtare

Krimin kompjuterik dhe kërcënimet kompjuterike i trajtuam në çështjet e mësipërme, si vepra penale, si krime dhe si kriminalitet i organizuar që cenojnë liritë dhe të drejtat e njeriut, institucionet shtetërore e publike, bizneset private dhe sigurinë kibernetike. Një nga parimet e sigurisë kibernetike është parimi i sigurisë shtetërore, sipas së cilit, siguria kibernetike është pjesë përbërëse e sigurisë shtetërore, mbështet funksionimin e shtetit dhe shoqërisë, konkurrencën e ekonomisë dhe inovacionin. Ky parim, nënkupton mbrojtjen e të drejtës për siguri dhe mbrojtje, për të gjithë qytetarët, përmes parandalimit të krimit kibernetik. Prandaj merr shumë rëndësi, infrastruktura kritike (telekomunikacioni, kompjuterët/softuerët, interneti, satelitët, etj.), e cila është prona, ose institucioni me rëndësi të madhe për të mirën publike, e që dështimi apo cenimi i së cilës do të çonte drejt tkurrjeve të qëndrueshme të furnizimit, çrregullimeve të konsiderueshme të sigurisë publike, apo në pasoja të tjera dramatike. Infrastruktura kritike e informacionit (IKI), (sistemet TIK) që janë infrastruktura kritike për vetveten apo që janë thelbësore për funksionimin e infrastrukturave kritike, kanë një rëndësi jetike për sigurinë shtetërore. Këto, janë në përputhje me dokumentin e metodologjive të ENISA-s, p*ër identifikimin e aseteve dhe shërbimeve të Infrastrukturës Kritike të Informacionit*[28].

Ky Dokument është gjithashtu në linjë me Agjendën Digjitale për Evropën 2020 (cit. *Rritja e besimit në TIK nëpërmjet forcimit të politikës së sigurisë për rrjetet dhe informacionin*) si dhe, në linjë me Strategjinë për Sigurinë Kibernetike të Bashkimit Evropian: Hapësirë kibernetike e hapur, e sigurt dhe e mbrojtur (ang. *Cybersecurity Strategy of the European Union*: *An Open, Safe and Secure Cyberspace*)[29].

[28] ENISAhttps://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/Methodologies-for-identification-of-ciis.

[29] Strategjia e Sigurisë Kombëtare (SSK),2014-2020, faqe 10.

Krimi kibernetik, si krim jokonvencional, është identifikuar si një prej rreziqeve, sfidave dhe kërcënimeve globale, që mund të cenojnë edhe sigurinë kombëtare. Dokumenti i Gjelbër i Programit Evropian për Mbrojtjen e Infrastrukturës Kritike, Komisioni Evropian, jep një listë treguese me 11 sektorë kritikë[30]: energjia; teknologjia e informacionit dhe komunikimit; uji; ushqimi; shëndetësia; financat; rendi dhe siguria publike e juridike; administrata civile; transporti; industria kimike dhe bërthamore; dhe, hapësira e hulumtimet. Miratimi dhe zbatimi i Strategjisë Kombëtare për Sigurinë Kibernetike, për vendosjen dhe respektimin e standardeve më të larta në drejtim të ruajtjes dhe mbrojtjes së informacionit, në të gjitha trajtat e ekzistencës së tij, duke përqendruar përpjekje të veçanta për mbrojtjen nga sulmet kibernetike,[31] i parashikuar në Strategjinë e Sigurisë Kombëtare, është realizuar.

Sipas Strategjisë së Sigurisë Kombëtare të Republikës së Shqipërisë, të miratuar në vitin 2014, shtojca C-Klasifikimi i rreziqeve, i cili është bërë duke shqyrtuar dy parametra kryesorë: gjasat e shfaqjes së rrezikut dhe pasojat që mund të shkaktojnë për sigurinë kombëtare. Në bazë të kombinimit të këtyre dy parametrave rreziqet janë klasifikuar në tri nivele. Në nivelin e parë janë grupuar rreziqet që kanë gjasa të larta shfaqjeje dhe pasoja të larta në rast se materializohen. Rreziqet e nivelit të parë Kategoritë e mëposhtme të rreziqeve kanë prioritetin më të lartë për sigurinë e RSH-së. Gjasat e shfaqjes dhe pasojat e tyre për sigurinë kombëtare vlerësohen të larta.•Korrupsioni dhe krimi i organizuar;•Kriza energjetike, që kërcënon sigurinë e furnizimit të RSH-së dhe cënon rritjen ekonomike; •Mangësitë në kontrollin dhe administrimin e territorit, që kërcënojnë sigurinë individuale dhe favorizojnë trafiqet e ndryshme; •*Sulmet kibernetike nga aktorë shtetërorë ose joshtetërorë*[32]**.**

Gjithashtu, Strategjia e Sigurisë Kombëtare shprehet se: "Ndërtimi i rrjetit kombëtar të komunikimit të sigurt, për qarkullimin e informacionit të klasifikuar dhe përmirësimi i zbatimit të procedurave të certifikimit"[33]**.** Por, "Shqipëria renditet ndër vendet ku zhvillimi i telekomunikacionit, qasja në internet dhe informatizimi i shoqërisë përparon shumë shpejt. Rritja e komunikimit përbën një vlerë të shtuar në zhvillimin ekonomik dhe shoqëror të vendit, por, në të njëjtën kohë, ajo e ekspozon atë ndaj rreziqeve të natyrës kibernetike me aktorë shtetërorë dhe joshtetërorë. Sulmet kibernetike kanë potencial për të dëmtuar rëndë shkëmbimin e informacionit në institucionet publike, të telekomunikacionit dhe sistemin financiar e bankar, duke shkaktuar edhe ndërprerje të shërbimeve jetike[34]. Ndërsa, Dokumenti i Politikave për Sigurinë Kibernetike, 2015-2017 përcakton vizionin:

"Për një hapësirë kibernetike më të sigurt, më të besueshme dhe më të qëndrueshme për qytetarët, biznesin dhe qeverinë në mbështetje të zhvillimit ekonomik dhe social të Shqipërisë"[35]*.* Prandaj, kërkohet që të zbatohen me përgjegjshmëri, në afatet e përcaktuara dhe me cilësi këto objektiva strategjike të Sigurisë kombëtare për sigurinë kibernetike,parandalimin dhe luftimin e kriminalitetit kompjuterik dhe kërcënimeve kibernetike, si dhe për sigurinë e komunikimit elektronik.

[30] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52005DC0576.
[31] Po, aty, faqe 10.
[32] Ligj, nr. 103/2014, date 31.7.2014, "Për miratimin e Strategjisë së Sigurisë Kombëtare të Republikës së Shqipërisë", data e miratimit: 31.7.2014, Fletore Zyrtare nr. 137, faqe 16 (Shtojca A-Qasja e re për funksionimin e arkitekturës së sigurisë Shtojca B -Analiza e rreziqeve, Shtojca C-Klasifikimi i rreziqeve.)
[33] Po aty, faqe 8.
[34] Po aty, faqe 15.
[35] Dokumenti i Politikave për Sigurinë Kibernetike, 2015-2017, faqe 19.

7. Përfundime dhe rekomandime

Studimi krimi kompjuterik dhe kërcënimet kibernetike cenojnë sigurinë kombëtare, merr një rëndësi të veçantë dhe i jep përgjigje hipotezës dhe pyetjes kërkimore të ngritur. Ai provon gjendjen e aspekteve ligjore e të ndjekjes penale e hetimit të krimeve kompjuterike e kërcënimeve kibernetike, si dhe të ndikimit të tyre në sigurinë kombëtare. Hapësira kibernetike sot është një nga sfidat më të mëdha ligjore dhe të sigurisë. Rritja e mundësive për sjellje kriminale përmes internetit ka çuar në rritjen e kriminalitetit dhe të kërcënimeve kombëtare dhe ndërkombëtare. Prandaj, nga ky studim, si zgjidhje më të suksesshme për të ardhmen do të ishte e rekomandueshme:

Së pari, me rritjen e aksesimit të internetit nga përdoruesit e saj në Shqipëri janë rritur edhe krimet kompjuterike dhe kërcënimet kibernetike dhe janë një ndër veprimtaritë kriminale të organizuara vonë, sepse lidhet me zhvillimin e vonshëm të teknologjisë së kompjuterëve elektronik digjital dhe reagimit me vonesë të institucioneve shtetërore për parandalimin e tyre.

Së dyti, baza ligjore dhe ndryshimet e bëra në fushën e sigurisë kibernetike, kanë qenë hapi i parë për goditjen dhe luftimin e krimit kibernetik. Strategjia Ndërsektoriale për Shoqërinë e Informacionit 2008-2013 (SNSHI) e miratuar me VKM nr. 59 datë 21.1.2009 përbën dokumentin e parë strategjik që përcaktonte drejtimet kryesore dhe objektivat e zhvillimit në fushën e shoqërisë së informacionit për periudhën 2008-2013, dhe ku përmendej shkurtimisht *siguria kibernetike*, si një nga fushat që duhej konsideruar me prioritet për shkak të vizionit të Qeverisë shqiptare për të rritur e zhvilluar qeverisjen përmes ofrimit të e-shërbimeve.

Së treti, lufta për parandalimin dhe goditjen e krimit kompjuterik dhe kërcënimeve kibernetike, filloi në mënyrë më të organizuar pas gjysmës së dytë të vitit 2009, pasi treguesit sipas statistikave të Policisë së Shtetit, në vitet 2008 dhe 2009, ishin zero dhe në vitin 2010, fillojnë statistikat zyrtare me 26 vepra penale të evidentuara, zbuluar 17 ose 63%. Në total për periudhën 2010-2015 janë evidentuar gjithsej 598 vepra penale, ose vetëm 1.92 % vepra penale në total, dhe janë zbuluar 307 vepra penale ose 51.33%, e veprave penale për krimet kompjuterike ose 1.04% e totalit të tyre. Prandaj, të dhënat e mësipërme për parandalimin dhe goditjen e krimit të organizuar kibernetik në Shqipëri, janë tregues të ulët dhe kërkohet një luftë më e organizuar ndaj kriminalitetit të organizuar kibernetik.

Së katërti, krijimi dhe implementimi i kërkesave minimale të detyrueshme të sigurisë kibernetike, për institucionet shtetërore,publike e private me qëllim mbrojtjen e infrastrukturës kritike të informacionit dhe parandalimin e krimeve kompjuterike dhe kërcënimeve kibernetike, si dhe shtimi i investimeve për rritjen e sigurisë në rrjetet/sistemet shtetërore. Gjithashtu, kërkohet rritja e ndërgjegjësimit dhe e nivelit të njohurive, aftësive dhe kapaciteteve për ekspertizë në fushën e sigurisë kibernetike.

Së pesti, kuadri ligjor që merret me sigurinë dhe krimin kibernetik në Shqipëri përfshin gjithsej katërmbëdhjetë struktura qeveritare ku përgjegjës është ministri përgjegjës për Administratën Publike dhe Inovacionin. Duke patur parasysh rëndësinë e madhe që ka siguria kibernetike; sulmet e vazhdueshme që bëhen nga krimi i organizuar; domosdoshmëria e rritjes së bashkëpunimit ndërmjet institucioneve shtetërore e private; si dhe faktin që në Strategjinë e Sigurisë Kombëtare, sulmet kibernetike nga aktorë shtetërorë ose joshtetërorë, janë klasifikuar rreziku i katërt në

rreziqet e nivelit të parë, dhe vazhdojnë të përbëjnë cenim të sigurisë kombëtare. Në kuadër të një reagimi të koordinuar ndaj kërcënimeve të ndryshme nga Ekipet Kompjuterike për Reagime Emergjente, sugjeroj që në këtë drejtim të përfitohet nga përvoja e aplikuar në Kosovë, "Caktimi i Koordinatorit Kombëtar dhe Këshillit Shtetëror për Sigurinë Kibernetike", si institucion përgjegjës për përmbushjen e objektivave dhe të monitorojë indikatorët e Strategjisë për Sigurinë Kibernetike dhe ti raportojë në mënyrë periodike Kryeministrit dhe Këshillit të Sigurisë Kombëtare. Gjithashtu, me miratimin e ligjit për sigurinë kibernetike, kërkohet që në bazë të Direktivës së BE-së 2016/1148, të Parlamentit Europian dhe të Këshillit, datë 6 korrik 2016, "Mbi masat për një nivel të përbashkët të lartë të sigurisë së rrjeteve dhe sistemeve të informacionit në Bashkimin Europian", të miratohen ndryshimet dhe plotësimet e dispozitave të Kodit Penal dhe të Kodit të Procedurës Penale, në lidhje me krimin kibernetik, për vepra penale të tjera në fushën e sigurisë kibernetike, siç i kanë parashikuar vendet e BE-së, ku Shqipëria po plotëson detyrimet e saj për t'u bërë pjesë e saj.

Së gjashti, universitetet publike dhe private të hartojnë programe mësimore dhe kurrikula për lëndën e re mësimore "Siguria kibernetike" e cila duhet të përfshihet ne drejtimet "bachelor" dhe master në shkencat teknologjisë së informacionit, sigurisë, juridike, ekonomike, shkencave politike, marrëdhënieve ndërkombëtare, administratës publike,etj.

Bibliografia

1. Vendim nr. 973, datë 02.12.2015,"Për miratimin e dokumentit të politikave për sigurinë kibernetike të Republikës së Shqipërisë, 2015 - 2017".
2. Ligj nr. 103/2014, date 31.07.2014, "Për miratimin e Strategjisë së Sigurisë Kombëtare të Republikës së Shqipërisë".
3. Strategjia Shtetërore për Sigurinë Kibernetike dhe Plani i Veprimit,2016-2019 të Republikës së Kosovës, dhjetor 2015.
4. D. Krapac: Kompjutorski kriminalitet, Zagreb, 1992.
5. Dr. sc. Veton Vula "Kriminaliteti i Organizuar", Prishtinë, 2013.
6. M. E. Kabay,*"A Brief History of Computer Crime",* 2008.
7. Strategjia Ndërsektoriale për Shoqërinë e Informacionit,2008-2013 (SNSHI) e miratuar me VKM nr. 59 datë 21.1.2009.
8. Tenhuen M."Combating Computer Crime", Interpol Review, nr. 147, 1989.
9. Mohr K. Polizeiliches Lagebild der Computer Kriminalitet "Die Policai no.2 Bremen, 1987.
10. Ligj nr. 9859, datë 21.1.2008 "Për disa shtesa dhe ndryshime në ligjin nr. 7895, datë 27.1.1995 "Kodi penal i Republikës së Shqipërisë", të ndryshuar.
11. Ligj nr. 10023, datë 27.11.2008 "Për disa shtesa dhe ndryshime në ligjin nr. 7895,datë 27.1.1995 "Kodi penal i Republikës së Shqipërisë", të ndryshuar.
12. Ligj nr. 10054, datë 29.12.2008 "Për disa shtesa dhe ndryshime në ligjin nr. 7905,datë 21.3.1995 "Kodi i procedurës penale i Republikës së Shqipërisë", të ndryshuar.
13. Ligj nr. 144/2013"Për disa shtesa dhe ndryshime në ligjin nr.7895,datë 27.1.1995 "Kodi Penal i Republikës së Shqipërisë", të ndryshuar.
14. August Bequaj "How to Prevent Computer Crime", John Walley & Sons, Inc,1983. Carter L.D. "Computer Crime Categories: How Techno-criminals Operate" FBI Law Enforcement Bulletin.
15. Ligj nr. 8888 datë 25.04.2002,"Për Ratifikimin e Konventës për Krimin Kibernetik",fletore zyrtare nr. 18 datë 17.05.2002, faqe 553.
16. Ligj nr. 9262 i datës 29.07.2004 "Për Ratifikimin e Protokollit shtesë të Konventës për krimin kibernetik, për penalizimin e akteve me natyrë raciste dhe ksenofobe të kryera nëpërmjet sistemeve kompjuterike".
17. Ligj nr. 9859 datë 21.01.2008 "Për disa shtesa dhe ndryshime në ligjin nr. 7895 datë 27.01.1995 (Kodi Penal i Republikës së Shqipërisë) i ndryshuar.
18. Ligj nr. 10054 datë 29.12.2009, "Për disa shtesa e ndryshime në ligjin nr. 7905 datë 21.03.1995 (Kodi i Procedurës Penale të Republikës së Shqipërisë) i ndryshuar .

19. Vendim i Këshillit të Ministrave nr. 14 datë 9.1.2008,"Për miratimin e Strategjisë së Policisë së Shtetit 2007-2013".
20. Urdhër nr. 372 datë 08.06.2009 i Ministrit të Brendshëm,"Për miratimin e strukturës dhe limitit të Organikës së Drejtorisë së Përgjithshme të Policisë së Shtetit".
21. Urdhër nr. 200 datë 16.06.2010 i Ministrit të Brendshëm,"Për disa ndryshime në Urdhrin nr. 372, datë 08.06.2009, të Ministrit të Brendshëm"Për miratimin e strukturës dhe limitit të organikës së Drejtorisë së Përgjithshme të Policisë së Shtetit".

Burime nga interneti

https://www.internetworldstats.com/stats.htm.
http://open.data.al/en/lajme/lajm/id/214/Number-of-internet-users-in-Albania.
http://www.balkaneu.com/albania-internet-users-italy-greece-world-bank.
https://www.indexmundi.com/albania/internet_users.html.
https://freedomhouse.org/.https://www.zeriamerikes.com/a/4114767.html.
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52013JC0001.
http://www.nsi.org/Library.Compsec/crimecom.html.
https: //arditmuca.files.wordpress.com/2010/07/kriminaliteti-kompjuterik.pdf.
ENISAhttps://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/Methodologies-for-identification-of-ciis.
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52005DC0576.
http:www.webnerds.com/ computercrime/main.html.
web: www.un.org/ documents/ ga/res /45/a 45r121.html.
web:http://www.interpol.int/News-and-media/Events/2015/Europol-INTERPOL-Cybercrime-Conference/Europol-INTERPOL-Cybercrime-Conference.


AKADEMIA E SIGURISË
AS
1971

Spiunazhi kibernetik, si instrument hibrid i shteteve ose shërbimeve të inteligjencës, për realizimin e synimeve, sa të vjetra, aq dhe të reja

■**Dr. Mimoza XHARO**
Eksperte në fushën e sigurisë
mxharo@hotmail.com

Abstrakt

Hapësira kibernetike, në evoluim, rritje e zgjerim të shpejtë, po shndërrohet në shënjestrën e ri të kërcënimeve hibride, për nga natyra. Aktorë shtetërorë dhe joshtetërorë preferojnë këtë hapësirë të administrojnë, ruajnë, transmetojnë, komunikojnë për aktivitetin e tyre social, ekonomik, politik dhe të sigurisë. Përveç krimit kompjuterik, sulmeve kibernetike për llogari të terrorizmit, krimit të organizuar, një ndër format e kërcënimeve kibernetike është edhe spiunazhi kibernetik. Grumbullimi i informacionit sensitiv po shndërrohet si një mjet real dhe në rritje nga shtetet/shërbimet e tyre të inteligjencës dhe entitetet e lidhura me to. Spiunazhi kibernetik duket si kërcënim më pak i dukshëm për publikun për nga impakti krahasuar me një sulm kibernetik për llogari të krimit dhe terrorizmit. Përdorimi i hapësirës kibernetike për spiunazh është më i sofistikuar, dizajnuar për të mbuluar identitetin, origjinën, vendin, organizatën, shtetin e origjinës apo që fshihet pas tyre. Kjo formë grumbullimi e shpërndarje informacioni/dezinformimi po ndikon në ekonomitë, kohezionin social, marrëdhëniet politike dhe arkitekturën e sigurisë. Përveç se në nivel global, është evidentuar aktivitet në rritje e vendeve si Rusia, Kina por edhe aktorë të tjerë globalë e lokalë, në raport me zhvillimet në rajonin tonë, problematikat ndërshtetërore, orientimet/hapat drejt proceseve integruese etj. Përveç prezencës me format klasike të spiunazhit, ka angazhime në aktivitete propagandistike, dezinformuese dhe spiunazhi kibernetik. Ky shkrim synon të japë një kuptim të përgjithshëm të spiunazhit kibernetik, adresojë shqetësimin në rritje të tij, e ndihmojë në ndërgjegjësimin për motivet, metodat, dhe rëndësinë e masave mbrojtëse për parandalim.

Fjalëkyçe:

hapësirë kibernetike, spiunazh kibernetik, sulme kibernetike, shërbime inteligjence, kërcënim, siguria kombëtare.

1. Hyrje

Në një epokë të udhëhequr nga teknologjia e informacionit, aktorë shtetërore e jo shtetërorë po preferojnë hapësirën kibernetike të administrojnë, ruajnë, transmetojnë, komunikojnë *online*, përdorin rrjete kompjuterike për aktivitetin e tyre social, ekonomik, politik dhe të sigurisë. Përdorimi i kësaj hapësire për motive spiunazhi, është një nga problemet ndërkombëtare më intriguese, po përdoret nga shtetet për synime gjeopolitike/gjeoekonomike dhe po influencon në një shkallë të konsiderueshme marrëdhëniet midis shteteve[1]. Në këtë realitet të ri, edhe mënyrat e grumbullimit të informacionit, të njohura dhe si mënyrat klasike të spiunazhit[2], kanë evoluar e janë sofistikuar. Është një veprimtari e heshtur, dhe ndryshe nga krimet e tjera, mund të kryhet për vite me radhë, pa u diktuar dhe me pasoja serioze për sigurinë kombëtare e ndërkombëtare. Përveçse për synime gjeostrategjike paraqitet me një agjendë të larmishme në objektiva kulturore, sociale, ekonomike dhe politike.

Spiunazhi kibernetik vepron në mbulim të plotë dhe detajet mbi "kush", "çfarë" dhe "pse" janë shpesh të paqarta. Është një nga fushat më shqetësuese dhe më të rëndësishme të sigurisë, ndërkohë që edhe numri i sulmeve kibernetike apo aktiviteteve influencuese *online*, të sponsorizuara nga shtetet, po rritet në mënyra mbresëlënëse, për shkak të angazhimit të qeverive në teknologjinë kibernetike. Sulmet kibernetike përbëjnë një mjet, mes aktiviteteve të tjera të ndërmarra në kohë paqeje. Përveç grumbullimit të inteligjencës, sulme që kanë shkaktuar dëme janë përdorur ndaj infrastrukturës kritike, të cilat iu janë atribuuar aktorëve shtetërorë. Sulme kibernetike

[1] Alina Polyakova, et al., *Kremlin's Trojan Horse*, November 2017.
[2] Nëpërmjet përdorimit të agjentëve.

me intensitet më të ulët, me motiv spiunazhi, kanë synuar të ushtrojnë një presion/ influencë politike ndaj një kundërshtari, por më frekuente se ato me intensitet më të lartë dhe pasoja imediate shkatërrimtare.

Për shumë përdorues të përditshëm të internetit, bota e fshehtë e spiunazhit kibernetik ndërkombëtar mund të duket e largët dhe pa ndonjë rëndësi, duket sikur nuk influencon direkt jetët e tyre, por kostot ndaj një shteti janë të mëdha. Impakti mund të fillojë me kosto monetare, dëmtim të infrastrukturës kritike, cenim të parimeve demokratike të një shoqërie, cenim të sigurisë kombëtare, shumëfishim force në konflikte ushtarake. Të dhënat e referuara nga ekspertët hedhin dritë mbi përmasat, trendin në rritje të përdorimit të hapësirës kibernetike për krim kibernetik përfshi spiunazh kibernetik. Sipas *Panda Security*, 1 në 131 email-e përmban viruse, 230 000 *malware* të reja prodhohen çdo ditë dhe me trend rritjeje, ku *Trojan-i* mbetet burimi kryesor, i gjetur përgjegjës për 51.45% të rasteve të zbuluara, 14.78% e individëve deklarojnë se e njohin rrezikun që vjen nga klikimi dhe përsëri nga kureshtja vijojë të klikojnë[3], 1 sulmues shpenzon rreth 146 ditë në një rrjet para se të detektohet (kohë e mjaftueshme për të marrë të dhëna sensitive)[4]. Vetëm nga një krahasim i thjeshtë statistikor, lidhur me motivet e sulmeve kibernetike, për të njëjtin muaj (korrik) të vitit 2016 dhe 2018, ka rezultuar nga 9.2% (2016) të lidhura me spiunazhin kibernetik, ka shkuar në 14.6%, (2018), çka dëshmon që spiunazhi kibernetik është në rritje.

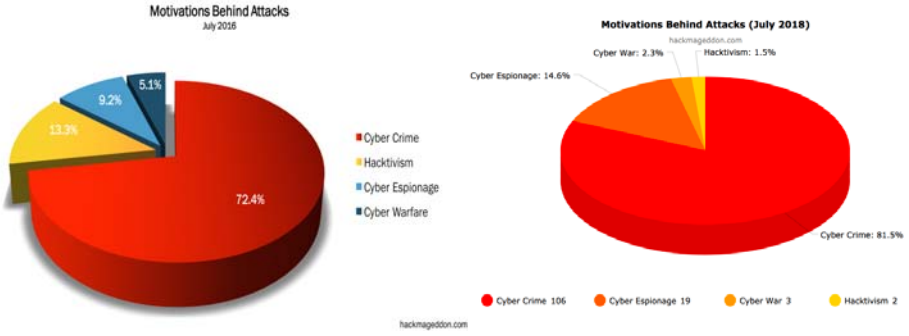


Figura 1. Statistika mbi motivet e sulmeve kibernetike, vetëm për muajin korrik 2016, 2018[5].

Kohët e fundit, ka shumë raportime në mbarë botën, për fushata të spiunazhit kibernetik, që kanë shënjuar qeveritë, sektorët e industrisë, shoqëritë demokratike. Shumica e këtyre goditjeve dyshohet se kanë të bëjnë me hakera të sponsorizuar nga shtete, të cilat kanë mundësi për të ofruar informacion sensitiv. Edhe në rajon dhe vendin tonë, zhvillimi i shpejtë i shërbimeve *online*, përveç avantazheve, po sjell edhe rrezikun e sulmeve dhe spiunazhit kibernetik. Shpesh publiku shqiptar mendon se vendi ynë është i vogël, dhe se aktorë të rëndësishëm globalë nuk janë të interesuar. Por kjo është një dukuri globale dhe janë aktorët globalë, ata që interesohen për të tjerët[6].

[3] Even this expert on hackers got tricked into clicking a scam email, Business Insider, 2016.
[4] Jupiner Research.
[5] Information security timelines and statistcis. https://www.hackmageddon.com/2018/.../june-2018-cyber-attacks.
[6] Henri Hide, Konferenca "Sfidat e Sigurisë Kibernetike në Shqipëri, Fondacioni Friedrich Ebert dhe Qendra Shqiptare për Qeverisje të Mirë në Shqipëri, 4 tetor 2017; https://www.fes-tirana.org/al/al-news.

Nëpërmjet studimit të rasteve të njohura publikisht, analizës së kontekstit të sigurisë, kërcënimin që paraqet spiunazhi kibernetik për sigurinë kombëtare, synohet të jepet, në formën e një përshkrimi analitik, një përqasje konceptuale, impakti në sigurinë kombëtare, ndërgjegjësimi për shkallën e rrezikut dhe rëndësia e masave mbrojtëse e parandaluese. Marrë në konsideratë aktivitetin në rritje, është e rëndësishme të elaborohet se çfarë kuptohet me spiunazh kibernetik, prirjet e tij dhe impaktin në çështje të sigurisë kombëtare.

2. Çfarë është spiunazhi kibernetik? Përqasje konceptuale.

Termat krim kibernetik, terrorizëm kibernetik, sulm kibernetik, duken më të përdorura dhe më të kuptuara nga publiku dhe të rregulluara në legjislacion. Shumë vende dhe organizma ndërkombëtare kanë krijuar përkufizime specifike, ndaj mbetet ende i vështirë një përkufizim i pranuar përbotshëm. Faktorë si natyra e dëmit që shkakton, identiteti i origjinës dhe metodologjia e përdorur për aksesin, vjedhjen e informacioneve nëpërmjet shfrytëzimit, ndërhyrjes, sulmit të hapësirës digjitale, janë përdorur si elementë që përafrojnë qasjet te spiunazhi kibernetik.

Spiunazhi si term linguistik përkufizohet si praktika e spiunimit/përdorimit të spiunëve për të marrë informacion mbi plane/aktivitete kryesisht ndaj një qeverie të huaj apo një kompanie kundërshtare[7]. Shumë studiues e cilësojnë si shënjim të informacionit sekret, për qëllime *malinje*,[8] por nuk përbën një përkufizim të fenomenit, pasi nuk adreson synimin, origjinën (shtet), natyrën e informacionit. Për disa ish-ekspertë sigurie, është një formë e sulmit kibernetik, nëpërmjet të cilit aksesohet informacion i klasifikuar, të dhëna sensitive apo pronësi intelektuale, për të përfituar një avantazh ndaj një kompanie apo entiteti qeveritar [9]. Mund të përkufizohet edhe si një mjet për zbatimin e një politike, po aq edhe për të influencuar një politikë të caktuar.

Sipas këtij përkufizimi ndahet në dy pjesë: operacione të mbuluara (mjet për ekzekutimin e një politike) dhe grumbullimi informacioni (mjet për të përcjellë ndikuar/influencuar një politikë). Kategoria e parë përfshin operacione aktive dhe kibernetike, të cilat ndërmerren cenuar sovranitetin e një vendi tjetër[10]. Vetë kjo formë mund të ndahet në operacione force detyruese, aksione politike dhe propagandë[11]. Ajo që i dallon janë metodat që përdoren si, përdorimi i forcave aktive dhe përdorimi i programeve kibernetike, të cilat mund të ndikojnë në synimin, por që kanë thjesht një element force apo një element influencues[12].

Nga burimet e rëndësishme të inteligjencës janë edhe burimet e hapura të informacionit[13], të akesueshme për publikun. Ndërhyrja në sisteme elektronike të paautorizuara, me qëllim marrje informacioni nuk ka të bëjë me këtë burim, por me

[7] Myriam Webster, shih edhe dictionary.com
[8] Schaap, Arie J, Cyber Warfare Operations: Development and Use Under International Law. AFL Rev. 64 (2009): pp.121.
[9] David Weissbrodt, Cyber-Conflict, Cyber-Crime and CyberEspionage, University of Minnesota Law School, weiss001@umn.edu
[10] Veronika Prochko, cituar Fatouros 1976, 193; Jackamo 1992, 992, The international legal wiew of espionage, 30 march 2018; e-international relations students.
[11] Martin Libicki, The Coming of Cyber Espionage Norms, 9th International Conference on Cyber Conflict publication, 2017 .
[12] Veronika Prochko, The international legal Vlew of espionage, 30 march 2018; -e-international relations students.
[13] OSINT, informacion i përftuar nga burimet e hapura në funksion të produktit final të inteligjencës.

spiunazh kibernetik, pasi tenton të aksesojë informacione sensitive, me shkallë klasifikimi dhe/ose akses të paautorizuar për kategori të caktuara. Ndërhyrja në sisteme elektronike është element i krimit kibernetik. *Motivi* është ai që e ndan atë nga spiunazhi kibernetik. Për krimin kibernetik motivi është financiar, individual apo për llogari të grupi krimi të organizuar[14]. Ndërsa hakerimi për motiv marrje informacioni për llogari të një shërbimi inteligjence të një shteti është spiunazh kibernetik. Ky hakerim mund të kryhet nga punonjës inteligjence/struktura, por edhe nga të tretë *(by proxy),* të cilët përdoren apo vihen në shërbim të një shërbimi inteligjence. Përdorimit i aktorëve të tretë përkundrejt pagesës financiare, nga disa studiues referohet si *mercenarizëm kibernetik*[15]. Hapësira kibernetike e krijon këtë avantazh, favorizon ndjeshëm pazbulueshmërinë, pasi shërbimet e inteligjencës në vend që të rekrutojnë agjentë, rekrutojnë të tretë, të cilët mund të jenë ekspertë teknologjie informacioni, kompani ose thjesht hakera. Në këtë rast, edhe këta të fundit udhëhiqen nga motivi financiar, por në vend që ta krijojnë direkt, e përfitojnë nga shërbimi që ofrojnë.

Hakerat, përveçse për motiv financiar, u referohen edhe aktorëve të motivuar nga një ideologji, më thjesht, për -*izmat* e ndryshëm si nacionalizëm, ekstremizëm, etj., për të promovuar agjendat e tyre etj. Hakerimi është forma e re e spiunazhit. Fusha bashkëkohore e betejës po kryhet në tastiera e sisteme, më shumë se në *dead box* apo *balaclavas*[16].

Disa studiues, elementët grumbullues, nëpërmjet spiunazhit kibernetik, i emërtojnë si *aktivitete influencuese online*, referuar aktivitete të koordinuara nga një aktor shtetëror, me synimin për të influencuar vendimmarrjen politike, perceptimin e publikut apo të një grupi të caktuar. Kryhet kryesisht nëpërmjet shpërndarjes së informacionit dezinformues/të rremë. Dallimi mes aktiviteteve dezinformuese dhe sulmeve kibernetike është i rëndësishëm, për dy arsye*: së pari* grupi i parë i aktiviteteve është shpesh i ligjshëm, ndërkohë që sulmet kibernetike përbëjnë krim; s*ë dyti* sulme të ndryshme kërkojnë masa në proporcion me kërcënimin. Efektet e sulmit kibernetik mund të jenë të përkohshme, nëse synimi nuk është përshkallëzim drejt konfliktit[17]. Në zonën gri mes luftës dhe paqes, sulmet kibernetike mund të përdoren për të mbështetur objektiva në mënyra të ndryshme, përfshi grumbullim inteligjence, infektim të pajisjeve kompjuterike dhe ueb-faqeve për të shpërndarë propagandë, vjedhje të dhënash sensitive/personale nga rrjetet sociale, dhe sulme të tipit DDoS[18].

Si përkufizim më përfshirës për spiunazhin kibernetik konsiderohet ai i dhënë në Manualin e Tallinit (2013)[19] si *një akt i ndërmarrë në mënyrë të fshehtë ose nën pretendime false, që përdor kapacitete kibernetike për të grumbulluar informacion me synimin e komunikimit dhe transmetimit të tyre një pale kundërshtare*"[20]. Pra, nga sa u përshkrua më lart, spiunazhi kibernetik nënkupton sulm, manipulim, ndërhyrje në sisteme kompjuterike, rrjete digjitale nga aktorë shtetërorë (shërbimet e inteligjencës së tyre), apo aktorë të tjerë që veprojnë për llogari të tyre, me synim manipulim,

[14] Denning, D. (2000). Cyber Terrorism. https://pdfs.semanticscholar.org/7fdd/.pdf
[15] Scott Depasquale and Michael Daly,The growing threat of cyber mercenaries, Politico magazine, 2016.
[16] Eric O'Neill, ish specialist FBI dhe ekspert në çeshtjet e sigurisë kombëtare; Carbon Black.
[17] 27 Martin C. Libicki, "The Convergence of Information Warfare," Strategic Studies Quarterly, Spring 2017: 49-65.
[18] Po aty
[19] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, referuar nga Michael. N. Schmitt, Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum, 2017; Harvard National Security Journal / Vol. 8, faqe 240.
[20] Michael. N. Schmitt, The Law of Cyber Warfare: Quo Vadis? 25 Stanford Law&Policy Review 2014, f. 298.

kompromet im, vjedhje informacioni sensitiv, dezinformim, fitim dhe mbajtje aksesi për qëllime dhe avantazh eventual apo strategjik. Aktivitete të kësaj natyre kanë sjellë më shumë raste ndërhyrje në zgjedhjet politike, krijuar kaos dhe lajme të rreme lidhur me zhvillime të rëndësishme ndërkombëtare dhe ndihmuar konkurrencën ekonomike, me motiv sigurimin e një avantazhi ekonomik. Përgjithësisht njihen dy tipa spiunazhi kibernetik: (a)spiunazh shtetëror, kur janë të përfshirë aktorë shtetërorë; (b)spiunazh industrial (ekonomik) kur janë të përfshirë aktorë tregtar[21].

3. Spiunazhi kibernetik, impakti në sigurinë kombëtare

Spiunazhi kibernetik përgjithësisht ka synime strategjike, ndërkohë që sulme të nivelit të ulët japin efekte taktike dhe operacionale, të cilat së bashku me operacionet/efektet psikologjike mund të cenojnë sigurinë. Impakti mund të fillojë me kosto të mëdha ekonomike, dëmtim serioz të infrastrukturës kritike, deri cenim të elementëve thelbësorë të sigurisë kombëtare. Kapacitetet kibernetike përdoren si shumëfishim force në konfliktet ushtarake dhe në kohë paqe. Sulmet kibernetike mund të prodhojnë efekte në pesë nivele:

(1) në set specifik të dhënash, duke kompromet uar konfidencialitetin, integritetin dhe disponueshmërinë e tyre; (2) në një sistem, kur informacioni kompromet ohet dhe bëhet i padisponueshëm; (3) në një vendimmarrje lidhur me sistem fizik e elektronik; (4) në një gamë më të gjerë sistemesh/individësh/organizatash/qeverish; (5) në një objektiv strategjik[22]. Efektet e nivelit të pestë cenojnë rëndë sigurinë kombëtare të një vendi. Synimi final është të ndryshojë sjelljen strategjike të kundërshtarit.

Shtetet ndërmarrin veprime spiunazhi kibernetik për shkatërrim/marrje informacioni, për interesat e tyre shtetërore. Në drejtim të spiunazhit kibernetik shtetëror mund të përmendet aktiviteti në rritje i Rusisë, Koresë së Veriut, Iranit, ndërsa në këndvështrimin e spiunazhit kibernetik ekonomik, si aktor global i spikatur është Kina. Rusia e ka bërë grumbullimin dhe konfliktimin e informacionit një bosht kryesor të strategjisë së saj kombëtare. Për këtë ndërmerr aktivitete influencuese, si ndërhyrje në proceset zgjedhore, me synim minimin e besimit në proceset demokratike, duke nxitur pasiguri, dyshime, konfuzion, frikë dhe kaos në shoqëritë perëndimore[23]. Në dokumentet strategjikë të saj[24] informacioni perëndimor perceptohet si kërcënim ndaj sigurisë dhe ambienti i informacionit si një fushë operacionesh. Në këtë mënyrë liria e informacionit dhe interneti shndërrohet në shënjestër të politikave të Rusisë[25]. Mekanizmat e saj kryesorë ndahen në informativo-psikologjike dhe informativo-teknike[26].

Rusia përveçse situatave politike, përdor edhe situata ekonomiko-sociale, procese që lidhen me globalizimin, inovacione teknologjike, nacionalizmin, fundamentalizmin, emigracionin, duke shfrytëzuar më së miri lirinë e shtypit dhe të shprehjes në vendet

[21] Shivaji Sengupta, Top 10 Cyber Security Needs in US Federal Government, https://mw.linkedin.com/pub/shivaji-sengupta/, June 26, 2018.
[22] David Ormrod and Benjamin Turnbull, "The cyber conceptual frameëork for developing military doctrine", Defence Studies 16(3) (2016): 270–98 [290–1].
[23] Government of Canada, Cyber threats to Canada's democratic process, Communications Security Establishment, Ottawa, 2017.
[24] Doktrina Ushtarake 2014, Strategjia e Sigurisë Kombëtare 2015.
[25] Stephen Blank, Russian Information war as Domestic Counterinsurgency, American Foreign Policy Interests 35(1) (2013): 31–44.
[26] informatsionoye protivoborstvo.

perëndimore[27]. Kur spiunazhi kibernetik shoqërohet me mjete tradicionale të luftës dëmet janë të mëdha. Në 2007, Rusia ndërmori një sulm DDoS në Estoni, që solli ndërprerjen e shërbimeve të komunikimit në gjithë vendin, edhe në 2008, në Gjeorgji, përdori të tilla sulme për të ndërprerë sistemin e komunikimit me/nga jashtë. Rasti i Estonisë referohet nga studiues të ndryshëm edhe si rasti i parë, ku spiunazhi kibernetik u përdor i kombinuar me luftën tradicionale. Në 2014, Rusia përdori të njëjtën taktikë në Ukrainë, para përdorimit të metodave tradicionale të luftës[28]. *Ne angazhohemi në politikën e jashtme në të njëjtën mënyrë se si angazhohemi në luftë, me çdo mjet, me çdo armë, me çdo pikë gjaku. Por, ashtu si dhe në luftë, ne varemi nga strategjia e gjeneralit të lartë dhe trimëria e ushtarit të thjeshtë*[29].

Media, portalet mediatike *online*, rrjetet sociale, gjithashtu janë instrumente të shkëlqyera për të kryer fushata të spiunazhit kibernetik. Përveç rrjeteve kompjuterike qeveritare, rrjetet sociale po përdoren për të rekrutuar agjentë që të arrijnë të marrin të dhëna mbi punonjës institucionesh shtetërore, që të përpunuara nga specialistë inteligjence ndihmojnë aktivitete spiunazhi. Teknikat kryesore të spiunazhit të zbatuara përmes platformës së medieve sociale mund të përmblidhen në: (1) ndërrimi i identitetit, ose aftësia për të imituar një përdorues tjetër; (2) simulimi i identitetit, krijimi i një profili të rremë; (3) ndërtimi i botëve personale/sociale, nëpërmjet një numri të madh profilesh të rreme (4) përdorimi i "boshllëqeve" të përdoruesve të vërtetë[30], p.sh. platforma *linkedin*, duke përfituar nga naiviteti njerëzor, u jep mundësinë spiunëve kibernetikë të qasen ndaj individëve të punësuar në institucione qeveritare apo organizata /institute joqeveritare[31].

Platforma *Facebook*, mbetet gjithashtu platformë e preferuar për aktivitete të tilla. Është bërë publik tashmë debati i përdorimit së të dhënave të Fb për të ndikuar dhe zhvilluar fushatën influencuese në zgjedhjet amerikane, rasti *Cambridge Analityca*[32]. Rasti i ndërhyrjes kundër komandantit më të lartë të NATO-s, ku nëpërmjet një llogarie të rreme në *Facebook*, u arrit të zbulohej rrjeti i miqve të tij dhe u aksesua informacion i ndjeshëm, si llogaritë private të postës elektronike, fotot, mesazhet etj[33]. Incidente të ngjashme janë shqetësuese.

Media sociale duket si një ambient efektiv edhe për aktivitete dezinformimi. Sipas një raporti të "Freedom on the Net 2017", është observuar manipulimi online dhe taktikat e dezinformimit që kanë ndodhur në proceset zgjedhore në 18 vende.[34]

4. Spiunazhi kibernetik ekonomik

Shtetet, gjithashtu përveç kompanive, përdorin spiunazhin industrial (ekonomik) për të siguruar një avantazh gjeoekonomik. Spiunazhi kibernetik për motive ekonomike

[27] Alina Polyakova et al., The Kremlin's Trojan Horses 2.0 (Washington DC: The Atlantic Council, November 15, 2017

[28] Elvis Chan, Cyber Security: Espionage and Social Networking, FBI, https://www.law.berkeley.edu/wp, Korrik 2015.

[29] Item, cituar Russian former diplomat, 2017.

[30] Perluigi Paganini, 10 Biggest Cyber Espionage Cases;2017; shih edhe Dana Rubenstein, Nation State Cyber Espionage and its Impacts, https://www.cse.wustl.edu/~jain/cse571-14/ftp

[31] William C. Banks,Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage;

[32] Mark Scott,Laurens Cerulus, facebook data scandal opens new era in global privacy enforcement, Politico, Europe Edition,Mars 2018 .

[33] Yason Lewis, How spies used Facebook to steal Nato chiefs' details, The Telegraph, 10 mars 2012.

[34] Sanja Kelly, Mai Truong, Adrian Shahbaz, Madeline Earp, Jessica White, Freedom on the Net 2017. Manipulating Social Media to Undermine Democracy (Washington DC: November 2017).

po njeh rritje dhe ka shkaktuar dëme të pallogaritshme. Kompanitë private dhe qeveritë, shpesh nuk raportojnë humbjet dhe në shumë raste nuk janë në gjendje të zbulojnë sulmet. Por, edhe kur arrijnë të zbulohen rastet e spiunazhit kibernetik, informacioni mbi ta mund të mbahet sekret për shkak të frikës nga dëmtimi i markës dhe/ose i reputacionit, dhe humbja e besimit të publikut. Kufijtë kombëtarë do të pengojnë spiunazhin ekonomik më pak se kurrë, përderisa më shumë biznese zhvillohen nga kudo që mund të ketë qasje në internet[35]. Si aktor kryesor, global, shtetëror, në këtë drejtim, është Kina, e cila ka ndërmarrë sulme kibernetike për të siguruar avantazh teknologjik/ekonomik[36]. Sipas raporteve qeveritare amerikane, sektori i energjisë, financiari, i IT-së dhe ai industrial janë sulmuar disa herë[37]. Ndërkohë edhe vetë Kina ka qenë objekt i sulmeve të tilla, por shumica janë ndërmarrë nga rrjete kriminale kundër bizneseve kineze[38]. Numri i korporatave viktimë nënvizon një prirje shqetësuese. Biznesi i vogël, gjithashtu, është një objektiv tërheqës, për shkak të mungesës së mekanizmave mbrojtës. Gjatë vitit 2017, rreth 43% e sulmeve kanë synuar bizneset e vogla[39].

Në këndvështrim të spiunazhit ekonomik mund të dallohen dy skenarë: (1) vjedhje informacioni sensitiv për t'ia shitur ofertuesit më të lartë; (2) përhapjen e viruseve për të vjedhur kredencialet e një përdoruesi për platformat bankare dhe të pagesave[40]. Biznesi po lulëzon për krimin kibernetik dhe gjithkush duhet të dijë për këtë fenomen[41]. Spiunazhi kibernetik ka kosto të madhe ekonomike, ndodh në të gjitha vendet e botës, pavarësisht sasisë, dëmit të shkaktuar, efektet janë të njëjta. Sipas *Microsoft*, kostoja e krimit kibernetik globalisht shkon rreth 500 miliardë dollarë[42]. Çdo shtet me informacion me vlerë në ekonominë globale mbetet shënjestër e spiunazhit kibernetik ekonomik e industrial.

5. Disa tipa e shembuj të njohur spiunazhi kibernetik

Sot shtetet përdorin lloje të ndryshme sulmesh për motive spiunazhi kibernetik. Ndër sulmet/viruset më të përdoruara të evidentuara janë sulme të tipit *DDoS*, viruset *Trojan horses.* Ndër raste sulmesh me impakt të madh janë raportuar "*Logic Bombs, Gauss Flam, DuQu, Moonlight Maze*, *Red October* etj[43]. Virusi i famshëm *Stuxnet* (2010), rezultoi shumë i sofistikuar edhe sepse ishte i pari sulm kibernetik madhor që mund të dëmtonte dhe godiste rëndë botën fizike dhe digjitale[44]. *Titan Rain*, (2003-2005), ndodhi për 20 minuta dhe në një ditë të vetme, konsiderohet si më i gjeri në historinë e spiunazhit kibernetik, i aftë për të shënjestruar profile të larta. Sulmi rriti

[35] *Randolph A. Kahn, Economic Espionage in 2017 and Beyond, Business law today magazine,May 2017.*
[36] Freeman, K. (2014). Game Plan: How to Protect Yourself from the Coming Cyber-Economic Attack Regnery Publishing. Gandhi, R, p. 80.
[37] William Van , Ellen Nakashima,Report ties cyberattacks on U.S. computers to Chinese military,The Washington Post, February 19, 2013.
[38] Nir Kshetri, Cybersecurity and Development, Markets, Globalization & Development Review, Article 3, 2016.
[39] Mat Mansfild, Technology trends, Small business review, 2017.
[40] Pierluigi Paganini, citim nga Uri Rivner, New Opportunities for Cyber Espionage and Cyber Crime, Internet and enterprise security news, insight and analisis magazine, 2012.
[41] Rik Ferguson, drejtor i hulumtimit dhe komunikimit të sigurisë, Trend Micro.
[42] Microsoft trend analytics, https://www.trendmicro.com.
[43] Murdoch Watney , The Way Forward in Addressing Cybercrime Regulation on a Global Level, Journal of Internet Technology and Secured Transactions (JITST), Volume 1/3, September 2012, f. 73.
[44] Dana Rubenstein, Nation State Cyber Espionage and its Impacts, htp://www.cse.wustl.edu/~jain/cse57114/ftp/cyber_espionage/index.html. Hakerat thyen rrjetet e Bazës së Forcës Ajrore Wright Patterson. Rusia u akuzua për këtë sulm por nuk u konfirmua me prova. Virusi i përdorur gjatë operacionit është akoma i përdorur gjërësisht në sulmet moderne.

nivelin e ndërgjegjësimit ndaj spiunazhit kibernetik. *GhostNet* (2009), ndërhyri në mijëra kompjuterë në 103 vende. *Night Dragon* (2011), ku origjinarët hynë në harta topografike mbi rezerva të fuqishme nafte. *Shady RAT,* goditi më shumë se 70 kompani dhe organizata, që prej vitit 2006. Viktimat përfshinë edhe Komitetin Olimpik ndërkombëtar disa muaj para lojërave olimpike (2018) në Beijing[45]. *Operacioni Aurora* (2010), i zbuluar publikisht nga *Google*, mendohet se kishte filluar në mes të vitit 2009 e vazhdoi deri në fund të vitit[46] etj.

Shembuj spiunazhi kibernetik ka njohur edhe rajoni ynë. Gjatë krizës në Kosovë, NATO-ja u përball me incidentet e saj të para të rënda të sulmeve kompjuterike. Kjo çoi, midis të tjerash, në bllokimin disaditor të llogarisë së postës elektronike të Aleancës për vizitorët e jashtëm dhe në ndërprerje të përsëritura të faqes së internetit të NATO-s[47]. Në Malin e Zi ka pasur raportime për sulme kibernetike ndaj rrjeteve shtetërore dhe medieve pro qeveritare[48]. Faqet zyrtare dhe infrastruktura digjitale u sulmua në ditën e zgjedhjeve parlamentare në 16 tetor dhe mediet spekuluan për hakera rusë të lidhur me sulmet[49].

Spiunazhit kibernetik mbetet i pazbuluar për një kohë të gjatë. Në disa raste, hakerët kanë arritur të vjedhin dokumente mjaft të ndjeshme për vite me radhë, duke ndryshuar mënyrën operative me kalimin e kohës. Niveli i sofistikimit të sulmeve, objektivat e zgjedhur dhe aftësitë e treguara nga sulmuesit puqen me angazhimin e një qeverie të huaj. Për më tepër, ekspertët e sigurisë besojnë se në shumë raste, fushatat e spiunazhit janë të lidhura me njëra-tjetrën.

6. Përfundime dhe rekomandime

Ndër karakteristikat kryesore që konturojnë përdorimin e hapësirës kibernetike për motive spiunazhi kibernetik, mund të përmblidhen në: (1) *hapësira online tashmë po shndërrohet terreni i aktivitetit të krimit dhe spiunazhit.*(2) *po bëhet më i sofistikuar, më i efektshëm, më profesional;* (3) *po shndërrohet në një mjet të pranuar si të preferuar lufte,* por kjo s'do të thotë që do zëvendësojë mjetet tradicionale të luftës, por po afekton realisht natyrën e konflikteve; (4) po përdoret nga shtetet/shërbimet e tyre të inteligjencës, *me nivele rritje dhe impakt në sigurinë ndërkombëtare e kombëtare*, për realizimin e synimeve sa të vjetra aq dhe të reja;(5) mbetet *kërcënimi më i vështirë për t'u detektuar* në ambientin e sotëm të sigurisë.

Rajoni ynë vijon të mbetet *një betejë influencash.* Përveç aktivitetit me format klasike të spiunazhit, operacionet mediatike të Rusisë janë zgjeruar, si p.sh. me shërbimet e reja të Sputnik dhe platforma të tjera. Kina, përmes platformës '16+1' ka ofruar rreth 10 miliardë euro investime infrastrukturore, për ta lidhur rajonin me iniciativën "One Belt One Road", e një sërë projektesh infrastrukturore të rëndësishme në rajon që ngrenë shqetësimin për sigurinë kibernetike[50]. Synimet e aktorëve globalë, kundërshtarë

[45] Marcell Gogan, How to Prevent Attacks on These 7 Most Vulnerable Connected Toys, Techspective review, news and analysis, 12 shkurt 2018.

[46] Google zbuloi se sulmet e sofistikuara e kishin origjinën në Kinë, konsistonin në përmasat e një sulmi kërcënues të vazhdueshëm. Sulmet kishin për qëllim dhjetra organizata që vepronin në sektorë të ndryshëm, përfshir Adobe Systems, Juniper Networks, Yahoo, Symantec, Northrop Grumman, Morgan Stanley dhe Dow Chemical.

[47] Revista e NATO-s, https://www.nato.int/docu/review/2011/ABOUT/AL/index.htm.

[48] Montenegro on Alert Over New Cyber Attacks, BalkanInsight, 22 shkurt 2017.

[49] Ben Farner, Montenegro asks for British help after cyber attacks in wake of 'Russian-backed coup plot, The telegraph; 28 shkurt 2017.

[50] EPSC Brief,Engaging with the Western Balkans An Investment in Europe's Security, European politicla strategy center,European Commission, f. 3.

të orientimit properëndimor të rajonit, nëpërmjet spiunazhit kibernetik dhe jo vetëm, janë gati të dëmtojnë proceset integruese euroatlantike, të influencojnë zhvillime politike sipas interesave të tyre, të përçajnë vendimmarrjen kombëtare në raport me organizma ndërkombëtare, të nxisin nacionalizmin/ekstremizmin dhe t'i amplifikojnë ato, si dhe të krijojnë avantazhe ekonomike etj.

Si hapa për kundërpërgjigje, e rëndësishme është:

(1) *Të kuptohet/identifikohet nga vjen kërcënimi*, analizimi i kontekstit të kërcënimeve ndaj sigurisë kombëtare, që mundëson identifikimin e aktorëve shtetërorë potencialë dhe shkallën e riskut;

(2) *Zbulimi i motivit.* Arsyet kur është i përfshirë një shtet variojnë, nga përfitimi i një avantazhi strategjik (politik, ekonomik, ushtarak), deri tek shkatërrimi i një rrjeti kompjuterik, ripublikimi i të dhënave nga aktorë të tjerë, edhe mediatikë, për të ndikuar në një zhvillim apo perceptimin e publikut mbi politika të caktuara të brendshme, dhe në raport me organizatat ndërkombëtare e marrëdhëniet ndërshtetërore. *Motivi ndihmon shpesh në të kuptuarin e metodologjisë.*

(3) Përveç adresimit specifik të duhur ligjor, ka shumë rëndësi *fokusimi tek mjetet mbrojtëse dhe parandalimi për të minimizuar impaktin.*

(4) Nevojitet *ndërgjegjësim*, i të gjithë aktorëve shtetërore e jo shtetërorë, mediatikë e publikut, *për shkallën, nivelin e kërcënimit, metodologjitë e përdorura* për të mos rënë prè e spiunazhit kibernetik. Një ndërgjegjësim më të madh për interesat e aktorëve shtetërorë si Rusia, Kina, Irani etj, me interesa në rajonin tonë, që po penetrojnë edhe në fusha jotradicionale të sigurisë si siguria kibernetike.

(5) *Reagime në nivel politik e diplomatik,* në momente të caktuara, për të përcjellë mesazhin se një aktivitet i tillë monitorohet nga institucionet e sigurisë dhe në këndvështrim politik shtetëror është i patolerueshëm (si rasti i përzënies së diplomatëve rusë në disa vende të botës, përfshi 2 raste në vendin tonë; viti 2018).

(6) Sigurimi i një sasie më të madhe njohurish, si në sektorin publik edhe në atë privat që mund të jenë në rrezik nga spiunazhi kibernetik. Ata që zhvillojnë sisteme të reja duhet të mendojnë *që siguria është në qendër të vëmendjes,* që në fillim të hedhjes së idesë për një objekt të caktuar.

(7) *Krijimi i kapaciteteve neutralizuese dhe mbrojtëse.* Zhvillimi i shpejtë i shërbimeve *online* në Shqipëri, po sjell me vete edhe rrezikun e sulmeve kibernetike. Marrja e *masave të duhura mbrojtëse* në përshtatje me metodologjinë në evoluim, *përditësimi i procedurave,* duke testuar në mënyrë efektive sigurinë e sistemeve.

(8)Aderimi, adoptimi i konventave, dokumenteve strategjikë në nivele të OKB-së, BE-së, KE-së, NATO-s, OSBE-së[51], që lidhen me sigurinë/mbrojtjen kibernetike dhe dokumentet kombëtare[52], duhen *mbështetur me kapacitete konkrete e të mirëfinancuara*.

(9) *Rritje e bashkëpunimit me partnerë* për trajnim/krijim kapacitetesh njerëzore e teknologjike.

(10) *Përditësimi i kurrikulave* arsimore dhe të trajnimeve të institucioneve të administratës mbi sigurinë kibernetike.

[51] UN Framework on Cybersecurity and Cybercrime 2013; UN System Internal Coordination Plan on Cybersecurity and Cybercrime in 2014;Konventa e Budapestit, Konventa Lanzaroe, Konventa e KE(CETS no.108), Axhenda dixhitale për Evropën (DAE), NATO cyber defence; Strategjia e sigurisë kibernetike e BE, smart grouth Europe 2020 etj

[52] Strategjia e Sigurisë Kombëtare (2014);Strategjia për Sigurinë e Informacionit (2008-2013); Strategjia për Mbrojtjen Kibernetike 2018-2020 etj.

Bibliografia

1. Akhgar, B., Staniforth, A., & Bosco, F. (2014), *Cyber crime and cyber terrorism investigator's handbook* (1st ed.),
2. Brenner, S. (2010). *Cyber threats* (1st ed.). Oxford: Oxford Univ. Press.
3. *Britain to enter 'new era of online opportunity'*. (2017).
4. Freeman, K. (2014). *Game Plan: How to Protect Yourself from the Coming Cyber-Economic Attack* (1st ed., p. 80). Regnery Publishing.
5. Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, (2011). *Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political*.
6. Fred Kaplan (2016), *Dark territory The secret history of cyber war*.
7. Ted Fair, Michael Nordflet, Eric Cole, (2005). *Cyber spying*,
8. Richard A. Clarke, Cyber war, (2010).*The next threat to national security and what to do about it*.
9. National Cyber Security Centre (2016). *Common cyber attacks: reducing the impact*. National Cyber Security Centre publication
10. SANS Institute publication (2003). *Federal Intrusion Detection, Cyber Early Warning and the Federal Response*.
11. Rusell Buchan (2018). *Cyber Espionage and International Law*.
12. Alina Polyakova, et. al, (2017). *Kremlin's Trojan Horse*. Atlantic Council, Eurasia Center.
13. EPSC Brief,*Engaging with the Western Balkans An Investment in Europe's Security*, European political strategy center,European Commission.
14. Murdoch Watney , "The Way Forward in Addressing Cybercrime Regulation on a Global Level", *Journal of Internet Technology and Secured Transactions* (JITST), Volume 1, Issue 3, September 2012.
15. Konferenca *Sfidat e Sigurisë Kibernetike në Shqipëri* , Fondacioni Friedrich Ebert, "Qendra shqiptare për një qeverisje të mirë", Tiranë.
16. "Krimi kibernetik – sfidë për shoqërinë e sotme" (*2016), Revista shkenca dhe jeta*.
17. Nertil Bërdufi, *Krimi kompjuterik, strategjia dhe siguria kombëtare,* Doktoraturë, UT.
18. Denning, *Some Aspects of Theft of Computer Software,* Auckland University Law Review, Vol. 4, 1988.
19. Schmidt, "Legal Proprietary Interests in Computer Programs: The American Experience", *Jurimetrics Journal*, Vol. 21, 1981.
20. EPSC Brief, *Engaging with the Western Balkans An Investment in Europe's Security*, *European politicla strategy center*, European Commission.
21. Marcell Gogan, *How to Prevent Attacks on These 7 Most Vulnerable Connected Toys, Techspective review, news and analysis*, 12 shkurt 2018.
22. Strategjia e Sigurisë Kombëtare (2014).
23. Strategjia për Sigurinë e Informacionit (2008-2013).
24. Strategjia për Mbrojtjen Kibernetike (2018-2020).
25. Direktiva 2013/40/EU mbi sulmet kundër sistemeve informative.
26. Vendim nr. 973, datë 2.12.2015 për miratimin e dokumentit të politikave për sigurinë kibernetike 2015-2017.
27. Ligji nr. 8888, dt. 25.4.2002 "Për ratifikimin e Konventës për Krimin në fushën e Kibernetikës".
28. Ligji nr. 9880, datë 25.2.2008 "Për nënshkrimin elektronik".
29. Ligji nr. 9887, datë 10.3.2008, ndryshuar me ligjin nr. 48/2012 "Për mbrojtjen e të dhënave personale".
30. Ligji nr 8457, datë 11.2.1999 "Për informacionin e klasifikuar 'Sekret shtetëror'".
31. https://www.gov.uk/government/ Cert-UK. (2015). Common Cyber Attacks: Reducing The Impact.
32. http://www.nato.int/cp,Cyber defence. (2017). NATO. 25 April 2017.
33. Veronika Prochko, *The international legal View of espionage*, 30 march 2018; -e-international relations students.
34. Tirana Post (2017). *Siguria kibernetike, si humbën bizneset shqiptare 2.5. milionë euro nga sulmet online*, 2 mars 2017, Gazeta Tirana Post.
35. https://www.nato.int/docu/review/2011/ABOUT/AL/index.htm-Revista e NATO-s.
36. Krimi kibernetik dhe siguria kibernetike në Shqipëri: Sfidat e reja në kuadër të procesit të integrimit, e-European Movement Albania;
37. Dana Rubenstein, *Nation State Cyber Espionage and its Impacts*, http://www.cse.wustl.edu/~jain/cse57114/ftp/cyber_espionage/index.html.


AKADEMIA E SIGURISË
AS
1971

Krimi kibernetik dhe menaxhimi i tij – qasja shqiptare

■**Dr. Fejzi LILA**
Kolegji ISPE, Prishtinë
fejzilila@gmail.com

Abstrakt

Aktualisht krimi kibernetik përbën një nga sfidat më të mëdha të shoqërive në zhvillim ku aktualisht ndodhet edhe shoqëria shqiptare. Zhvillimet në teknologjinë e komunikimit dhe zgjerimi i përdorimit të internetit, veçanërisht në dekadat e fundit, kanë sjellë një evoluim dhe hapje ndaj fenomeneve pozitive dhe negative të përdorueseve. Statistikat aktuale mbi përdoruesit e internetit theksojnë se në nivel global rreth 4.5 miliard njerëz janë online. Hapësira kibernetike përbën sfidë të madhe shoqërore, ndikon në shfaqjen një formave të tjera të krimit nga qasjet tradicionale deri tek ato të panjohura aktualisht. Mjedisi, risitë e internetit dhe komunikimit bëjnë të mundur fushës së kibernetikës dhe përdorueseve të saj të krijojnë raport me individët, pronën, organizatat dhe shoqëritë. Referuar sfidave, hapjes globale ndaj këtyre fenomeneve të shoqërisë shqiptare kërkon rikonceptim të përgjithshëm dhe përshtatje më të shpeshta si pjesë e Strategjisë së Sigurisë Kombëtare. Realiteti shqiptar ndodhet në evoluim e sipër dhe kërkon agjenci funksionale, struktura ligjzbatuese dhe bazë bashkëkohore ligjore, kapacitete njerëzore e strategji të qarta. Këto masa, reflektuar në Strategjinë Kombëtare dhe atë kibernetike, janë më pak pjesë e qasjeve të brendshme tradicionale kombëtare, dhe më tepër të alternuara me qasjet e jashtme, referuar qasjeve akademike dhe partnerëve ndërkombëtarë, veçanërisht ndaj BE-së, NATO-s dhe SHBA-së. Në dekadat e fundit, realiteti shqiptar po ballafaqohet me përpjekje të drejtuara e të qëllimshme, për të përfituar akses, manipulim, ndërhyrje, dëmtim të integritetit dhe konfidencialitetit nga individë apo subjekte pa autoritet ligjor të drejtë për ta ushtruar. Menaxhimi i krimit kibernetik ngre mjaft dilema. Këto dilema lidhen me objektin referues: shtetin dhe individin. Shteti, si qasje tradicionale dhe territoriale, ndërsa individi si subjekt i lirisë, aksesit dhe të drejtës së ushtrimit e të përfitimit nga teknologjia e risitë informative. Sfida kibernetike lidhet me raportin e shtetit me mbrojtjen e shtetarëve të vetë, dhe me mbajtjen e përgjegjësive për të parandaluar, për të reaguar dhe për të rindërtuar.

Fjalëkyçe:
krimi kibernetik dhe menaxhimi, siguria kombëtare, hapësira kibernetike, shoqëria shqiptare dhe legjislacioni.

1. Hyrje

Shoqëria shqiptare është duke u përballur me problematika të reja e të papërjetuara më herët, ku mjaft qytetarë e kanë humbur besimin në kapacitetin e institucioneve politike në të gjitha nivelet për trajtimin e menaxhimin e këtyre sfidave. Realiteti shqiptar në raport me arritjet e BE, konkretisht me politikat mbi integrimin evropian është në mëdyshje e disbalancë, referuar lëvizjes së lirë dhe kufijve të brendshëm e të hapur të këtij unioni. Ballafaqimet e këtij realiteti në ndryshim e evoluim, të shoqëruara me risitë e internetit dhe komunikimit, u bëjnë të mundur përdoruesve të tij, të krijojnë raport me individët, pronën, organizatat dhe shoqëritë. Këto ballafaqime përmbajnë dilema që lidhen me objektin referues: shtetin dhe individin; shtetin si qasje tradicionale dhe territoriale, ndërsa individin si subjekt i lirisë, aksesit dhe të drejtës së ushtrimit e të përfitimit nga teknologjia e risitë informative.

Faza aktuale si kandidat potencial për në BE, në të cilën po atakohet shoqëria shqiptare, me përgatitjen e kapaciteteve, infrastrukturës, legjislacionit për hapjen e negociatave me këtë organizatë ndërkombëtare, kërkon që të ketë qasje më të mirë të mallrave dhe shërbimeve digjitale, infrastrukturë të besueshme me shpejtësi të lartë dhe marrjen e përfitimeve në maksimumin e ekonomisë digjitale. Interneti dhe teknologjia digjitale (TIK) po e transformojnë botën. Strategjia për tregun e vetëm digjital u propozua nga Komisioni Europian (KE) në maj të vitit 2015 e në vazhdimësi, strategji e cila përmban një mori veprimesh që duhet të arrihen, si: "Ofrimin e një qasje më të mirë interneti mbi mallrat dhe shërbimet digjitale; njohje dhe kontroll rigoroz të rregullave për të gjitha shërbimet digjitale, aplikacionet, përmbajtjet, disponueshmëri e shpejtësi të lartë dhe infrastrukturë e sigurt; maksimizim potenciali të zgjerimit të

ekonomisë digjitale me investime në infrastrukturën e TIK-ut"[1]. Kjo agjendë europiane, përqafuar nga shoqëria shqiptare dhe institucionet përkatëse vendimmarrëse, mbi punësimin, zhvillimin, drejtësinë dhe ndryshimeve demokratike, do të ndikojë në shërbime më të mira publike, në akses dhe performancë më të mirë digjitale për qytetarët shqiptarë, drejt një "shoqërie gjithëpërfshirëse"[2].

E ardhmja do të varet nga teknologjia, informacioni dhe komunikimi (TIK). Sistemet digjitale aktualisht janë nyje të funksionimit dhe mbijetesës së shtetit, shoqërisë dhe sipërmarrjeve të ndryshme nacionale e më gjerë. Këto sisteme me informacionet që përcjellin, krahas risive pozitive, kanë dhe potencialin për të sjellë shkatërrimin e tyre. Shkeljet e raportuara të sigurisë së informacionit dhe trendi i viteve të fundit mbi kërcënimet kibernetike, po rriten me 50-52% çdo vit. Ekspertët e sigurisë së sipërmarrjeve publike e private hedhin termin "fatalitet" ose "shkelje digjitale", ndërkohë që krimi kibernetik vazhdon të rritet. Rreziqet janë të kufizuara, shpërblimet potenciale janë të larta, sponsorizimi i qeverisë për krimin kibernetik me mbështetje financiare janë jo të mjaftueshme. Sipas anketave të fundit për sigurinë e informacionit global, organizatat e ndryshme ndërkombëtare dhe shtetet, si subjekt të marrëdhënieve ndërkombëtare, përpiqen të japin përgjigjen e duhur ndaj rreziqeve në rritje të krimit kibernetik, por e kanë të vështirë të harmonizojnë strategjitë e tyre të sigurisë me strategjitë ndaj krimit kibernetik në botën reale.

Shumica e këtyre aktorëve, si shtetërorë dhe privatë, si ata me qasje nacionale, rajonale e më gjerë, pranojnë se përgjegjësia për shmangien e sulmeve kibernetike nuk mund të shuhet më në departamentet e IT-ve. Kjo është një çështje më e gjerë: përfshirje e bordeve vendimmarrëse, si mënyra më e sigurt për të kundërshtuar kërcënimin kibernetik, me një qasje strategjike me rrënjë sigurinë digjitale në botën reale të mirëfunksionimit aktual, dhe bazë për të ardhmen. E rëndësishme është që të ndihmohen anëtarët e bordit dhe vendimmarrësit, në nivele të ndryshme menaxhimi, që të kuptojnë marrëdhëniet midis përgjegjësive, shkallës së kërcënimit kibernetik dhe një qasje të sugjeruar e të fokusuar në strukturën, kulturën dhe rreziqet e pritshme.

2. Rritja eksponenciale e rrezikut të krimit kibernetik

Rreziqet në rritje të sigurisë kibernetike, do të shkojnë paralelisht me rëndësinë e qëndrimit përpara krimit kibernetik. Kërcënimet për sigurinë kibernetike evoluojnë me shpejtësi, paraqesin kompleksitet dhe ndikim të pashembullt. Organizatat, sipërmarrësit, shoqëria shqiptare përgjithësisht nuk po pyesin "a jemi të sigurt?", por "si mund të sigurojmë që informacioni më i rëndësishëm për mirëfunksionimin tonë do të jetë mjaft i sigurt?". Të dhënat aktuale na japin një mënyrë e re të së parit të peizazhit nacional e global; një natyrë kritike të së dhënave, në pothuajse çdo aspekt të ndërmarrjes moderne dhe nga ana tjetër, ngritjen e kriminelëve kibernetikë që kërkojnë ta minojnë atë. Këta aktorë të brendshëm e të jashtëm, në të gjithë sektorët, po përballen jo thjesht duke shkallëzuar rrezikun, por po përjetojnë sigurinë që do të vuajnë nga shkeljet e sigurisë së informacionit.

Në fakt, realiteti i ashpër i mjedisit të sotëm të sigurisë, do të thotë se ka të ngjarë të ketë përjetime tashmë të dy lloje subjektesh: ata që janë shkelur dhe e dinë, dhe ata që

[1] https://eeas.europa.eu/sites/eeas/files/ten-priorities-for-europe.pdf
[2] http://ec.europa.eu/priorities/digital-single-market/index_en.htm

mbeten të rrezikshëm e kontingjent potencial për këtë. Ky rishikim radikal mbi sigurinë e krimin kibernetik, është një thirrje zgjimi që duhet të rezonojë rreth tryezave politikëbërësve dhe vendimmarrësve. Krimi kibernetik, paraqet rrezikshmëri mbi: pronën intelektuale; të dhënat e klientëve; të dhënat operative dhe financiare; mashtrimet dhe mbi reputacionin organizativ. Lidershipi politik dhe ai administrativ, janë të informuar e po e kuptojnë, se është koha për një rishikim themelor të sigurisë së informacionit, qasje ndaj krimit kibernetik dhe pozicionim brenda organizimeve të tyre. Eksperienca po tregon se nuk është e mjaftueshme për ta trajtuar atë si një funksion të IT (qasje teknike), ndërkohë që ekspertiza e sistemeve mbetet thelbësore mbi gatishmërinë, vetëm kur siguria kibernetike kuptohet brenda strukturës së përgjithshme të menaxhimit të rrezikut të organizatës. Lidershipi ekzekutiv mund të ketë besimin, se pasuria e vetme më e rëndësishme, që është informacioni, dhe indicjet e mjaftueshme për t'u mbrojtur nga kërcënimet e sotme e në zhvillim që mund të shkaktojnë dëme potencialisht katastrofike, mund ta bëjnë një ditë një viktimë të organizimit në internet. Njohja dhe mbrojtja më e mirë mundëson një performancë efektive dhe rrit aftësinë e të vepruar çdo ditë; demonstron qëndrueshmëri përballë kërcënimeve të vazhdueshme e në zhvillim.

1.1 Spektri i kërcënimit të krimit kibernetik

Natyra e sigurisë së krimit kibernetik vështrohet nga dy perspektiva: nga kërcënimet e brendshme dhe të jashtme. *Kërcënimet e brendshme* rrjedhin nga gabimet e thjeshta si: humbja e përdoruesve, humbja e pajisjeve mobile, qëllimi i keq për mashtrim ose vjedhja e të dhënave. Ndërsa mbështetet produktiviteti përmes integrimit të shpejtë të sjelljes së pajisjes suaj (BYOD), *cloud-computing* dhe aspekte të tjera të lëvizshmërisë totale, ekziston një rritje korresponduese me rrezikun në të cilin informacioni i vendosur, ose i qasur nëpërmjet këtyre kanaleve, është i ekspozuar. Jo vetëm që qasja e pandarë e këtyre sistemeve prodhon dobësi, por ato gjithashtu kërkojnë procese gjithnjë e më komplekse të integrimit. *Kërcënimet e jashtme* sillen nga hakerët, të cilët sot janë të mirëfinancuar, të vazhdueshëm dhe të sofistikuar. Njerëzit dhe proceset, janë gjithnjë e më shumë një objektiv, njëlloj si teknologjia. Kriminelët kibernetikë janë të motivuar dhe evoluojnë shumë më shpejt, ndërkohë që mbrojtja duhet të jetë njëlloj e shkathët e me të njëjtin ritëm.

Kërcënimet nga krimi kibernetik kanë zhvillim të shpejtë, shumëdimensional dhe ekzistojnë në të gjithë sektorët jetësorë. Spektri i saktë i rrezikut ndryshon në sektorë të ndryshëm. Ajo që kërkohet është vlerësimi i të dhënave në aftësinë e organizatës për lulëzim, sesa në performancën e rrjetit apo platformës. Korniza e sigurisë së një organizate mund të jetë e mjaftueshme për sektorin e saj origjinal ose gjeografinë, por zgjerimi dhe ekspozimi kërkon që masat e sigurisë të rishikohen hap pas hapi."Nuk është thjesht se shpejtësia dhe kompleksiteti i ndryshimit po përshpejtohen, por ashpërsia e ndikimit po ngjitet lart. Hendeku i aftësisë së një organizate, në menaxhimin e ritmit të ndryshimit, është një problem, por rreziqet për të mos e mbushur atë, janë më serioze se kurrë më parë"[3].

1.2 Rreziku kibernetik në projeksion rritje me përparimin teknologjik

Sipërmarrjet publike e private në të gjithë sektorët dhe hapësirat gjeografike, janë të

[3] Mike Trovato, EY Asia-Pacifc Security Practice Leader © 2013 EYGM Limited.

varura nga sistemet e informacionit e teknologjitë që u mundësojnë atyre zhvillim, por çdo përparim teknologjik është edhe po aq i rrezikshëm. Ndërkohë që ndryshimi teknologjik qarkon momentin dhe informacioni bëhet më kritik për aktivitetet e fundit, shpejtësia dhe ashpërsia e kërcënimeve të sigurisë intensifikohen. Sasia e madhe e hulumtimeve globale mbi mbizotërimin e krimit kibernetik zbulon se rreziku i një sulmi kibernetik është në rritje nga risia teknologjike, pasi hakerët bëhen gjithnjë e më të sofistikuar, më të shkathët dhe më të mirëfinancuar. Gjetjet kyçe në anketën globale të sigurisë së BE-së, tregojnë një shqetësim në rritje lidhur me rrezikun nga kërcënimet e jashtme, në raport me rrezikun nga kërcënimet e brendshme, dhe pothuajse një e treta e të anketuarve (31%), raporton se nuk ka programe inteligjence për kërcënimet, për të zbuluar se ku janë apo nga ku mund të vijnë sulmet kibernetike[4]. Pak më shumë se një e treta e të anketuarve, pohojnë se kanë vetëm një program joformal dhe shumë prej tyre mbeten shqetësues e të ngadaltë, për ta parë sigurinë e informacionit si një rrezik që meriton angazhimin e plotë të drejtuesve të nivelit të lartë.

Referuar angazhimit të nivelit të lartë në sigurinë kibernetike, hulumtimet mbi pronësinë e sigurisë së informacionit tregojnë mospërshtatje të strategjisë së sigurisë kibernetike me strategjinë e përgjithshme kombëtare. Një pjesë, ka përshtatur dhe harmonizuar strategjinë e IT-së, me "oreksin" e riskut të organizatës ose me tolerancën se, buxheti i tyre i sigurisë së informacionit, është rritur, por mbetet ende i paplotësuar[5].

1.3 Tipologjia e krimit kibernetik dhe evoluimi i tij

Drejtori i Europolit, Rob Wainwright, shprehet se: "Rritja e pamëshirshme e krimit kibernetik, mbetet një kërcënim i vërtetë dhe i rëndësishëm për sigurinë tonë kolektive në Evropë. Europol është i shqetësuar për mënyrën se si një komunitet në zgjerim kibernetik, është në gjendje të shfrytëzojë më tej varësinë tonë në rritje, nga teknologjia dhe interneti"[6]. Kërkesa për siguri kibernetike shtrihet në një kohë të gjatë, ndërsa kriminelët kibernetikë vazhdimisht kërkojnë mënyra të reja për t'ju kundërpërgjigjur. Lufta ndaj krimit kibernetik duhet të vazhdojnë me intensitet dhe ta përshtatë reagimin sipas prirjeve të këtyre sulmeve. Në fillimet e para të dekadës së dytë, të viteve 2000, mbizotëronin këto prirje të krimit kibernetik[7]:

1. *Kriminelët kibernetikë me qasje ndërkombëtare e bënë të vështirë gjetjen dhe ndalimin e aktiviteteve të paligjshme të tyre*. Ky trend ekspozoi mungesën e bashkëpunimit ndërkombëtar, shitjen e të dhënave të korporatave dhe tregtimin e informacionit duke sjellë formimin e një "mafie kibernetike" - një rrjet i gjerë ky, që përfshiu e goditi mjaft vende. Pengesa më e madhe për të mposhtur këto qarqe ndërkombëtare të krimit kibernetik, u bënë vetë qeveritë e këtyre vendeve. Mungesa e bashkëpunimit të këtyre qeverive, çoi në krizë reagimi ndaj këtij problemi në rritje.

2. *Aksesi në rritje i shoqërisë në medien sociale krijoi mundësi për sulme kibernetike* me forma nga " spear phishing", sulmet e dizajnuara e deri tek të vjedhurit e të dhënave të një institucioni apo të një kompanie. Sulmet e inxhinierisë sociale pësuan rritje, por me një ritëm më të ngadalshëm.

3. *Sulmet e vazhdueshme e në rritje u shoqëruan me dëmtime, moszbulim dhe vjedhjen e të dhënave.* Realitetin e shfrytëzuan hakerët duke depërtuar në sisteme të

[4] *Under cyber attack: EY's Global Information Security Survey 2013*
[5] Ibid
[6] https://www.itgovernance.co.uk/blog/top-8-cyber-crime-trends-identified-by-europol/
[7] http://www.disaster-resource.com/index.php?option=com_content&vieë=article&id=1611&ltemid=141

ndryshme të enteve publike dhe kompanive, për periudha të gjata kohore, e duke shkaktuar vjedhjen e të dhënave kritike. Këto sulme synonin institucione e kompani specifike që kërkonin një mbrojtje më të avancuar se sa zakonisht dhe inspektime mbi forenzikën e rrjetit (*network forensics*).

Sipas vlerësimit nga *kërcënimi i krimit të organizuar në Internet* (IOCTA), 2016 dhe prezantimit vjetor mbi peizazhin kërcënues të krimit kibernetik nga Qendra Europiane për Krimin në Internet (EC3), konfirmohet se krimi kibernetik vazhdon të përbëjë një kërcënim të rëndësishëm në të gjithë Evropën dhe është i shoqëruar me vepra penale që tejkalojnë krimet tradicionale në disa shtete anëtare të BE-së.

Gjatë gjysmës së dekadës së dytë të viteve 2000, u identifikuan këto prirje të krimit kibernetik[8]:

1. *Krimi kibernetik si shërbim*, i cili u siguron kriminelëve kibernetikë qasje në mjetet dhe në mjediset ku mund të mësojnë, reklamojnë, blejnë dhe shesin. Falë forumeve *darknet*, *e-mail* dhe metoda të tjera të komunikimit, ofruesit e mjeteve dhe shërbimeve të krimit kibernetik janë në kontakt të drejtpërdrejtë me një numër në rritje të mashtruesve, grupeve të krimit të organizuar dhe organizatave terroriste.

2. *Ransomware ose cryptoware* janë variantet e ndryshme "malware" mbi vjedhjen e të dhënave. Kjo kategori synonte nga pajisjet e përdoruesve individualë deri tek organizatat e mëdha dhe qeveritë.

3. *Përdorimi i të dhënave nga kriminelët kibernetikë* për mashtrimet dhe sulmet *ransomware-ve* në grabitje të drejtpërdrejtë e me lehtësi, ofrohet shpejtë, sjell fitim financiar nga shitja në rrjetin e errët.

4. *Mashtrimi nëpërmjet pagesave,* duke shënjuar ATM-të, mashtrim pagesash dhe blerjeve me CNP (*card-not-present*), dhe lloje të reja të mashtrimit të pagesave që përfshijnë kartelat pa kontakt (NFC).

5. *Abuzimi seksual i fëmijëve në internet,* është përshkallëzuar me rritjen e përdorimit të platformave të shkëmbimit të koduara dhe sistemeve anonime të pagesave. Është evidentuar edhe një rritje e dukshme në transmetimin e drejtpërdrejtë të abuzimit të fëmijëve.

6. *Abuzimi me rrjetat e errëta e të fshehura* (*darknet*), ngelet vendi i preferuar i kriminelëve kibernetikë në aktivitete të paligjshme. Këto rrjete janë vendi për të gjetur mjete dhe burime të krimit kibernetik nga grupet ekstremiste.

7. *Inxhinieria sociale,* identifikoi rritje në mashtrimet "phishing", "gjueti balenash", "bulling" apo mashtrimet e CEO.

8. *Monedha virtuale,* ngelet preferencë për pagesat penale-kriminale (C2C); ajo siguron një nivel të lartë anonimiteti dhe monedhë favorizuese për pagesat zhvatëse *ransomware* ose sulmeve DDoS.

1.4 Prirjet aktuale të krimit kibernetik dhe reagimi ndaj tij

Viti që lamë pas (2017) u shoqërua me shkelje të mëdha, ku 143 milionë klientë dhe mijëra organizata kishin rrjedhje në informacioni, ndërsa periudha aktuale (2018), kërkon rregullim të rreptë dhe krijimin e roleve të reja. Siguria kibernetike është shndërruar në çështje themelore për drejtuesit e fushave të ndryshme. Pyetja shtrohet se: cilat janë prirjet dhe çështjet e sigurisë kibernetike të pritshme për 2018?[9]

[8] https://www.itgovernance.co.uk/blog/top-8-cyber-crime-trends-identified-by-europol/
[9] https://www.information-age.com/10-cyber-security-trends-look-2018-123463680/

1. *Përmirësimi i legjislacionit mbi sigurinë kibernetike.* Natyra dinamike dhe lëvizshmëria e sigurisë kibernetike i tejkalon reagimin ndaj saj, duke u bazuar në legjistacionin dhe rregulloret aktuale. Këto rregullore janë të ngadalshme, të ngathëta dhe ndikojnë në ndërtimin e një kulture papajtueshmërie e një ndjenje të rreme sigurie, përballë kundërshtarëve të shkathët, të motivuar dhe të mençur. Ne duhet të shohim përmirësim të vazhdueshëm të rregulloreve dhe mënyrës sesi do të zbatohen ato praktikisht, mbi sigurinë kibernetike.

2. *Vjedhja e të dhënave dhe manipulimi i tyre.* Sulmuesit kibernetikë dhe hakerat e internetit kanë tendencë të ndryshojnë metodologjinë e tyre të punës, nga vjedhja e pastër e të dhënave në sulmin mbi vërtetësinë e tyre. Ky lloj sulmi, në krahasim me vjedhjet e drejtpërdrejta të të dhënave, do të shkaktojë dëme afatgjata dhe, duke i bërë njerëzit, që të vënë në dyshim integritetin e të dhënave në fjalë.

3. *Kërkesa në rritje mbi aftësitë reaguese ndaj krimit kibernetik*. Një mungesë e shkathtësive reaguese të sigurisë kibernetike, ndaj këtij lloj krimi i bën organizatat objektiva më të dëshirueshme për hakimin. Rritja e kërkesës për ekspertizë do të rritet, pasi strategjitë aktuale nuk janë të mjaftueshme për reagim. Gjithashtu, sektori publik e privat gjithnjë e më tepër do të synojnë të furnizojnë nevojat e tyre të sigurisë, ku trajnimi i brendshëm dhe rritja e aftësive duhet të vazhdojnë e të përshpejtohen.

4. Gjenerata e ardhshme e *sulmeve kibernetike do të jetë mjaft dinake duke imituar sjellje të caktuara* përdoruesish, dhe duke mashtruar edhe personelin e kualifikuar të sigurisë. Kjo përfshin aftësinë e të krijuarit fusha komplekse, të besueshme për mashtrime dhe nga ana tjetër ndërgjegjësimin mbi prezencën e kësaj shkalle rrezikshmërie (Cyber Security & Internet of Things, IoT).

5. *Sulmuesit do të vazhdojnë të synojnë pajisjet e konsumit*. Gjatë vitit 2018 e në vazhdim, nga hakera ose *ransomware* do të shohim që konsumatorët e përditshëm do jenë në shënjestër në një sërë objektesh të lidhura. Ky skenar është i mundshëm, si p.sh. grabitqarët e fëmijëve që synojnë pajisjet IoT (lodra të dizajnuara për fëmijët) ose synimi i "televizionit të zgjuar" në shtëpi nëpërmjet sulmeve *ransomware* duke kërkuar nga përdoruesi që të paguajë një tarifë zhbllokimin e tij.

6. *Sulmuesit do të bëhen më të guximshëm, më komercialë më pak të gjurmueshëm*. Hakerët do synojnë të jenë më të organizuar dhe më të komercializuar. Ata do të kërkojnë të bazohen në hapësira e viktima, ku krimi kibernetik do konsiderohet e vendoset, jashtë juridiksioneve të policisë.

7. *Sulmuesit do të bëhen më të mençur*. Ky kontingjent krimi do të synojë në vazhdimësi përmirësim më të shpejtë sesa ç'janë aftësitë mbrojtësve për kundërshtim. Fushë-aktiviteti do të jetë: shfrytëzimi i rrjeteve të errëta (*Dark Web*), eksplorimi në rrjete për tu fshehur me sukses dhe komunikimi me kriminelët e tjerë.

8. *Shkeljet do të bëhen më të ndërlikuara dhe më të vështira për reagim.* Kriminelët kibernetikë do të shikojnë rritjen e aktiviteteve me qëllim të keq, duke përdorur *ransomware* gjithnjë e më të devijuara. Nëpërmjet varianteve *ransomware,* është zbuluar dhe përdorur një sistem inovativ për të rritur infektimet, ndërsa *softwear* -i i kthen viktimat në sulmues, duke ofruar një skemë të stilit piramidal.

9. *Sigurimi i rrezikut nga krimi kibernetik do të bëhet më i zakonshëm*. Ky lloj sigurimi gjithnjë e më shumë do të bëhet pjesë operacionale e strategjisë së rrezikut, ku industria e sigurimeve, duhet të përshtatë produkte specifike për nevojat e klientit. Ndërsa industria evoluon, fushë e zgjeruar ndaj sigurimit të krimit kibernetik do të jetë mbulimi i humbjes së reputacionit, i besimit të klientëve, i humbjes së të ardhurave të

pritshme, i ndikimeve negative dhe i kostove të përmirësimit të infrastrukturës së sigurisë apo përmirësimeve të sistemit.

10. *Shfaqja e autoritetit kryesor mbi krimin kibernetik me përgjegjësi të përditshme,* për mbrojtjen e sistemeve kompjuterike nga sulmet dhe parandalimin e shkeljeve, do të merrte drejtimin nëse do të kishte ndodhur një shkelje, dhe do të siguronte një lidhje të fortë midis pjesës drejtuese (bordit) dhe pjesës tjetër të sipërmarrjeve publike e private.

3. Bashkëpunimi në nivel kombëtar dhe ndërkombëtar

Momenti në të cilin ndodhet vendi ynë si kandidat potencial për në BE, kërkon adoptim me direktivat e reja të BE-së për sigurinë kibernetike. Institucionet përkatëse shqiptare në procesin e integrimit të Shqipërisë për në Bashkimin Europian, pritet të konsultohen me aktorë të ndryshëm, lidhur me kapitullin 10, "Aspekte të sigurisë kibernetike" dhe me kapitullin 24, "Krimi kibernetik dhe çështjet e sigurisë së brendshme".

Bashkëpunimi në nivel kombëtar synon bashkëpunimin me institucionet e sigurisë, partneritetin me subjektet private dhe biznesin e TI-së, për të siguruar qëndrueshmëri në infrastrukturë, siguri në rrjetet kompjuterike dhe në produktet që merren nga këto shërbime të ofruara. Siguria kibernetike në nivel kombëtar është aftësia e shteteve dhe institucioneve për të mbrojtur hapësirën e tyre kibernetike, në mënyre kolektive dhe individuale[10]. Hapësira kibernetike është një fushë në të cilën si aktorët privatë dhe ata publikë, civilë e ushtarakë, kombëtarë e ndërkombëtarë, duhet të veprojnë në të njëjtën kohë dhe të jenë reciprokisht të varur nga njëri-tjetri[11].

Bashkëpunimi në nivel ndërkombëtar, është bashkëpunim me subjektet dhe vendet, që aspirojnë dhe veprojnë në nivele të ngjashme sigurie, zhvillim të përbashkët të mjeteve, aftësive dhe teknikave, shkëmbimit të njohurive dhe eksperiencave në këtë fushë.

Vendi ynë si pjesë e NATO-s dhe qasjes drejt BE-së, vepron sipas Memorandumit të Mirëkuptimit për Mbrojtjen Kibernetike (*CDMB - Cyber Defence Management Board*) me vendet anëtare, me Zyrën Europiane të Policisë (*Europol - European Police Office)*, Qendrën Evropiane për Krimin Kibernetik (*EC3 - European Cyber Crime Centre)*, Agjencinë e Bashkimit Evropian për Sigurinë e Rrjetit dhe Informacionit (*ENISA - European Union Agency for Network and Information Security*), Agjencinë e Bashkimit Europian mbi Mbrojtjen (*EDA-European Defence Agency*). Nga këto institucione ndërkombëtare Shqipëria, njihet me ekspertizën mbi sigurinë kibernetike në Evropë, informohet, këshillohet që të përgatitet për të parandaluar, zbuluar dhe përgjigjur problemeve të sigurisë së informacionit dhe atij mbi krimin kibernetik.

Strategjia e Kibernetikës së BE-së (një Hapësirë Kibernetike e hapur dhe e sigurt) u botua bashkërisht, nga Komisioni Europian dhe Përfaqësuesi i Lartë i Bashkimit Evropian për Punë të Jashtme dhe Politikën e Sigurisë (OSBE), në vitin 2013, për të shoqëruar Direktivën e Rrjetit dhe Sigurinë e Informacionit (NIS)[12]. Kjo strategji e BE-së mbi kibernetikën, referuar qasjes franceze dhe irlandeze, sqaron parimet që duhet të

[10] Strategjia për Mbrojtjen Kibernetike | Ministria e Mbrojtjes nëntor 2014.

[11] Hapësirë kibernetike – konsiderohet hapësira virtuale globale e të gjithë sistemeve të Informacionit të ndërlidhur në nivel
global të dhënash.

[12] Traininghttps://www.itgovernance.eu/en-ie/nis_directive_training-ie

udhëzojnë politikën e sigurisë kibernetike në BE dhe në nivel ndërkombëtar. Strategjia e Kibernetikës së BE-së, shprehet me pesë prioritete strategjike: arritja e elasticitetit kibernetik; reduktimi drastik i krimit kibernetik; zhvillimi i politikave dhe aftësive të mbrojtjes kibernetike, sipas kornizës të politikës së përbashkët të sigurisë dhe mbrojtjes (PSDK), zhvillimi i burimeve industriale dhe teknologjike për sigurinë kibernetike dhe krijimi i një politikë koherente ndërkombëtare të hapësirës kibernetike për Bashkimin Evropian, dhe promovimi i vlerave kryesore të BE-së[13]. Bashkëpunimi me BE i jep mundësinë Shqipërisë, njohjen dhe eksesin, në ISO 27001 - Standardi Ndërkombëtar i Praktikës më të Mirë, Sistemin ISMS - Sistem i Menaxhimit të Sigurisë së Informacionit, Horizon 2020 - Program Kërkimi dhe Inovacionit në BE, Digital Forensics - Procesi Zbulimit dhe Interpretimi i të Dhënave Elektronike.

4. Përgjegjësia ndaj krimit kibernetik: pse siguria mënjanohet nga drejtuesit, vendimmarrësit (bordet)?

Kërkesat në rritje e konkurruese të TIK dhe një qasje e vjetruar ndaj krimit kibernetik e kërcënimeve, nxjerrin në dukje dobësitë dhe nxisin diskutimin mbi sigurinë. Drejtues të niveleve të ndryshme dhe këshillat administrativë (bordet) hezitojnë të luftojnë e të marrin masa mbi sigurinë kibernetike. Arsyet ndryshojnë nga njëra tek tjetra organizatë, por shumica kanë të rrënjosura përgjithësisht këto pengesa të rëndësishme:

- Siguria e informacionit është një nga shumë çështje të ngutshme që kërkon angazhim në nivelin drejtues e vendimmarrës, veçanërisht në një kohë të vazhdueshme paqëndrueshmërie ekonomike.

- Siguria e informacionit është menduar tradicionalisht si një çështje IT, që fokusohet më shumë në mbrojtjen e sistemeve të TI-së që përpunojnë dhe ruajnë informacionin, sesa në vlerën strategjike të vetë informacionit.

- Siguria kibernetike është parë si parësore vetëm në sektorët ushtarakë apo financiarë. Por, nëse qasja zgjerohet edhe në sektorë të tjerë, duke u mbështetet në të dhënat digjitale, për të vepruar dhe konkurruar, informacioni dhe sistemet e TIK do të jenë më të përgatitur për menaxhim të duhur të rrezikut nga krimi kibernetik.

- Ndryshe nga shumë lloje rreziqesh e problemesh organizative, kërcënimet kibernetike janë të vështira për t'u parashikuar e për të vlerësuar rreziqet dhe ndikimet e mundshme. Udhëheqësit e lartë dhe drejtuesit e niveleve më të ulëta, mendojnë se nuk kanë ekspertizën e nevojshme për vendimmarrje të plotë ose që të mund të jenë të kujdesshëm, ndaj proceseve teknike.

- Përballë kërkesave konkurruese të tregut dhe burimeve të pakta në dispozicion, mund të jetë e vështirë për lidershipin ekzekutiv të investojë para, njerëz dhe kohë në të panjohurën e paparashikueshme, sesa në drejtime apo nevojat më të dukshme.

5. Dobësitë e sektorëve publikë e privatë me rritjen e kërcënimit kibernetik dhe sigurisë së informacionit

Investimet në IT dhe në fushat e lidhura të adresuar në sigurinë kibernetike mund të keqdrejtohen. Organizatat kanë tendencë të investojnë më shumë në mbrojtjen e aseteve

[14] https://www.itgovernance.eu/fr-fr/eu-cybersecurity-strategy-fr&https://www.europol.europa.eu/partners-agreements/member-states/ireland

të IT-së, ndërkohë që investimet sipas strategjisë të natyrës së kërcënimeve, ka gjasa të prishin objektivat e balancat financiare. Pothuajse një në katër të anketuar (23%), nuk identifikon dobësitë dhe pranon natyrën e vërtetë të kërcënimeve që u shkaktojnë atyre dëmtime më të mëdha.

Dobësitë që ekspozojnë ndaj krimit kibernetik lidhen me këto kategori:

- siguria kibernetike nuk është e orientuar në raport me prioritetet organizative;
- kornizat e reagimit ndaj krimit kibernetik janë të vjetruara, jo të plota dhe mbeten më tepër të fokusuara në IT;
- zgjidhjet tradicionalisht janë mbështetur në përmirësimet e "bolt-on", PC dhe një numër të produkteve heterogjene të softuerit të sigurisë;
- linjat e llogaridhënies brenda organizatave janë të paqarta;
- analizat periodike dhe rast pas rasti janë të pakta e të papërdorura;
- organizatat globale kanë kompleksitetin e menaxhimit të sigurisë digjitale nëpër rajone ose sektorë me standarde të ndryshme, të cilat çojnë në konflikte dhe mospërputhje.

Potenciali i krimit kibernetik për "një goditje fatale" nuk ka qenë kurrë më i madh. Kërcënimet në rritje e të shpejta dhe gjithnjë e më komplekse janë të nxitura nga kundërshtarët e jashtëm ose të brendshëm, të cilat shpeshtohen nga boshllëqet sistemike. Një qasje krejtësisht e re, për të kuptuar sigurinë digjitale organizative dhe atë kibernetike, është e nevojshme për tu kundërvënë hakerëve të sotëm.

6. Ndikimet e lidershipit

Rreziqet dhe dobësitë që lidhen me teknologjitë dhe risitë digjitale të sotme shkojnë përtej mendimit konvencional mbi IT. Një sulm në internet mund të ndikojë në aftësinë e një organizate për të përmbushur detyrën e saj. Shkeljet e sigurisë janë një zbavitje e kushtueshme dhe në rastin më të keq mund të çojnë në dështime katastrofike. Në mes qëndron një gamë e gjerë e ndikimeve ndaj biznesit, që kërcënon operacionet, aftësitë prodhuese, të dhënat e klientit dhe/ose punonjësve, ekspozimin e përgjegjësisë dhe pronësinë intelektuale. Cilido mund të rrezikojë vazhdimësinë dhe integritetin e biznesit. Potenciali mbi dëmtimin e reputacionit nuk mund të ekzagjerohet, por kur bordet dhe udhëheqja e lartë nuk janë në dijeni për kontekstin e gjerë të ekspozimit ndaj rrezikut, ato mbeten në pakujdesi e të pavëmendshëm për të identifikuar dhe lehtësuar këtë ekspozim. Qasja për mbrojtjen e sipërmarrjeve publike e private duhet të kombinojë njerëzit, proceset, teknologjinë dhe lidershipin.

Suksesi i një strategjie efektive të sigurisë kibernetike qëndron në aftësinë për të parë në avancë, mundësitë dhe kërcënimet e së ardhmes. Udhëheqja politike e ekzekutive duhet të marrë në konsideratë, nëse aspektet e sigurisë të sipërmarrjeve publike e private i konsiderojnë këto çështje:

1. Si do të reagojë lidershipi politik e ekzekutiv ndaj kërcënimit në rritje të informacionit? Rreziku rregullator.
2. Cili është ekspozimi i organizatës ndaj këtyre goditjeve? Sa e vetëdijshme është organizata në IT? Goditja gjeopolitike.
3. Si do të ndikonte në reputacionin dhe emrin e organizatës sulmi kibernetik? Rreziku i reputacionit.
4. A ekzistojnë boshllëqe, dobësi nga faktorët kontribuues në sigurinë e IT? Dështimet e kontrollit.

5. Si do adresohet elasticiteti dhe rrjedhja e të dhënave nga organizata si fusha kryesore të rrezikut të sigurisë? Rreziku i informacionit.

6. A kemi rritje e zgjerim të kompanisë në sfidën e vazhdimësisë së saj? Zgjerimi e zhvillimi në treg.

7. Sa do të ndryshonte profilin përballë rrezikut të informacionit? Rikonceptim i biznesit.

8. A do të përdorte si ndihmë mbi rreziqet në rritje të sigurisë dhe IT, nga palët e treta ose nga qendrat e përbashkëta të shërbimeve ndihmuese? Qendrat e shërbimeve të përbashkëta.

9. A mundet organizata të reagojë ndaj rrjedhjeve së të dhënave, humbjeve dhe punonjësve mashtrues? Siguria e të dhënave.

10. Sa të suksesshme janë investimet e organizatës në raport me integrimin e informacioni të përfituar? Investimet dhe integrimi.

11. Hacktivist-ët janë ideologjikë nga natyra dhe mund të nxjerrin çështje si politika mbi taksat, paga dhe menaxhimi i mjedisit duke u bërë një objektiv kibernetik, - goditja e titujve.

7. Suksesi kërkon një zgjidhje potenciale përgjithësuese

Udhëheqësit duhet të aplikojnë një qasje përgjithësuese në planifikimin dhe menaxhimin e sigurisë së informacionit, fokusuar në strukturën, kulturën dhe rreziqet e organizatës (biznesit tuaj) dhe të lejojë mbrojtjen e menaxhimin e të dhënave për mbijetesë dhe suksesin e organizatës. Kjo kërkon evoluimin, mbi kuptimin e sigurisë së informacionit brenda organizatës (biznesit) drejt krijimit e aplikimit të një programi sigurie, duke analizuar kërcënimet e vazhdueshme kibernetike dhe impaktet e rreziqet në organizatë (biznes). Menaxhimi i programeve kibernetike (EY's Cyber Program Management, CPM) që identifikon mënyra për të qenë përpara krimit kibernetik, do të mbështeste elasticitetin e vazhdueshëm ndaj rrezikut. Ky program i jep përparësi një qasjeje të shumëllojshme që lidh menaxhimin e sigurisë me performancën e biznesit. Programi ofron këto objektiva:

- shtrirje me objektivat e organizatës (biznesit),
- rritje të gatishmërisë, përshkallëzimit dhe fleksibilitetit;
- aplikim në të gjitha nivelet, shkallët,
- cikël rigoroz të identifikimit dhe menaxhimit të rrezikut,
- fokusim për të parashikuar sfidat e reja.

Objektivat e këtij programi lidhin strategjinë e sigurisë me performancën e biznesit: identifikojnë rreziqet reale; mbrojnë atë që ka më shumë rëndësi; mbështesin një program ndërmarrjeje (sipërmarrje); ofron optimizëm për ecurinë e mëtejshme[14].

Qasja përgjithësuese duhet të bazohet në analizë vlerësuese. Aktualisht, në vendin tonë ndodhen shumë pak sipërmarrje publike e private, me aftësitë dhe burimet e duhura për të siguruar efektivitet maksimal të informacionit, në raport kohor, të njëjtë me objektivat e tyre, ku subjektet e të gjithë sektorëve, të mund të përfitojnë nga një vlerësim objektiv i programeve dhe strukturave të sigurisë së tyre të informacionit.

[14] https://www.ey.com/Publication/vëLUAssets/EY-cyber-program-management/$FILE/EY-cyber-program-management.pdf

"Kuadri inovativ i menaxhimit të programit të sigurisë" të KE-së është ndërtuar mbi analizën, se si siguria e informacionit, formon dhe përshtatet në strukturën e përgjithshme të menaxhimit të rrezikut të një organizate[15]. Në themel të saj janë fokusuar qartë prioritetet strategjike të organizatës dhe objektivat e biznesit. Një vlerësim i këtij programi, i ndihmon subjektet me:

- kuptimin e ekspozimit ndaj rrezikut të organizatës (sipërmarrjeve);
- vlerësimin e maturitetit të programit aktual të sigurisë së informacionit dhe identifikimin e fushave për përmirësim;
- ndërtimin e një harte prioritare mbi investimet e projektit dhe të ndryshimeve organizative;
- mbledhjen e informacionit për krijimin e standardeve në raport me organizatat e tjera;
- investimet e kryera, se sa janë vlerësuar ato dhe a kanë përmirësuar sjelljen në siguri;
- një vlerësim të programit, që mundëson kryerjen e balancimit të shpenzimeve, identifikon boshllëqet në aftësitë ekzistuese të sigurisë, ndihmon në vendimmarrje mbi investimet me përparësi strategjike për nevojat e sipërmarrjeve dhe rrit vlerën e kompanisë (organizatës).

Në themel, ky program ofron balancim të kostos, rrezikut dhe vlerës. Ken Allan, udhëheqësi global i KE-së, mbi sigurinë e informacionit, shprehet se: "Ndaj një rreziku kaq të madh për: pronësinë intelektuale, klientët, operacionet e të dhënat financiare, si dhe për reputacionin organizativ, udhëheqësit e informuar po kuptojnë se është koha për një rishikim themelor se si siguria e informacionit kuptohet dhe pozicionohet brenda organizatës së tyre".

8. Siguria e informacionit (InfoSec-*Informationsecurity*)

Siguria e informacionit, përcakton mbrojtjen e informacionit nga qasja, përdorimi, zbulimi, shkatërrimi, modifikimi, leximi, inspektimi apo regjistrimi i paautorizuar. Është një term i përgjithshëm që mund të përdoret, pavarësisht nga forma e të dhënave që mund të marrim (elektronike, fizike, etj.)[16].

". . . Siguria e informacionit është një disiplinë për menaxhimin e rrezikut, detyra e së cilës është menaxhimi i kostos së rrezikut të informacionit biznesin"[17].

Dy aspektet më të mëdha të sigurisë së informacionit janë:

- siguria e IT ose siguria kompjuterike: siguria e teknologjisë së informacionit është siguria e informacionit e aplikuar në teknologji, si formë e sistemit të kompjuterit;
- sigurimi informacioneve: akti i sigurimit të së dhënave nga dëmtimet natyrore, mosfunksionim i kompjuterit / serverit, vjedhja fizike, shembuj të tjetër ku të dhënat kanë potencialin për të qenë të humbura.

Trekëndëshi i konfidencialitetit (fshehtësia), integritetit dhe disponueshmërisë qëndron në zemër të sigurisë së informacionit[18]. Konfidencialiteti (fshehtësia), integriteti dhe disponueshmëria përmenden në literaturë si: atributet e sigurisë, vetitë, siguria,

[15] http:/ec.europa.eu /dgs /home- affairs/doc centre/borders/docs/1 en autre document travail service part1 v3.pdf.
[16] ISACA. *Glossary of terms*, 2008: http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf
[17] B., McDermott, E., & Geer, D. (2001). Information security is information risk management. In Proceedings of the 2001 Workshop on New Security Paradigms NSPW '01, (pp. 97 – 104). ACM. doi:10.1145/508171.508187
[18] Perrin, Chad. "The CIA Triad". Marrë më 31 May 2012.

qëllimet, aspektet themelore, kriteret e informacionit, karakteristikat kritike informacionit dhe blloqet themelore të ndërtimit. Në sigurimin e informacionit, *fshehtësia* "është karakteristika, që informacioni nuk është vënë në dispozicion apo nuk zbulohet nga persona, subjekte, apo procese të paautorizuar"[19]. Në sigurimin e informacionit, *integriteti* i të dhënave do të thotë ruajtje, sigurim i saktë dhe plotësim i të dhënave mbi tërë ciklin e saj[20]. *Disponueshmëria* për çdo lloj sistemi informacioni: duke i shërbyer qëllimit të tij, informacioni duhet të jetë në dispozicion kur është i nevojshëm. Siguria e informacionit është një zonë studimore shumëdisiplinore dhe aktiviteti profesional, që përfshin zhvillimin edhe zbatimin e mekanizmave të sigurisë së të gjitha llojeve në dispozicion (teknike, organizative, njerëzore dhe ligjore), me qëllim mbajtjen e informacionit brenda perimetrit të organizatës.

9. Përfundime

Udhëheqësit e organizatave dhe të sipërmarrjeve të ndryshme, po informohen se ka ardhur koha për një rishikim lidhur me kuptimin e sigurisë së informacionit dhe se vendin që zë ajo brenda organizatave të tyre. Siguria e informacionit nuk mund të vështrohet si një pengesë e risive teknologjike, por si akses për zhvillim të shpejtë dhe si përshtatje me strategjitë në tregje, duke sjellë një avantazh konkurrues. Bordet vendimmarrëse e mbikëqyrëse duhet të rrisin mbështetjen për sigurinë dhe të përcaktojnë njerëzit përgjegjës mbikëqyrës. Këto komisione (borde) duhet të jenë të informuar mirë për proceset e kompanisë, të shfrytëzojnë informacionet dhe të kuptojnë nëse administrata ka njerëzit dhe proceset e duhura. Siguria kibernetike dhe lufta ndaj krimit kibernetik nuk është vetëm një çështje teknologjike, por është një rrezik sipërmarrjeje publike e private që kërkon një përgjigje të gjerë.

- *Identifikimi i problemeve dhe sigurimi i informacionit mbi krimin kibernetik në nivel nacional, rajonal dhe ndërkombëtar.* Ka shumë rëndësi identifikimi sipas ekspertizës mbi sigurinë kibernetike në Evropë: programit ISO 27001- Standardi Ndërkombëtar i Praktikës më të Mirë; Sistemit ISMS - Sistem i Menaxhimit të Sigurisë së Informacionit; Horizon 2020 - Program Kërkimi dhe Inovacionit në BE; Digital Forensics - Procesi Zbulimit dhe Interpretimi i të Dhënave Elektronike.

- *Adoptimi i legjislacionit përkatës me plotësimet e mëtejshme të kuadrit ligjor mbi sigurinë kibernetike.* TIK-u, me risitë e tij, përbën sfidë në përfshirjen në hartimin e ligjeve dhe në zbatimin e kuadrit ligjor. Adaptimi i legjislacionit aktual dhe miratimi i ligjeve të reja duhet të harmonizohet me legjislacionin e BE-së. Këto ndryshime duhet të pasqyrojnë dinamikën në fushën e sigurisë kibernetike, mungesën e informacionit të plotë nga sipërmarrësit publikë e privatë dhe gjithëpërfshirjen.

- *Ndërtimi i institucioneve të specializuara sidomos në sistemin e sigurisë për krimin kibernetik.* Këto institucione (autoritete, departamente) do të mbikëqyrin, informojnë, monitorojnë, identifikojnë parashikojnë, bashkëpunojnë dhe menaxhojnë më mirë problemet e lindura të krimit kibernetik, dhe sigurinë kibernetike. Këto institucione duhet të aplikojnë në kushtet shqiptare analizën SWOT (*strength, weakness, opportunities, threats*)[21]. Kjo analizë (SWOT) lidh pikat e forta, të dobëta, mundësitë dhe

[19] Fragment ISO27000.
[20] Boritz, J. Efrim. "IS Practitioners' Vieës on Core Concepts of Information Integrity". International Journal of Accounting Information Systems. Elsevier. Marrë më 12 August2011.
[21] Dokumenti i Politikave për Sigurinë Kibernetike 2015 - 2017

kërcënimet prezentë në realizim ose që ndikojnë në mosrealizimin të suksesshëm të saj.

- *Trajnimi dhe forcimi i kapaciteteve njerëzore kundër krimit kibernetik.* Kapacitetet duhet të shtrihen krahas trajnimeve e ekspertëve TIK në procesin e *Digital Forensics - procesi i zbulimit dhe interpretimi i të dhënave elektronike*, edhe te ekspertët e terrenit që do të parandalojnë e dokumentojnë shkeljet ligjore (Policia e Shtetit), dhe në rritjen e performancës së organit të akuzës (prokurorisë), gjyqësorit (gjykatat) dhe të krijohet bashkëpunim kundër krimit kibernetik.

- *Bashkëpunimi me aktorë të tjerë në nivel kombëtar dhe ndërkombëtar.* Bashkëpunimi i brendshëm duhet të kultivohet ndërmjet sektorit publik, atij privat, organizatave qeveritare e joqeveritare dhe me shoqërinë civile. Ky bashkëpunim duhet të synojë përfitime financiare reciproke, menaxhim të rrezikut dhe një analizë në kuadër bashkëpunimi.

- *Informimi, sensibilizimi, monitorimi mbi krimin kibernetik dhe se si mund ta menaxhojmë atë.* Informacioni mbi këtë prirje në rritje krimi, duhet të shtrihet më tepër në kurikulat shkollorë, në atë të arsimit nëntëvjeçar.

- *Alokimi i fondeve dhe mjeteve financiare të nevojshme* për përballimin e sfidave në rritje ndaj krimit kibernetik. Këto fonde duhet të alokohen në risi teknologjike, përgatitje kapacitetesh, stërvitje të përbashkëta me partnerë të brendshëm e të jashtëm, ndryshime strukturore, drejtime në raport me trendin digjital dhe problemet e identifikuara të krimit kibernetik.

Bibliografia

1. Strategjia e Sigurisë Kombëtare (SSK), 2014 – 2020.
2. Strategjia për Mbrojtjen Kibernetike, Ministria e Mbrojtjes, nëntor 2014.
3. Strategjia për Mbrojtjen Kibernetike 2018-2020, Ministria e Mbrojtjes.
4. Komisioni Europian: "Dhjetë Prioritete të Bashkimit Europian".
5. Republika e Kosovës, Ministria e Punëve të Brendshme: "Strategjia Shtetërore për Sigurinë Kibernetike dhe Plani i Veprimit 2016 – 2019", dhjetor 2015.
6. Dokumenti i Politikave për Sigurinë Kibernetike 2015 – 2017, Tiranë 2015.
7. Alan Collins: "Studime bashkëkohore të sigurisë", UET / Press.
8. Tim Dunne, Milja Kurki, Steve Smith: "Teori të marrëdhënieve ndërkombëtare", UET / Press, 2010.
9. Fabian Zhilla, Besfort Lamallari: "Vlerësim i riskut të krimit të organizuar në Shqipëri", Tiranë 2015.
10. Ministria e Brendshme - Drejtoria e Përgjithshme e Policisë së Shtetit, Buletin informativ Aktiviteti i Policisë - prill 2018.
11. Ministria e Çështjeve Sociale dhe Rinisë: Broshura-Fëmijë-të-sigurt-në-internet
12. Autoriteti i Komunikimeve Elektronike dhe Postare, AKEP: www.akep.al.
13. Agjencia e lajmeve Sot News: www.sot.com.al.
14. Agjencia për Projektet e Mbrojtjes për Kërkime të Avancuara :www.darpa.gov.
15. Agjencia Europiane e Rrjeteve të Informacionit: www.enisa.europa.eu.
16. Asambleja e Mbrojtjes dhe Sigurisë Europiane, Forumi ndërparlamentar i Asamblesë perëndimore të BE-s: www.assembly-weu.org.
17. Autoriteti Kombëtar për Certifikimin Elektronik, AKCE : www.akce.gov.al.
18. Drejtoria e Sigurimit të Informacionit të Klasifikuar DSIK: www.nsaalbania.gov.al.
19. Siguria kibernetike dy vjet më vonë, Raport i CSIS, janar 2011.
20. Strategjia ndërkombëtare për hapësirën kibernetike, maj 2011.
21. Strategjia Ushtarake e Republikës së Shqipërisë, Tiranë 2008.
22. Strategjia Kombëtare për Zhvillim dhe Integrim 2007-2013, Tiranë, mars 2008-2015, Tiranë gusht, 2009.
23. Strategjia ndërsektoriale për shoqërinë e informacionit 2008-2013", Tiranë 2009.
24. Studim i OKB-së për qeverisjen elektronike për vitin 2010.

25. Ligj nr. 9887, datë 10.3.2008, i ndryshuar "Për mbrojtjen e të dhënave personale".
26. Ligji nr. 9918, datë 19.5.2008 për "Komunikimet elektronike në Republikën e Shqipërisë".
27. Ligj nr. 8457, datë 11.2.1999 "Për informacionin e klasifikuar "Sekret Shtetëror".
28. VKM nr. 922 datë 19.12.2007 "Për sigurimin e informacionit të klasifikuar "Sekret Shtetëror" që prodhohet, ruhet, përpunohet apo transmetohet në sistemet e komunikimit (INFOSEC)".
29. VKM nr. 690, datë 5.10.2011 "Për miratimin e rregullores "Për mbrojtjen kriptografike të informacionit të klasifikuar "Sekret Shtetëror".
30. Ligj nr. 10325, datë 23.9.2010 "Për Bazat e të Dhënave Shtetërore" dhe VKM nr. 945, datë 2.11.2012 për miratimin e rregullores "Administrimi i Sistemit të Bazave të të Dhënave Shtetërore".
31. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - Join(2013) 1 final - 7.2.2013.
32. Mike Trovato, EY Asia-Pacifc Security Practice Leader, 2013 EYGM Limited.
33. *Under cyber attack: EY's Global Information Security Survey 2013.*
34. https://www.itgovernance.co.uk/blog/top-8-cyber-crime-trends-identified-by-europol/
35. http://www.disaster-resource.com/index.php?option=com_content&vieëarticle&id1611&Itemid141
36. https://www.itgovernance.co.uk/blog/top-8-cyber-crime-trends-identified-by-europol/
37. https://www.information-age.com/10-cyber-security-trends-look-2018-123463680/
38. http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
39. Traininghttps://www.itgovernance.eu/en-ie/nis_directive_training-ie
40. https://www.itgovernance.eu/fr-fr/eu-cybersecurity-strategy-fr&https://www.europol.europa.eu/partners-agreements/member-states/ireland
41. https://www.ey.com/Publication/vwLUAssets/EY-cyber-program-management/$FILE/EY-cyber-program-management.pdf
42. B., McDermott, E., Geer, D. (2001). Information security is information risk management. In Proceedings of the 2001 Workshop on New Security Paradigms NSPW '01, (pp. 97 – 104).
43. Perrin, Chad. "The CIA Triad".
44. Boritz, J. Efrim. "IS Practitioners' Views on Core Concepts of Information Integrity". International Journal of Accounting Information Systems. Elsevier.


AKADEMIA E SIGURISË
AS
1971

Sfidat e reja dhe arritjet kundrejt krimit kibernetik, në Ballkanin Perëndimor dhe në botë

■**MSc. Qetësor GURRA**
Akademia e Sigurisë
qetesor.gurra@asp.gov.al

Abstrakt

Fokusi i kësaj teme është trajtimi i rrezikshmërisë që mbart krimi kibernetik. Fillimisht, do të trajtohen të dhënat e fundit, nga organizmat ndërkombëtare dhe institucionet shtetërore. Në këtë lloj forme, do të evidentohen problematikat më të spikatura, duke analizuar dhe ndryshimin e sofistikuar që ka pësuar kjo vepër penale, fantazmë së fundmi. Në vijim do të paraqiten tablo konkrete në rajon dhe në rang ndërkombëtar, në lidhje me nivelin e zbulueshmërisë, marrjes së masave në kuadër legjislativ, infrastrukturë dhe cilësi profesionalizmi. Një rëndësi të veçantë do të ketë dhe përqasja me qëllimet dhe objektivat e fundit të Bashkimit Evropian, duke qenë etaloni shembull që duhet të merret parasysh nga vendi ynë. Së fundi, do të përmbyll në rekomandime të vlefshme, duke marrë parasysh dhe grafikët e 8 viteve të fundit në Republikën e Shqipërisë, të cilët paraqesin një realitet që lë tej mase për të dëshiruar. Trajtesa synon të evidentojë politikat e ndryshme që përqafon çdo shtet në varësi të zhvillimit dhe mirëqenies duke na ndihmuar të marrim parasysh shembuj alternativ të përmirësimit dhe ndryshimit të situatës në favorin tonë.

Fjalëkyçe:
kibernetik, implementim, eficencë, dispozita ligjore, përmirësim etj.

1. Hyrje

Zhvillimet e fundit, po tregojnë terrenin e jashtëzakonshëm që po fiton krimi kibernetik, qoftë në vendet me standard të lartë tek të cilat fitimi është shumë më i madh se në çdo vend tjetër, edhe në vendet të cilat lënë ende për të dëshiruar kundrejt implementimit bashkëkohor, koherent të kuadrit legjislativ dhe më tej. Në vijim, paralelizmi midis shteteve të Ballkanit Perëndimor dhe Amerikës, do ta dëshmojë më së miri këtë fakt. Shuma shumë të mëdha të ardhurash, po investohen për parandalimin dhe investigimin e rasteve të shumta, se si kjo vepër penale po ndryshon formë, por realisht alarmi i pamundësisë për të evidentuar subjektet është shumë i madh. I ngjasojnë disa fantazmave të padukshme, të cilat tejet të afta mundet të hyjnë kudo pa trokitur dhe të largohen duart plotë, duke lënë pas mjerim dhe dëme në çdo familje dhe biznes që shënjohet. Tema synon të trajtojë imtësisht fakte dhe fenomene demaskuese për të cilat duhet të gjenden zgjidhje afatshkurtra dhe afatgjata.

2. Ballkani Perëndimor

Nuk ka asnjë hulumtim në dispozicion, që trajton në mënyrë specifike zhvillimet në Ballkanin Perëndimor, në fushën e sigurisë kibernetike. Sidoqoftë, disa raporte globale pasqyrojnë situatën në disa ose shumicën e vendeve të rajonit, si "Indeksi Global i Cybersecurity 2015 i ITU-së dhe profili Cyberwellness" dhe BSA-së "Dashboard 2015 e maturisë së kibernetikës së BE-së"[1]. Disa raporte në dispozicion, të cilat fokusohen vetëm në aspekte të veçanta të sigurisë kibernetike, të tilla si, vlerësimi ITU i nevojave

[1] http://cybersecurity.bsa.org/

dhe aftësive për të krijuar CIRT kombëtare, sipas programit IMPACT[2] dhe OECD "Competitiveness in South East Europe Outlook Policy"[3] të 2016-s, shkruajnë shkurtimisht mbi statusin e legjislacioni të krimit kibernetik dhe partneritetet e politikave të sigurisë kibernetike. Raportet e vendeve të Komisionit Evropian, mbi gjendjen e secilit prej vendeve kandidatë nga Ballkani Perëndimor, mbulojnë fushat e shoqërisë informative dhe të medies, si dhe sigurinë, duke treguar informata themelore në lidhje me sigurinë kibernetike. Për shkak të statusit të saj, Kosova nuk paraqitet në shumë prej raporteve, por një burim veçanërisht i rëndësishëm i informacionit për vlerësimin e zhvillimeve në sigurinë kibernetike, është një dokument kërkimor me titull "Vlerësimi i kapacitetit të kibernetikës në Republikën e Kosovës"[4], i qendrës për kapacitete të sigurisë kibernetike, të Universitetit të Oksfordit, botuar me mbështetjen e Bankës Botërore[5]. Kjo e fundit, bazohet në metodologjinë e modelit të maturisë së sigurisë kibernetike të qendrës së kapaciteteve të sigurisë kibernetike, të përdorura në rastin e Kosovës, për herë të parë në Ballkanin Perëndimor.

Duke u bazuar në gjetjet e këtyre raporteve, si dhe në punën kërkimore shtesë, paraqiten profile të shkurtra të vendeve, duke u fokusuar kryesisht në nivelin e maturimit të kuadrit ligjor dhe të politikave (siç janë ligji kombëtar, strategjia kombëtare me planin e veprimit dhe përputhshmëria me kornizat ndërkombëtare) si dhe krijimin e kornizës operacionale (siç janë autoritetet kompetente kombëtare, ekipet e përgjigjeve në incidentin kibernetik, krimin kibernetik dhe njësitë e mbrojtjes dhe kapacitetet përkatëse), por gjithashtu duke marrë parasysh, qasjet e mundshme gjithëpërfshirëse ndaj partneriteteve publiko-private, formatet e bashkëpunimit, si dhe iniciativat e edukimit strategjik. Përmbledhja, e cila ofron një perspektivë "zoom-out" të rajonit, sillet këtu, si më poshtë.

2.1 Shqipëria

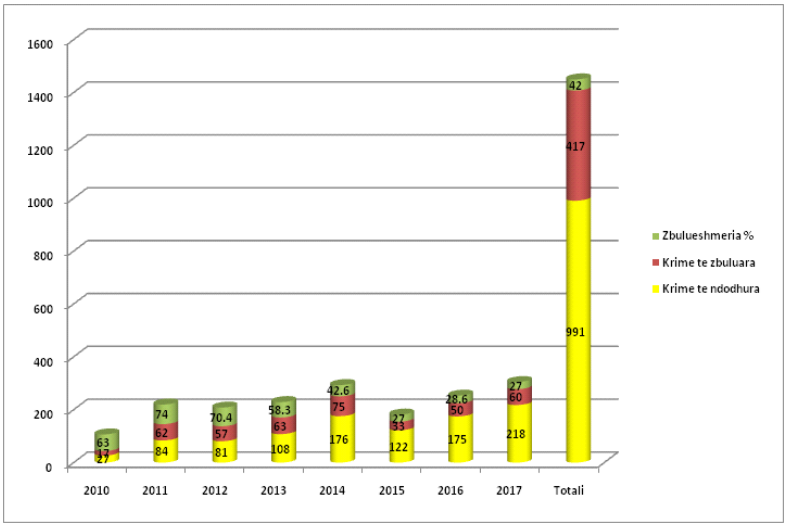
Rruga e Shqipërisë drejt një hapësire më të sigurt dhe më elastike ka filluar me "Strategjinë kombëtare ndërsektoriale të sigurisë së informacionit" (2008-2013). Dokumenti përmend shkurtimisht sigurinë kibernetike, si një nga fushat që duhej të konsiderohej si prioritet. Strategjia parashikoi gjithashtu krijimin e Agjencisë Kombëtare të Sigurisë Kibernetike (ALCIRT)[6], si institucion kombëtar për reagimin ndaj incidenteve kibernetike. ALCIRT, e vendosur nën autoritetin e kryeministrit, u krijua në vitin 2011 me mbështetjen e "Programit shqiptar të sigurisë kibernetike" të USAID-it, duke përfshirë seminare trajnimi të sektorit qeveritar dhe joqeveritar, nga Instituti i Inxhinierisë Programuese të Universitetit Carnegie Mellon (SEI), në drejtim të ndërtimit të kapaciteteve për t'i rezistuar kërcënimeve operacionale dhe për të zhvilluar procese për menaxhimin e incidenteve të sigurisë kibernetike[7]. ALCIRT është gjithashtu përgjegjëse për pjesëmarrjen në përgatitjen e strategjisë kombëtare të sigurisë kibernetike, hartimin e legjislacionit përkatës, bashkëpunimin me të gjitha institucionet relevante, organizatat ndërkombëtare, sektorin privat dhe organizimin e fushatave ndërgjegjësuese,

[2] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/assessmentEur.pdf
[3] http://www.oecd.org/publications/competitiveness-in-south-east-europe-9789264250529-en.htm
[4] https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/ files/CMM_Review_Report_Kosovo_June_2015.pdf
[5] http://www.worldbank.org/en/news/press-release/2015/06/25/ world-bank-supports-kosovo-efforts-in-strengthening-cyber-security
[6] R. Bofati dhe J. Josifi: "Towards a more resilient cyberspace: the case of Albania", Information & Security: An International Journal, vol. 32, 2015, available at: https://procon.bg/system/files/3310_albania.pdf
[7] https://www.usaid.gov/albania/press-releases/usaid-completes-project-support-albania%E2%80%99s-new-cyber-incident

trajnimeve dhe materialeve edukative. Megjithatë, me vetëm gjashtë punonjës (drejtori dhe pesë ekspertë), ajo ka kapacitete shumë të kufizuara njerëzore dhe infrastrukturore, dhe nuk ka qenë në gjendje të kryejë mirë, si përgjigjen ndaj incidenteve kibernetike, edhe aktivitete më të gjera si, arsimi dhe fillimi i një partneriteti të qëndrueshëm publiko-privat.

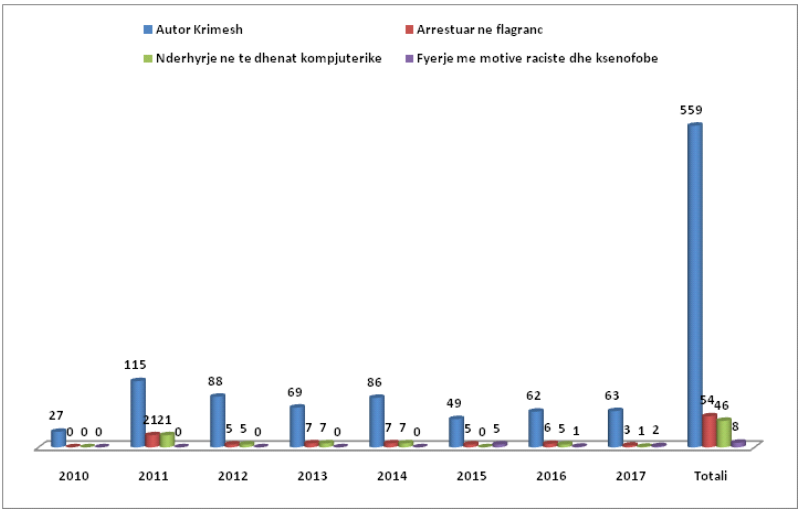
Po kështu, si strukturë për zbulimin dhe goditjen e veprimtarisë kriminale në fushën e krimit kompjuterik, në Drejtorinë e Përgjithshme të Policisë së Shtetit, funksionon, sektori për hetimin e krimit kompjuterik, në departamentin e policisë kriminale, në cilin punojnë 5 specialistë të hetimit të këtij krimi; po ashtu, është edhe një seksion i hetimit të krimit kompjuterik në drejtorinë vendore te policisë, në Qarkun e Tiranës, me 2 specialistë hetimi. Ky sektor është i ri dhe bën përpjekje për të zbuluar dhe goditur këtë veprimtari kriminale. Ajo çka ja vlen të diskutohet, janë rezultatet e arritura në 8 vitet e fundit, 2010-2017, rezultate të cilat nuk janë ato që presim dhe tregojnë njëkohësisht se ku duhet të përqendrohemi për të zbuluar dhe goditur autorët e këtyre veprave penale.

Sipas statistikave zyrtare, në tetë vitet e fundit janë evidentuar gjithsej 991 vepra penale në fushën e krimin kibernetik, dhe janë zbuluar nga këto vepra penale vetëm 417 të tilla, pra e thënë më qartë: janë zbuluar 42% e krimeve të ndodhura.



Janë evidentuar si autorë krimesh, nga veprat penale të ndodhura, gjithsej 551 autorë, por kur diskutohet se sa autorë janë arrestuar, shifrat tregojnë që janë jashtëzakonisht shumë pak. Gjithsej janë arrestuar 54 autorë të këtyre veprave penale të ndodhura: 21 autorë në vitin 2011 dhe për shtatë vite të tjera vetëm, 33 autorë.

Interes për auditorin e respektuar, ka që të dijë se sa vepra penale kanë ndodhur sipas ndarjes apo llojit të tyre. Kështu, vepra penale, si "Ndërhyrje në të dhënat kompjuterike", në tetë vite të marra së bashku, kanë ndodhur gjithsej 686 vepra penale; ndërsa "Fyerje me motive raciste dhe ksenofobe", kanë ndodhur 305 vepra penale. Nga 54 personat e arrestuar gjatë tetë viteve, 46 janë arrestuar për veprën penale të "Ndërhyrjes në të dhënat kompjuterike" dhe 8 autorë për veprën penale "Fyerje me motive raciste dhe ksenofobe". Se çfarë duhet të ndryshojë, janë rekomanduar në pjesën e fundit të këtij punimi.



Në vitin 2014, ALCIRT mori iniciativën dhe udhëhoqi grupin ndërinstitucional për hartimin e "Dokumentit të politikave kombëtare për sigurinë kibernetike" për periudhën 2015-2017. Dokumenti u adoptua kohët e fundit dhe synon të vlerësojë situatën aktuale dhe tendencat në lidhje me sigurinë kibernetike në vend. Sidoqoftë, ende nuk ekziston një strategji kombëtare e sigurisë kibernetike, megjithëse krijohet grupi i punës për hartimin e strategjisë. Gjithashtu, draft i parë i ligjit ekziston dhe është duke u shqyrtuar nga aktorët kryesorë në këtë fushë.

Në krahasim me vendet e tjera të rajonit, siguria kibernetike dhe mbrojtja kibernetike janë të larta në agjendën e institucioneve të mbrojtjes shqiptare. Në këtë drejtim, Strategjia e Sigurisë Kombëtare të Shqipërisë (2014-2020)[8] klasifikon sulmet kibernetike si një lloj i një rëndësie të veçantë. Si anëtare e NATO-s, Shqipëria nënshkroi Memorandumin e Mirëkuptimit, me Qendrën e Përgjithshme të Përgjegjësisë Cyber, të NATO-s, për rritjen e mbrojtjes kibernetike, në 2013, dhe po negocion nënshkrimin e versionit të ri të këtij memorandumi. Ky version bazohet në dokumentin e mbrojtjes kibernetike "Politika e mbrojtjes kibernetike të NATO-s", e miratuar nga të gjitha vendet e NATO-s në samitin e Wells-it në vitin 2014[9]. Për më tepër, Shqipëria mori pjesë në stërvitjen vjetor të koalicionit *Cyber*, - stërvitja më e madh kibernetike e NATO-s, - si vend vëzhgues, dy herë, dhe u bë pjesëmarrëse aktive që nga nëntori i vitit 2016. Shqipëria gjithashtu merr pjesë aktive në projektet e NATO-s[10], lidhur me sigurinë kibernetike. Në të njëjtën kohë, Shqipëria po zbaton zyrtarisht grupin fillestar të masave të ndërtimit të besimit, të OSBE-së për hapësirën kibernetike, që nga viti 2014 dhe ka pranuar në parim, që të vazhdojë më tej procesin në fjalë.

2.2 Bosnje dhe Hercegovina

Bosnja dhe Hercegovina (BIH) nuk ka përparuar në mënyrë adekuate në fushën e sigurisë kibernetike, as nuk ka harmonizuar legjislacionin e saj në përputhje me rrethanat

[8] http://www.mod.gov.al/images/PDF/Strategjia_per_Mbrojtjen_Kibernetike.pdf
[9] http://www.nato.int/cps/en/natohq/official_texts_112964.htm
[10] http://ncia.nato.int/Documents/Agency%20publications/Communications%20and%20Information%20Partnerships% 20and%20Multinational%20Projects.pdf

dhe ende nuk ka një qasje gjithëpërfshirëse strategjike për të adresuar çështjen e krimit kibernetik dhe kërcënimeve të sigurisë kibernetike[11]. Legjislacioni ekzistues në nivel shtetëror që mund të lidhet me sigurinë kibernetike, zor se trajton edhe pjesërisht çështjet relevante, të cilat nuk zbatojnë plotësisht dispozitat e kornizës ndërkombëtare së cilës ajo i përmbahet, siç është Konventa për Krimin Kibernetik[12]. Ky shtet, nuk ka një ligj të nivelit shtetëror mbi sigurinë e informacionit. Përkundrazi, entiteti i tij, Republika Srpska, ka miratuar ligjin "Për sigurinë e informacionit". Gjithashtu, dokumenti i vetëm në nivel shtetëror që trajton drejtpërsëdrejti çështjet e sigurisë kibernetike, është strategjia për krijimin e një CERT-i në Bosnjë dhe Hercegovinë. Megjithatë, megjithëse kjo strategji është miratuar në vitin 2011 dhe grupi i punës parasheh që BERT-CERT-i[13] të krijohet, ky i fundit ende nuk ekziston dhe plani i veprimit i hartuar nga GP-ja, për arsye politike, është ende në pritje të miratimit.

Në anën tjetër, departamenti për sigurinë e informacionit, në kuadër të Agjencisë për Shoqërinë e Informacionit të Republikës Srpska, u bë funksional në qershor të vitit 2015. Kjo njësi ka për detyrë të koordinojë parandalimin dhe mbrojtjen nga incidentet e sigurisë në kompjuter dhe të mbikëqyrë zbatimin e standardeve dhe masave të sigurisë së informacionit, por vetëm në Republikën Serbe. Bashkëpunon ngushtë me departamentet përkatëse të Ministrisë së Brendshme të Republikës Srpska, veçanërisht Njësia e saj për Parandalimin e Krimit të Lartë Teknik. Sa i përket mundësive në arsim, BIH strehon Qendrën e Sigurisë Kibernetike të Evropës Juglindore (SEECSC) - njësi kërkimore dhe zhvillimi në Universitetin Amerikan në Bosnjë dhe Hercegovinë. Universiteti ofron arsimim të sigurisë kibernetike (të dyja në nivel profesional dhe akademik, - përmes kurseve MA dhe PhD) dhe bashkëpunon me institucionet e sigurisë, inteligjencës dhe mbrojtjes në Bosnjë dhe Hercegovinë.

2.3 Kroacia

Si i vetmi vend anëtar i BE në rajon, Kroacia ishte e detyruar të kompletonte kuadrin institucional dhe ligjor në fushën e sigurisë kibernetike gjatë procesit të saj të pranimit. Për këtë arsye, ajo ka miratuar plotësisht të gjitha ligjet dhe rregulloret e nevojshme dhe i ka bërë ato në përputhje me rregulloren e BE-së. Për këtë qëllim, Kroacia miratoi ligjin e saj mbi sigurinë e informacionit, në vitin 2007, i cili përcaktoi krijimin e një CERT-i kombëtar, i ashtuquajtur CARN[14].

Detyra e tij kryesore është përpunimi i incidenteve në internet, ruajtja e sigurisë së informacionit në Kroaci. Përveç kësaj, ekziston edhe një CERT i qeverisë i quajtur ZSIS-CERT, i vendosur në Byronë e Sigurisë së Sistemeve të Informacionit (ISBB). ISBB është autoriteti qendror shtetëror, përgjegjës për fushat teknike të sigurisë së informacionit, të organeve shtetërore të Republikës së Kroacisë, i cili përfshin: krijimin e standardeve të sigurisë së informacionit, akreditimin e sigurisë në sigurinë e informacionit, menaxhimin e materialeve të kriptuara, të përdorura në shkëmbimin e informacionit të klasifikuar dhe koordinimin e parandalimit, dhe reagimit ndaj kërcënimeve kompjuterike ndaj sigurisë së sistemit të informacionit.

Dokumente të tjera ligjore që plotësojnë kornizën e Kroacisë, janë: ligji i sistemeve të

[11] www.ec.europa.eu/enlargement/pdf/key_documents/2015/20151110_report_bosnia_and_herzegovina.pdf
[12] S. Barakovic and J. BarakovicHusic: "'We have Problems for Solutions': The State of Cybersecurity in Bosnia and Herzegovina", Information & Security: An International Journal, vol. 32, 2015, https://procon.bg/system/files/3205_bih_barakovic.pdf
[13] www.msb.gov.ba/docs/Strategija_za_CERT.doc
[14] http://www.cert.hr/en/start

sigurisë dhe inteligjencës, të Republikës së Kroacisë (2006)[15]; "Akti i fshehtësisë së të dhënave" (2007)[16]; "Rregullorja mbi masat e sigurisë së informacionit" (2007) dhe "Akti mbi infrastrukturat kritike" (2013). Të gjitha këto tregojnë një mjedis të harmonizuar ligjor dhe operacional.

Strategjia kombëtare e sigurisë kibernetike, e Republikës së Kroacisë, dhe plani i veprimit për zbatimin e saj, u miratuan në tetor 2015[17]. Kjo strategji gjithëpërfshirëse është dokumenti strategjik më gjithëpërfshirës dhe sistematik, në lidhje me sigurinë kibernetike në Ballkanin Perëndimor. Strategjia ka për qëllim "të arrijë një përgjigje të ekuilibruar dhe të koordinuar, të institucioneve të ndryshme që përfaqësojnë të gjithë sektorët e shoqërisë, ndaj kërcënimeve të sigurisë në hapësirën kibernetike të sotme. Strategjia njeh vlerat që duhet të mbrohen, institucionet kompetente dhe masat për zbatimin sistematik të një mbrojtjeje të tillë".

Në mënyrë të qartë përcakton nevojën për krijimin e dokumenteve strategjikë në lidhje me mbrojtjen kibernetike dhe krimin kibernetik. Në nivel institucional, strategjia supozon krijimin e Këshillit Kombëtar të Sigurisë Kibernetike, i cili do të ketë kompetenca të mëdha në monitorimin dhe koordinimin e zbatimit të strategjisë, ndryshimet e mundshme të tij, si dhe në propozimin e organizimit të ushtrimeve kombëtare. Megjithatë, puna e tij nuk është e kufizuar në monitorimin e zbatimit të strategjisë. Ai ka autoritetin për të adresuar çështjet thelbësore për menaxhimin e sigurisë kibernetike dhe ndër të tjera, të lëshojë vlerësime periodike të gjendjes së sigurisë dhe të përcaktojë, planin e veprimit të krizës kibernetike. Në nivel teknik, këshilli do të mbështetet nga grupi koordinues i operacioneve dhe teknikave të sigurisë kibernetike, dhe më e rëndësishmja, ajo ka për detyrë të dorëzojë raportet drejtpërdrejtë në qeveri. Së fundi, edhe pse strategjia përcakton nevojën për partneritete të forta publike-private, për momentin nuk ka dëshmi të tilla në Kroaci. Në të njëjtën kohë, disa forma të edukimit profesional dhe ngritjes së kapaciteteve kryhen nga ISBB-ja, CERT-i kombëtar dhe "Qendra universitare për sigurinë e informacionit".

2.4 Kosova

Kosova nuk ka një ligj të vetëm për sigurinë kibernetike. Megjithatë, dispozitat ligjore dhe mbrojtja e të dhënave personale ekzistojnë, respektivisht, në ligjin "Për komunikimet elektronike" dhe ligjin themelor për "Parandalimin dhe luftimin e krimit kibernetik[18]. Në janar 2016, qeveria e Kosovës miratoi "Strategjinë kombëtare të sigurisë kibernetike dhe planin e veprimit, 2016-2019"[19]. Strategjia parasheh që ligji "Për identifikimin dhe mbrojtjen e infrastrukturës kritike" do të hartohet në vitin 2016, me CIIP që është një pjesë e rëndësishme e këtij ligji. Gjithashtu, strategjia përcakton nevojën për rishikimin e ligjit "Për parandalimin dhe luftimin e krimit kompjuterik". Ministria e Punëve të Brendshme (MPB), e cila formoi grupin e punës (GP) në vitin 2015, ishte mjaft interesante. Në mënyrë të veçantë, grupi i punës përfshinte një sërë aktorësh: të gjitha institucionet shtetërore, shoqatat profesionale, sektorin privat, qytetarët e shoqërisë

[15] https://www.zsis.hr/UserDocsImages/Sigurnost/Security/Security %20and%20Intelligence %20 System%20 Act.pdf

[16] https://www.zsis.hr/UserDocsImages/Sigurnost/Security/Data%20Secrecy%20Act.pdf

[17] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/croatian-cyber-security-strategy/view

[18] Ligji 03/L-166, Law on Prevention and Fight of the Cyber Crime, http://www.kuvendikosoves.org/common/docs/ligjet/2010-166-eng.pdf

[19] https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/kosovo-national-cyber-security-strategy-and-action-plan-2016-2019

dhe partnerët ndërkombëtarë. Strategjia parasheh disa zgjidhje institucionale për të arritur qëllimin e saj, objektivat kryesore, si, emërimi i koordinatorit kombëtar të sigurisë kibernetike, "... i mandatuar për të koordinuar, udhëzuar, monitoruar dhe raportuar për zbatimin e politikave, aktiviteteve dhe veprimeve në lidhje me *Strategjinë kombëtare të sigurisë kibernetike*". Strategjia parasheh që ministri i Punëve të Brendshme (ose personi i autorizuar prej tij) të caktohet si koordinator, duke marrë kështu shtysë dhe rëndësi politike, për zbatimin e strategjisë. Ky mesazh i rëndësishëm politik shoqërohet me krijimin e të ashtuquajturit *Sekretariati i strategjisë*, organi përgjegjës për monitorimin dhe koordinimin e aktiviteteve të strategjisë. Së fundi, në një përpjekje për të nxitur koordinimin e autoriteteve kompetente dhe relevante qeveritare, dhe përfaqësuesve të sektorit privat, strategjia parasheh krijimin e "Këshillit kombëtar të sigurisë kibernetike". Krijimi i këshillit, është një zgjidhje unike në Ballkanin Perëndimor, për të rritur dhe madje përforcuar, bashkëpunimin e institucioneve të ndryshme brenda qeverisë, por edhe për krijimin e partneritetit kuptimplotë dhe potencialisht të fuqishëm publik-privat.

Me ndihmën e madhe të projektit ENCYSEC, të financuar nga BE, KOS-CERT[20] kohët e fundit ka filluar punën CERT ("Njësia kombëtare e sigurisë kompjuterike"). Ende është një punë në progres, por është i pranishëm vizioni i krijimit të një ekipi të vogël, shumë të aftë përgjegjës për raportimin dhe trajtimin e incidenteve, si dhe koordinimin e aktiviteteve ndërgjegjësuese në nivel kombëtar. KOS-CERT, është një njësi funksionale brenda "Autoritetit rregullativ të komunikimit elektronik dhe postar". Edhe pse ekzistenca e strategjisë dhe qëllimet e saj ambicioze tregojnë se siguria kibernetike është njohur si një prioritet në të gjithë qeverinë, një numër faktorësh të tjerë tregojnë se Kosova është ende në fazën fillestare të zhvillimit të aftësive të sigurisë në kibernetikë. Arsimi i sigurisë në internet është i pakët dhe ekziston si fragmentar, vetëm në Universitetin e Prishtinës; programet e trajnimit ekzistojnë vetëm në një mënyrë *ad-hoc*; ndërgjegjësimi i kibernetikës është i kufizuar dhe themelor, dhe duhet të nxitet ndërmjet pjesëve të ndryshme të popullsisë, në mënyra të ndryshme.

Megjithatë, një numër i këtyre mangësive njihet nga strategjia dhe trajtohen në planin e veprimit. Duhet të theksohet se i gjithë procesi është ende në një pjesë të madhe, i drejtuar nga donatorët. Kjo duket më së shumti te plani i veprimit, i cili ka një kolonë për secilin aktivitet të përcaktuar, që tregon institucionin mbështetës për aktivitetin. Një numër i madh i aktiviteteve duhet të mbështeten nga "partnerët ndërkombëtarë", përkatësisht: SHBA, "Ndihma për trajnimin ndërkombëtar të hetimeve penale programi" (ICITAP), programi pilot i BE-së "Përmirësimi i sigurisë kibernetike" (ENCYSEC), UNDP dhe OSBE. Megjithatë, është e paqartë nëse organizatat ndërkombëtare (pavarësisht nga projekti ENCYSEC) të jenë zotuar tashmë, që të ndihmojnë shumë në zhvillimin e një kuadri të sigurisë kibernetike; apo nëse kjo është vetëm një listë e dëshirës së grupit të punës që hartoi strategjinë. Megjithatë, duke pasur parasysh se përfaqësuesit e organizatave ndërkombëtare ishin pjesë e grupit të punës, opsioni i parë duket si më i mundshëm.

2.5 Mali i Zi

Mali i Zi ka avancuar shpejtë në fushën e sigurisë në internet, që nga viti 2010, kur u miratua pjesa përbërëse e legjislacionit: ligji "Për sigurinë e informacionit", së bashku

[20] http://kos-cert.org/assets/cms/uploads/files/KOS-CERT%20RFC2350.pdf

me "Rregulloren për masat e sigurisë së informacionit". Një strategji kombëtare e sigurisë kibernetike për Malin e Zi, për periudhën 2013-2017, është miratuar në tetor 2013. "Plani i veprimit për zbatimin e strategjisë", për periudhën 2013-2015 është pjesë e strategjisë, si një shtojcë, edhe pse nuk kishte plan veprimi, për periudhën 2015-2017, në kohën e publikimit të këtij raporti.

Sa i përket një kornize institucionale, detyra e parë e parashikuar nga plani i veprimit, ishte krijimi i "Këshillit kombëtar për siguri në kibernetikë/sigurinë e informacionit". Kjo nuk ka ndodhur akoma deri sot, megjithëse ishte përsëri në përputhje me ndryshimet e ligjit "Për sigurinë e informacionit", të miratuara në janar 2015. Pasi të jetë operacional, këshilli supozohet të jetë institucioni kyç që ka të bëjë me çështjet e sigurisë kibernetike. Këshilli gjithashtu do të jetë përgjegjës për krijimin e procedurave për shkëmbimin e rregullt të informacionit, midis autoriteteve shtetërore dhe institucioneve kyçe nga sektori privat, ofruesit e internetit, agjentët, sektori bankar, kompanitë e energjisë elektrike dhe kompanitë që ofrojnë shërbime elektronike në Malin e Zi[21].

CIRT-i i Malit të Zi u bë funksional në vitin 2012, me ndihmën e programit ITU-IMPACT. N-CIRT është e pozicionuar në Ministrinë e Shoqërisë së Informacionit dhe Telekomunikacionit dhe kryen detyra të rregullta të CIRT-it. CIRT-i kombëtar është gjithashtu shumë aktiv në promovimin e kulturës së sigurisë në hapësirën kibernetike. Në vitin 2015, ajo zhvilloi dokumentin me titull "Udhëzimet për sigurinë dhe mbrojtjen e informacionit në *Cyberspace*". Në bashkëpunim me ITU, CIRT-i organizoi një stërvitje në internet, në shtator 2015, nga Evropa. Trajnimi u ndoq nga më shumë se 50 pjesëmarrës, nga Mali i Zi dhe vende të tjera. Përveç kësaj CIRT-i merr pjesë aktive në projektin gjithëpërfshirës TEMPUS në lidhje me edukimin e sigurisë kibernetike në Mal të Zi. Në tetor 2014, qeveria e Malit të Zi miratoi "Metodologjinë e identifikimit të infrastrukturës kritike të informacionit" (CII) dhe planin e veprimit për zbatimin e saj. Ky dokument është përgatitur dhe publikuar, pavarësisht nga mungesa e një ligji mbi infrastrukturën kritike të Malit të Zi dhe për shkak të rëndësisë për të bërë përparim shtesë në këtë fushë. Ky është i vetmi dokument kombëtar që lidhet me Ballkanin Perëndimor.

Për më tepër, në vitin 2015, Ministria e Shoqërisë së Informacionit dhe Telekomunikacionit zhvilloi metodologjinë për vlerësimin e modelit të maturitetit të kapacitetit të kibernetikës. Kjo metodologji u hartua me ndihmën financiare të Bankës Botërore dhe në bashkëpunim me modelin e maturitetit të kapacitetit ekzistues të kibernetikës së sigurisë, së "Qendrës botërore të sigurisë kibernetike" së Universitetit të Oksfordit. Mali i Zi ka një program të nivelit "master" të nivelit të lartë të universitetit, për politikën e sigurisë kibernetike, të zhvilluar dhe ofruar nga Universiteti Donja Gorica në Podgoricë, i cili jep një përzierje unike të njohurive teknike, të bazuara në politika mbi një sërë çështjesh të sigurisë në kibernetikë. Universiteti Donja Gorica është gjithashtu një partner në projektin e lartpërmendur TEMPUS të financuar nga BE.

2.6 Republika e Maqedonisë

Maqedonia nuk ka një ligj gjithëpërfshirës që merret ekskluzivisht me sigurinë kibernetike. Në vend të kësaj, një numër dokumentesh ligjore prekin disa çështje që

[21] http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Montenegro_2013_Cyber % 20 Security %20Strategy % 20for %20Montenegro.pdf

lidhen me sigurinë kibernetike: ligji "Për të dhënat personale", ligji "Për tregtinë elektronike", ligji "Për komunikimet elektronike", ligji "Për ndalimin e komunikimeve", ligji "Për qasjen e lirë në informacionin publik", ligjin "Mbi të dhënat në një formë elektronike dhe nënshkrimi elektronik". Përveç kësaj, ndryshimet në ligjin "Mbi procedurën penale", të miratuara në vitin 2013, në mënyrë specifike trajtojnë krimin kibernetik dhe krimet e kryera me përdorimin e kompjuterëve, si dhe mbledhjen e provave digjitale nga autoritetet e zbatimit të ligjit. Megjithëse disa organizata ndërkombëtare kanë lehtësuar diskutimet gjatë përgatitjes së "Strategjisë kombëtare të kibernetikës" (për shembull, UNDP ka porositur një studim vlerësimi për kërkesat për përgatitjen e një strategjie kombëtare të sigurisë kibernetike), strategjia kombëtare është ende në procesin e hartimit[22]. Rrjeti kombëtar akademik dhe hulumtues *MARnet*, i krijuar në vitin 2010, mori përsipër aftësitë dhe detyrat e CERT-it akademik, i cili më parë ishte i vendosur në Universitetin Kiril dhe Metodij në Shkup.

Megjithatë, me një impuls të fituar nëpërmjet zbatimit të projektit pilot të sigurisë së kibernetikës, të financuar nga BE-ja nën ENCYSEC të BE-së, një CERT-CERT kombëtar u formua në vitin 2015, si pjesë e Agjencisë së Komunikimit Elektronik (AEC), duke kryer funksione të rregullta CERT. Për sa i përket kapaciteteve institucionale për t'u marrë me çështjet e krimit kibernetik, njësia për krimin kibernetik, që gjendet brenda departamentit për shtypjen e krimit të organizuar dhe të rëndë, dhe departamenti i forenzikës, i Ministrisë së Brendshme, u futë në një departament të vetëm për krimin kibernetik dhe digjital, duke formuar kështu një njësi efektive hetimore.

2.7 Serbi

Kuadri ligjor dhe institucional i Serbisë, në fushën e sigurisë kibernetike bazohet në ligjin "Për sigurinë e informacionit", i cili u miratua në fillim të vitit 2016. Aktet nënligjore të rëndësishme (për masat mbrojtëse, në listën e operatorëve që kryejnë veprimtari me interes publik duke përfshirë infrastrukturën kritike incidentet raportuese) janë duke u hartuar, megjithëse kryesisht brenda qarqeve qeveritare dhe pa konsultime më të gjera. Ligji përcakton se operatorët e sistemeve të TIK-ut me rëndësi të veçantë (disa prej të cilave do të renditen si infrastrukturë kritike e informacionit), duhet të miratojnë një akt mbi sigurinë e sistemit të TIK-ut me masa mbrojtëse të dedikuara, mbikëqyrjen e sistemeve të TIK-ut dhe personave përgjegjës për kryerjen e këtyre detyrave. Për më tepër, ligji parashikoi krijimin e Trupit për Koordinimin e Sigurisë së Informacionit, me mundësi të krijimit të nëngrupeve të ekspertëve që mund të përfshijnë përfaqësues të organeve të tjera publike, industrisë, komunitetit akademik dhe shoqërisë civile[23].

Nevoja për të krijuar një sistem të duhur lidhur me sigurinë kibernetike është njohur në nivelin strategjik, në "Strategjinë për zhvillimin e shoqërisë së informacionit", në Republikën e Serbisë, deri në vitin 2020, e cila e cilëson sigurinë e informacionit si një nga gjashtë fushat e saj më me përparësi. Si vazhdim, grupi i punës për zhvillimin e strategjisë kombëtare për sigurinë kibernetike, është themeluar në vitin 2016 dhe ka mbajtur sesionet e para; strategjia u prit të miratohej në tremujorin e parë të vitit 2017. Megjithatë, infrastruktura kritike e informacionit nuk është përcaktuar ende dhe standardet e sigurisë kibernetike ende nuk janë miratuar.

Ligji mandatoi krijimin e CERT-it në "Agjencinë rregulluese për komunikimet

[22] http://ec.europa.eu/enlargement/pdf/key_documents/2015/20151110 _report_the_ former_yugoslav_ republic_of_ macedonia.pdf

[23] Artikulli 5, paragrafi 2 Law on Information Society, RS Official Gazette no. 6/2016.

elektronike dhe shërbimet postare" (RATEL). Ndërsa është themeluar zyrtarisht, është në fazën e zhvillimit dhe aktualisht nuk ka aftësi dhe burime teknike; me ngritjen e duhur të kapaciteteve, pritet të bëhet operacionale në vitin 2017. Në të njëjtën kohë, ekzistojnë ose janë në formim edhe disa CERT-ë të tjerë: CERT-i akademik është pjesë e rrjetit akademik (AMRES) dhe mbron rrjetin e arsimit, shkencës dhe kërkimit institucioneve; Ministria e Brendshme ka krijuar CERT-in e saj, për të mbrojtur bazat e të dhënave të ndjeshme të qytetarëve dhe sistemin që operon bazat e të dhënave; regjistri kombëtar i *domain*-it të Internetit RNIDS po krijon CERT-in për domenet kombëtare ndërkohë që sektori civil, po punon për krijimin e një CERT të pavarur, për të ndihmuar në reagimin ndaj sulmeve ndaj medieve. Në këtë moment, megjithatë, nuk ka ndërveprim mes këtyre.

Ngjashëm me vendet e tjera në rajon, ekzistojnë mekanizmat ligjorë për të luftuar krimin kibernetik. Kodi Penal parashikon norma për veprat penale në përputhje me kornizat ligjore të Bashkimit Europian dhe BE-së. Kodi Penal nuk rregullon terrorizmin kibernetik si kundërvajtje, edhe pse terrorizmi kibernetik mund të ndiqet penalisht në bazë të veprave ekzistuese kundër terrorizmit dhe të dhënave kompjuterike. Në lidhje me një kornizë institucionale, është krijuar njësia e krimit të lartë teknike, pranë zyrës së prokurorisë speciale. Për më tepër tre njësi të specializuara: për analizën e krimit; terrorizmit, ekstremizmit; parandalimi i drogës, varësia dhe represioni, janë krijuar brenda MPB-së. Të gjitha këto njësi kanë nevojë për staf të mëtejshëm, dhe nevojiten trajnime të specializuara dhe burime adekuate buxhetore.

Duhet të përmirësohet më tej niveli i bashkëpunimit ndërmjet agjencive, rrjedhjes së informacionit dhe shkëmbimit ndërmjet agjencive të zbatimit të ligjit. Megjithatë, bashkëpunimi i brendshëm midis policisë dhe zyrës së prokurorisë speciale për krimin kibernetik po përmirësohet. Nuk ka një edukim të duhur multidisiplinar të sigurisë në internet në nivelin e politikave. Ngritja e ndërgjegjësimit të përgjithshëm në lidhje me sigurinë në internet, sidomos në mesin e të rinjve, trajtohet përmes fushatës "*Smart* dhe *Safe*" të drejtuar nga Ministria e Tregtisë, Turizmit dhe Telekomunikacionit, por fushëveprimi i saj është i kufizuar.

3. Analizë e shkurtuar

Ekzistojnë dallime të rëndësishme dhe ngjashmëri të rëndësishme në zhvillimin e politikës së sigurisë kibernetike në të gjithë rajonin e Ballkanit Perëndimor. Në shumicën e vendeve, legjislacioni specifik mbi sigurinë e informacionit le për të dëshiruar. Megjithatë, është e jashtëzakonshme që Mali i Zi kishte kaluar një ligj të tillë në vitin 2010, ndërsa në Serbi ky i fundit nuk ishte miratuar deri në fillim të vitit 2016. Bosnja dhe Hercegovina, nga ana tjetër, ende nuk ka arritur të zhvillojnë ndonjë legjislacion të rëndësishëm në nivel shtetëror për sigurinë kibernetike.

Më shumë progres duket se janë arritur me strategjitë e sigurisë kibernetike dhe vlerësimet gjithëpërfshirëse të rrezikut. Përsëri, Mali i Zi ka udhëhequr prirjen, ndërsa Serbia ende nuk ka finalizuar një strategji ndërkohe që Bosnja dhe Hercegovina as që ka filluar të punojë në një të tillë. Megjithatë, vendet e Ballkanit Perëndimor duket të jenë të ngadalta në zbatimin e strategjive për të qenë plotësisht efiçente. Progresi është parë në disa vende për të bërë më efikase veprimtarinë e zbatimit të ligjit në fushën e krimit kibernetik, stafi i CERT-it dhe në QLA-të në përgjithësi ende nuk kanë resurse dhe kapacitete. Vështirë se ndonjë politikë serioze arsimore është ndërmarrë në asnjë nga

vendet e rajonit. Janë ndërmarrë pak gjëra në kuadrin e sektorit privat dhe nuk është ngritur asnjë partneritet i rëndësishëm publiko-privat me aktorët e kësaj fushe.

3.1 Të dhëna statistikore, kryesisht SHBA-ja, për sigurinë kibernetike

1. Në vitin 2016, qeveria e Shteteve të Bashkuara shpenzoi një shumë prej 28 miliardë dollarësh për sigurinë kibernetike, ndërkohë që kjo shumë pritet të rritet në 2017-2018[24].

2. Nëntë vite më parë, në vitin 2007, qeveria e SHBA-së harxhoi 7.5 miliardë dollarë për të luftuar sulmet kibernetike, të cilat filluan të ishin mjaft shqetësuese për komunitetin. Kjo shumë është e pavlerë, në krahasim me buxhetin për sigurinë kibernetike, të vitit 2016, e cila rezulton të jetë 28 miliardë dollarë (një rritje prej 373 për qind nga viti 2007). Ky investim përkon të jetë një ndër më të mëdhatë se disa buxhete totale të disa vendeve të mbledhura tok.

3. Sipas *Microsoft*[25], kostoja potenciale e krimit kibernetik ndaj komunitetit global është alarmues rreth 500 bilion dollarë, ndërkohë që një shkelje e të dhënave çka do të prezumonte informacione të vjedhura, futje në sistem pa dijeni, qoftë autorizime vjedharake etj., do t'i kushtojnë një kompanie mesatare rreth 3.8 milionë dollarë.

Sipas të dhënave nga grupi studimor "Hulumtimi i Juniper'', kostoja mesatare e shkeljes së të dhënave, do të tejkalojë 150 milion dollarë[26] deri në vitin 2020 dhe deri në vitin 2019, krimi kibernetik do t'i kushtojë bizneseve mbi 2 trilion dollarë pra, një rritje katërfish nga viti 2015.

Microsoft tha se një shkelje e të dhënave i kushton tej mase një kompanie mesatare. Nga të dhënat e hulumtimeve tregohet se kjo shumë do të rritet në një masë prej 3.947 për qind në mbi 150 milionë dollarë deri në vitin 2020. Ndërsa kompanitë do të zhvillohen dhe potencialet e tyre mund të jenë tej mase premtuese, ndërkohë që interneti vazhdon të zhvillohet me një ritëm masiv, domosdoshmërish një përqindje e buxhetit, duhet t'i dedikohet përmirësimit të sistemit të sigurisë.

4. Sulmet *Ransomware* (çka përkojnë të jenë një lloj programi infektues, të cili bllokon ose merr kontrollin e një sistemi duke kërkuar shpërblim për ta prishur totalisht ndërkohë që gjithmonë e më shumë, ky i fundit dëmton, duke pasur nën fokus sulmin dhe infektimin e kompjuterit me qëllimin primar fitimin e të ardhurave nga pronari i saj)[27] u rritën me 36 për qind në vitin 2017.

Hulumtimet nga *Symantec* tregojnë se sulmet *Ransomware* në 2017, në mbarë botën u rritën me 36 për qind më shumë se 100 familje të reja të konstatuara të dëmtuara nga hakerat. Megjithatë, interesante është se njerëzit, e veçanërisht 64 për qind e amerikanëve, janë të gatshëm të paguajnë një shpërblim, pasi bëhen viktima të sulmeve *ransomware*, krahasuar me 34 përqindëshin e njerëzve nëpër glob.

5. Shuma mesatare e kërkuar për rregullimin e sistemit pas një sulmi *ransomware,* është 1077 dollarë. Kjo shumë rezulton të ketë një rritje prej 266 për qind, krahasuar me vitet e kaluara. Krejt natyrshëm, duke konstatuar se njerëzit do të paguajnë pa hezitim për mbrojtjen dhe riparimin e aktiviteteve të tyre elektronike, hakerat nxiten akoma më shumë për të sofistikuar dhe për të shtuar sulmet e tyre. Padyshim, shuma rregulluese do të shtohet vit pas viti.

[24] http://www.taxpayer.net/library/article/cyberspending-database
[25] https://www.microsoft.com/en-us/cloud-platform/advanced-threat-analytics
[26] https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion
[27] https://www.symantec.com/security-center/threat-report

6. Në tërësinë e *email*-ve, 1 në 131[28] rezulton të jetë specifikisht i dizajnuar të ndërpresë, dëmtojë, fitojë kontrollin a qoftë eksesin, në sistemet e dëshiruara. Një statistikë e tillë mund të mos duket shqetësuese, por duke analizuar 5 vitet e shkuara, i bie të jetë më e larta dhe natyrisht, kjo do të përbëjë gjithnjë e më tepër një kërcënim më të shpeshtë për komunitetin global e lokal.

7. Në vitin 2017, 6.5[29] për qind e njerëzve kanë qenë viktima të mashtrimit të identitetit, duke shkaktuar dëme prej 16 miliardë dollarësh. Kjo e dhënë mbështetet nga grupi studimor ''Javelin & Research'' të cilët kanë pasur si kampion analize, 69 000 qytetarë të vrojtuar që në vitin 2003. Studimi tregoi se mashtrimet e identitetit në SHBA, u rritën në 15.4 milion në 2016; rreth 2 milion më shumë.

8. Konstatohet se 43 për qind e sulmuesve kibernetikë, kanë nën fokus bizneset e vogla. Ndërkohë që mund të dëgjojmë raste për sulme të kompanive të mëdha si, *Target, Ebay, Yahoo, Sony* etj., të cilat fitojnë një vëmendje mediatike, duhet të dimë se sulmet kibernetike janë më shumë të përqendruara në kompani dhe biznese të vogla, të cilat nuk kanë imunitetin dhe buxhetin e mjaftueshëm të fortifikojnë aktivitetet e tyre *online*. Kjo përqindje pritet të rritet duke detyruar çdo subjekt të investojë në këtë drejtim edhe pse do të ndikojë ndjeshëm në financat e tyre.

9. Numri i vendeve të punës për specialistët e sigurisë kibernetike, do të arrijë në 3.5 milion deri në vitin 2021[30], krahasuar me 1 milion që ishte në vitin 2016. Ndërkohë që kjo shifër globale mund të mos duket shumë e madhe, duhet pasur parasysh që ekziston një lidhje proporcionale me këtë pozicion pune dhe zhvillimit të trajektores së sulmeve kibernetike, çka do të vijojë me një rritje të punësimit në këtë sektor: 200 për qind deri në vitin 2021.

10. Sipas investitorit miliarder, Warren Buffett[31], sulmet kibernetike përbëjnë një ndër kërcënimet me të mëdha për njerëzimin, më shumë sesa dhe vetë armët nukleare. Ky konstatim nuk përbën një vlerë statistikore, por nëse analizojmë me kujdes tërësinë e të dhënave, logjika të çon në një nevojë imediate për të bërë vendimmarrje efiçente, të cilat do t'i shërbejnë të ardhmes dhe jo vetëm kaq. Duhet lënë vend për parandalim. Nëse rrezikshmëria kibernetike është tej mase e vështirë të merret nën kontroll, në një vend të zhvilluar si SHBA-ja, i cili ka mundësi të investojë shuma marramendëse, a e imagjinoni se si mund të jetë për shtetet e tjera, në rajonin tonë? Padyshim, një strehë mjaft e sigurt për sulmuesit kibernetikë, të cilët përfitojnë nga vakuumet e shumta që rezultojnë të jenë deri tashmë.

11. Çdo ditë prodhohen 230 000[32] lloje të reja sulmesh dhe dëmtimesh kibernetike të cilat do të shtohen kohë pas kohe. Sipas grupit studimor *Panda Security*, *softwar*–i Trojan është një ndër kërcënuesit më të shpeshtë, pasi maskohet si i ligjshëm ndërkohë që përdoret nga vjedhësit dhe hakerat, të cilët përpiqen të fitojnë qasje në sistemet e përdoruesve. Zakonisht, mashtrimet ndodhin në trajtën e ekzekutimit në sisteme, si formë e inxhinierisë sociale, në ngarkimin e komandave. Pasi aktivizohen, krijojnë një mjedis të volitshëm për spiunim, vjedhje, fshirje, bllokim, modifikim të dhënash, ndërprerje të performancës së rrjeteve kompjuterike etj.

12. Kina është një ndër vendet me numrin më të madh të sistemeve elektronike të

[28] https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html
[29] http://www.businessinsider.com/warren-buffett-cybersecurity-berkshire-hathaway-meeting-2017-5
[30] https://www.pandasecurity.com/mediacenter/press-releases/all-recorded-malware-appeared-in-2018
[31] https://swimlane.com/10-hard-hitting-cyber-security-statistics/
[32] https://www.techinasia.com/indonesia-world-leader-vpn-usage

infektuar. Sipas grupit studimor *Panda Security,* 57.24 për qind e kompjuterëve në Kinë, janë prekur nga një sulm kibernetik, duke pasur vlerë të pariparueshme në dëmin e kryer. Vijon Tailanda, me vlerën e përqindjes 49.15 dhe Turqia 42.52 për qind[33].

13. Gjatë një dite ndodhin mesatarisht 4000 sulme kibernetike. Sipas të dhënave të raportuara nga FBI-ja konstatohet një rritje 300[34] për qind, lidhur me sulmet kibernetike të ndodhura në vitin 2015, duke përbërë një fenomen shqetësues. Ditë pas dite testohen dhe analizohen kurthet më të mira kibernetike, të cilat jo vetëm përmirësohen, por shtohen me ritme marramendëse.

14. Rreth 78 për qind e njerëzve, njohin rrezikun e klikimit në faqet e dyshimta gjatë lundrimit në internet, a qoftë korrespodencës së kryer nëpërmjet *email*–ve, por sërish klikojnë tek to. Sipas studimit të kryer nga Universiteti Erlangen-Nuremberg, edhe pse komuniteti e kupton saktësisht llojin e klikimit sulmues kibernetik, sërish vijojnë ta klikojnë. Ndoshta kjo gjë lidhet me pakujdesinë, paditurinë shkujdese të momentit, por gjithsesi ka dhe doza neglizhence në këtë drejtim.

15. Një biznesi i duhen mesatarisht 197[35] ditë që të zbulojë infektimin nga një sulm kibernetik. Kjo shifër, është më shumë se 6 muaj. Ndërkohë, aktiviteti mund të vijojë dhe subjekti nuk ka as idenë më të vogël se çfarë është duke ndodhur me të. Hakerat janë tej mase të sofistikuar, duke sulmuar, zhvilluar terrenin dhe në pjesën më dërrmuese, duke u larguar me objektivat e tyre të përmbushura.

16. *Android*-i është platforma e dytë më e shënjuar nga hakerat, pas *Windows*-it. Numri i sulmeve kibernetike që synojnë pajisjet *Android,* është duke u rritur me shpejtësi: rreth 98 për qind. Hakerat nuk po kufizohen vetëm në kompjuterët desktop, por po ashtu synojnë pajisjet e telefonisë së lëvizshme (celulare), ndërsa vazhdojmë të përdorim pajisje celulare për aktivitete edhe më të rëndësishme, si p.sh. transaksionet financiare.

4. Konkluzione

Në bazë të studimit të zhvilluar në kuadër të këtij punimi, pasi u identifikuan sfidat dhe problematikat kryesore të shtetit shqiptar në luftën ndaj krimit kibernetik, duke u bazuar në analizën e dispozitave ligjore, arritjeve të deritanishme, statistikave dhe rezultateve të përfituara nga intervistat e zhvilluara me specialistët përgjegjës për hetimin, ndjekjen penale dhe luftimin e krimit kibernetik, u arrit të nxirren disa rekomandime që duhen ndjekur nga shteti shqiptar për përmirësimin e situatës aktuale, në lidhje me krimin kibernetik në Shqipëri. Këto rekomandime, janë si më poshtë:

- Ndërhyrje dhe ndryshime në terminologjinë e përdorur në legjislacion, për sa i përket kuptimit të termave "krim kompjuterik" dhe "krimi kibernetik".

- Hapja e programeve të studimit të ciklit të dytë dhe të tretë në fushën e krimit kibernetik, si dhe një programi rajonal në këtë fushë.

- Nevojitet të merren masa për ndarjen dhe qarkullimin e të dhënave dhe informacionit në mënyrë më të sigurt, si brenda institucioneve publike ashtu edhe atyre private, me qëllim parandalimin dhe luftën kundër krimit dhe garantimin e politikave të duhura të sigurisë.

- Rritja e ndërgjegjësimit mbi sfidat e sigurisë kibernetike, me qëllim përmirësimin e

[33] https://www.comparitech.com/vpn/vpn-statistics/
[34] https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view
[35] http://www.zdnet.com/article/businesses-take-over-six-months-to-detect-data-breaches/

politikave në këtë fushë. Kjo mund të arrihet nëpërmjet: zhvillimit të kërkimeve shkencore akademike, me qëllim që shteti shqiptar të ketë të dhënat statistikore të nevojshme, për të krijuar një qasje më të mirë të rrezikut ndaj sigurisë kibernetike, si dhe zhvillimit të kërkimeve mbi politikat e sigurisë kibernetike, me qëllim që të zbulohen mangësitë dhe arritjet; përdorimit të këtij informacioni për të rritur ndërgjegjësimin e politikëbërësve kryesorë, aktorëve në fushën e industrisë dhe publikut të gjerë; gjetjes së mënyrave kreative për të tërhequr vëmendjen e medieve dhe publikut mbi këtë fushë.

- Planifikimi i një strategjie mbrojtjeje. Për këtë, duhet: të jemi të ndërgjegjshëm që çështje të tilla komplekse kërkojnë një kohë të gjatë për t'u diskutuar, për të negociuar dhe për rënë dakord; të jemi të gatshëm të propozojmë hapa të shpejtë afatshkurtër në raste incidentesh kibernetike; t'i kushtohet kohë gjetjes së zgjidhjeve, e jo të fokusohemi vetëm në identifikimin e problemeve; të mendohet në mënyrë strategjike dhe të krijohen aktivitete më të mëdha, ku të përfshihen aktorë të ndryshëm, të cilët do të marrin pjesë në panele diskutimi mbi sigurinë.

- Në kuadër të sigurisë kombëtare kundër rreziqeve dhe sulmeve kibernetike, është thelbësor miratimi i draftstrategjisë kundër krimit kibernetik, si dhe hartimi e miratimi i ligjeve të reja në këtë kuadër. Nevojitet gjithashtu një qasje sinergjike e të gjithë aktorëve të prekur nga ky fenomen, nëpërmjet: mbledhjes së komunitetit akademik, për të punuar mbi kërkimin shkencor dhe përmirësimin e kurrikulave, në lidhje me sigurinë kibernetike dhe politikat e internetit; identifikimit të infrastrukturës kritike dhe infrastrukturës së informacionit kritik të vendit dhe të rajonit; bashkëpunimin ndërmjet industrisë dhe qeverisë mbi problematikat dhe politikat e sigurisë kibernetike, si dhe gjetjen e zgjidhjeve teknike.

- Qeveria shqiptare nevojitet të marrë masat për të ndërmarrë një qasje sinergjike e cila do të rrisë partneritetin mes sektorit publik dhe privat, në luftën kundër krimit kibernetik. Në këtë mënyrë, do të arrihet të rritet siguria e përbashkët, duke bërë të mundur përfitimin për të dy sektorët: publik dhe privat, si dhe për qytetarët, te rritja e sigurisë ndaj rreziqeve që sjell zhvillimi i teknologjisë.

- Nevojitet gjithashtu që sektori privat të kuptojë që siguria kibernetike për sektorin privat nuk ka të bëjë vetëm me krimin kibernetik apo standardet e sigurisë, por është gjithashtu thelbësore për ekonominë, dhe, që nevojitet hartimi i politikave më të gjëra për të garantuar infrastrukturë dhe trafik të sigurt. Përmirësimi i edukimit mbi sigurinë kibernetike është gjithashtu një aspekt tjetër i rëndësishëm: fëmijët dhe të rriturit duhet të përgatiten për ambientin e ri digjital; edukimi nuk duhet të përfshijë vetëm mësimin e përdorimit të pajisjeve, por duhet edhe t'u mësojë individëve se si të lundrojnë në botën digjitale të sigurt dhe në mënyrë të ndërgjegjshme.

- Fuqizimi i institucioneve ekzistuese: identifikimi i institucioneve kryesore në fushën e sigurisë kibernetike dhe sigurimi që ata të kenë staf të mjaftueshëm. Këto institucione duhet të kenë një përzierje specialistësh, të fushës juridike dhe informatike (IT), të cilët duhet të trajnohen vazhdimisht.

- Përditësimi i kurrikulave të trajnimeve kombëtare të institucioneve të administratës publike dhe akademive diplomatike.

- Fuqizimi i CERT-it kombëtar, duke mundësuar që ai të këtë kapacitetin e nevojshëm për t'iu përgjigjur çdo lloj incidenti.

- Duhet të krijohen kushtet dhe të merren masat për rritjen e bashkëpunimit dhe përfshirjes së agjencive të specializuara të zbatimit të ligjit në luftimin më adekuat të krimit kibernetik. Duhet të punohet mbi krijimin e ndërlidhjeve ndërmjet legjislacionit

dhe politikave kundër krimit kibernetik. Pra, të këtë një lidhje logjike ndërmjet strategjisë kombëtare të sigurisë kibernetike, strategjisë kombëtare të sigurisë, strategjisë së mbrojtjes kundër krimit kibernetik, legjislacionit mbi sigurinë e informacionit, mbi mbrojtjen e të dhënave dhe privatësinë, mbi shërbimet qeveritare etj. Nevojitet gjithashtu të punohet në nivel ndërkombëtar dhe rajonal nëpërmjet: identifikimit të çështjeve ndërkombëtare dhe rajonale. si p.sh. mbrojtja e infrastrukturës dhe futja e tyre në agjendën kombëtare.

- Pjesëmarrja në organizata dhe mbledhje rajonale dhe ndërkombëtare mbi sigurinë kibernetike.

- Krijimi i një grupi pune publik-privat është një tjetër hap i nevojshëm në luftimin më efikas të krimit kibernetik.

- Përmirësimi i kapaciteteve operacionale dhe reagimit të autoriteteve të zbatimit të ligjit ndaj sulmeve kibernetike. Në këtë kuadër, nevojitet rritja e numrit të ekspertëve në fushën e hetimit dhe ndjekjes penale të krimit kibernetik, nëpërmjet organizimit të shpeshtë të trajnimeve të specializuara, si dhe dërgimit të zyrtarëve përkatës për specializime jashtë vendit. Nëpërmjet këtyre trajnimeve, duhet të arrihet specializimi i ekspertëve në fushën e krimit kibernetik, njohja e tyre me legjislacionin vendas dhe ndërkombëtar të fushës dhe mbi metodat dhe mënyrat e zbatimit sa më adekuat dhe efikas të këtij legjislacioni.

Në këtë kuadër, nevojitet jo vetëm trajnimi i punonjësve ekzistues, por edhe huazimi i më shumë specialistëve në këtë fushë, pasi specialistët në fushën e luftimit të krimit kibernetik në Shqipëri janë shumë të paktë. Përveç ekspertëve ligjorë, nevojiten edhe ekspertë në fushën e teknologjisë së informacionit, të cilët duhet të jenë të pranishëm në çdo strukturë të policisë, prokurorive dhe gjykatave që merren me luftimin e krimit kibernetik, për t'i asistuar zbatuesit e ligjit me eksperiencën e duhur teknike në hetimin sa më rezultativ të sulmeve kibernetike. Duke marrë shembullin e shumë shteteve të cilat e kanë ndërmarrë këtë hap, hartimi i një ligji të posaçëm mbi krimin kibernetik do të ishte një masë tjetër shumë efikase në parandalimin dhe luftimin e këtij krimi.

Bibliografia

1. Ligji nr. 8888, datë 25.4.2002 për ratifikimin e "Konventës për krimin në fushën e kibernetikës".
2. Ligji nr. 9880, datë 25.2.2008 për "Nënshkrimin elekronik".
3. Ligji nr. 9887, datë 10.3.2008 për "Mbrojtjen e të dhënave personale".
4. Ligji nr. 9918, datë e 19.5.2008 për " Komunikimet elektronike në Republikën e Shqipërisë".
5. Kodi Penal i Republikës së Shqipërisë.
6. Vendim i Këshillit të Ministrave nr. 710, datë 21.8.2013 "Për Krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të nivelit të shërbimit.
7. Urdhër i Kryeministrit nr. 202, datë 16.12.2005 për "Forcimin e transparencës, nëpërmjet rritjes së përdorimit të internetit dhe përmirësimit të faqeve ekzistuese të internetit".
8. Vendim i Këshillit të Ministrave nr. 120, datë 20.3.2014 për "Dokumentin e politikave për sigurinë kibernetike".
9. Konventa e Këshillit të Europës mbi "Kriminalitetin kompjuterik", 23 nëntor 2001.
10. Begaj, Eranda, Albania's vision towards Cyber Security, DCAF Young Faces, 2014.
11. European Commission, Legal Aspects of Computer, janar 1998.
12. European Commission, Cybercrime strategy of the European Union, Brussels, 2013.
13. Gercke, M, Understanding Cybercrime, Switzerland, 2011.
14. Kshetri, Nir, The Global Cybercrime Industry, USA, 2010.
15. Moore, Robert, Investigating High Technology Computer Crime, USA, 2011.
16. Vula, Veton, Kriminaliteti kompjuterik si formë e re e fenomelogjisë kriminale, Prishtinë, 2011.
17. Yar, Majid, Cybercrime and Society, India, 2013.

18. Wall, David, The Transformation of the Crime in the Information Age, UK, 2007
19. http://www.taxpayer.net/library/article/cyberspending-databas
20. https:// www.microsoft.com/en-us/cloud-platform/advanced-threat-analytics
21. https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion
22. https://www.symantec.com/security-center/threat-report
23. https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new
24. https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html
25. https://www.csoonline.com/article/3200024/security/cybersecurity-labor-crunch-to-hit-35-million-unfilled-jobs-by-2021.html
26. http://www.businessinsider.com/ëarren-buffett-cybersecurity-berkshire-hathaway-meeting-2017-5
27. https://www.pandasecurity.com/mediacenter/press-releases/all-recorded-malware-appeared-in-2015/
28. https://www.fbi.gov/file-repository/ransomëare-prevention-and-response-for-cisos.pdf/view
29. http://www.businessinsider.com/expert-phishing-emails-2016-8?IR=T
30. https://www.venafi.com/assets/pdf/wp/Venafi_2016CIO_SurveyReport.pdf
31. http://www.zdnet.com/article/businesses-take-over-six-months-to-detect-data-breaches/
32. https://www.computerworld.com/article/2475964/mobile-security/98–of-mobile-malëare-targets-android-platform.html
33. https://swimlane.com/10-hard-hitting-cyber-security-statistics/
34. https://www.esecurityplanet.com/network-security/over-80-percent-of-americans-are-more-worried-about-privacy-security-than-a-year-ago.html
35. https://www.comparitech.com/vpn/vpn-statistics/
36. https://www.techinasia.com/indonesia-world-leader-vpn-usage

Bashkëpunimi ndërkombëtar për parandalimin e sulmeve kibernetike

Dr. Eldjona SHUKALLARI[1]
Kolegji ISPE, Prishtinë
eldjona.shukallari@planet-albania.com

Abstrakt

Teknologjia e informacionit dhe komunikimit (TIK) paraqet një nga sfidat më aktuale për sigurinë globale. Në një botë gjithnjë e më shumë digjitale dhe të ndërlidhur, mbrojtja e qytetarëve të BE nga kërcënimet kibernetike është një përparësi kryesore. Masat e reja të propozuara, synojnë të rrisin bashkëpunimin për sigurinë kibernetike brenda BE-së dhe në nivel global, të nxisin risi, dhe të investojnë në ndërgjegjësimin dhe ndërtimin e kapaciteteve. Paralelisht, BE dhe NATO, po kryejnë stërvitje të koordinuara për të testuar aftësinë e tyre për t'iu përgjigjur kërcënimeve kibernetike dhe hibride. Kërcënimet [2] kryesore të sigurisë së kibernetikës kërkojnë bashkëpunimin urgjent ndërkombëtar. Në të vërtetë, kërcënimet kibernetike janë më të larmishme dhe më komplekse, shpesh, duke synuar ndërmarrjet private dhe duke rrezikuar integritetin teknik të botës digjitale[3]. Legjislacioni i kohëve të fundit, siç është Direktiva e vitit 2016 e Parlamentit Europian për sigurinë e sistemeve të rrjetit dhe informacionit, u fokusua gjerësisht në kërcënimet ndaj infrastrukturës kritike dhe kishte për qëllim përmirësimin e sigurisë në kibernetike për të mbrojtur të ashtuquajturat shërbime thelbësore si tregjet në internet, motorët e kërkimit dhe shërbimet e informatikës, që janë jetike për bizneset, qeveritë dhe qytetarët[4]. "Qasja e BE-së ndaj sigurisë kibernetike, i jep përparësi zgjidhjes së mosmarrëveshjeve në hapësirën kibernetike, me mjete paqësore. Megjithatë, BE-ja do të rrisë kapacitetin e saj për t'iu përgjigjur kërcënimeve kibernetike. Aty ku është e nevojshme, masat kufizuese mund të merren në përgjigje të aktiviteteve kibernetike me qëllim keqdashës"[5].

Fjalëkyçe:
sulme kibernetike, siguria kibernetike në Shqipëri, strategjia e mbrojtjes kibernetike, politika kibernetike, BE, NATO.

1. Hyrje

Sulmi kibernetik është tashmë një nga sfidat më të mëdha ligjore. Sulm kibernetik[6] quhet një sulm i qëllimshëm në sistemet kompjuterike, si dhe ndaj ndërmarrjeve të cilat kanë akses në internet. Sulmi kibernetik është një aktivitet kriminal, që përfshin: infrastrukturën e teknologjisë së informacionit, aksesin e paligjshëm, përgjimin e paligjshëm, ndërhyrjen e të dhënave, falsifikimin dhe mashtrimin elektronik. Hapësira kibernetike është një nga sfidat më të mëdha ligjore, e cila ka nxitur një formë tjetër të krimit, duke krijuar një mjedis për metodat e reja të krimit.

"Krimi kibernetik është përcaktuar si një krim në të cilin një kompjuter është objekt i krimit (*hacking*, *phishing*, *spamming*) ose përdoret si një mjet për të kryer një vepër penale. Kriminelët kibernetikë mund të përdorin teknologjinë kompjuterike për të pasur akses në të dhënat personale ose përdorin internetin për qëllime shfrytëzuese ose keqdashëse"[7].

[1] Dr. Eldjona Shukallari, mban gradën shkencore "doktor" në shkenca politike dhe marrëdhënie ndërkombëtare, nga Universiteti i Studimeve të Barit Itali. Pedagoge, Universiteti Publik Tiranë, Fakulteti i Shkencave Sociale. Drejtore e shoqatës *Social Studies Albania*. Këshilltare për zhvillimin e biznesit tek *Planet Albania*, Tiranë; Pedagoge në Kolegjin ISPE, Prishtinë.

[2] Kërcënimet në rritje mund të shkaktojnë dëme masive ekonomike dhe shoqërore.

[3] Digjitalizimi pothuajse total i modeleve të biznesit e bën ekonominë globale më të prekshme ndaj sulmeve kibernetike, jo vetëm nga shtetet, por edhe nga organizatat kriminale dhe aktorët e tjerë jo shtetërorë.

[4] Çdo ndërprerje e madhe në këto shërbime mund të shkatërrojë modelet ekzistuese të biznesit dhe të gjenerojë kosto të mëdha operacionale.

[5] https://eeas.europa.eu/topics/eu-international-cyberspace-policy/32160/eu-drives-international-cooperation-cybersecurity-tests-ability-respond-threats_en

[6] https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en.

[7] http://www.ekon.al/2015/09/01/rendesia-e-sigurise-kibernetike-roli-i-alcirt/.

Sulmet kibernetike ndahen në disa kategori. Ato mund të përmblidhen duke u bazuar në tre lloje të përgjithshme sipas Brenner:

a. sulme ndaj kompjuterëve (*hacking*, përhapja e viruseve),

b. sulmet duke përdorur kompjuterin (mashtrimet *online*),

c. manipulimi me të dhëna për aktivitete kriminale. Pra, këto sulme kryhen me anë të internetit, duke e përdorur atë[8].

Mbrojtja kibernetike është një mekanizëm mbrojtës i rrjetit kompjuterik që përfshin reagimin ndaj veprimeve dhe mbrojtjen e infrastrukturës dhe sigurimin e informacionit për organizatat, entitetet qeveritare dhe rrjetet e tjera të mundshme. Mbrojtja kibernetike përqendrohet në parandalimin, zbulimin dhe sigurimin e përgjigjeve në kohë ndaj sulmeve ose kërcënimeve në mënyrë që asnjë informacion të mos ngatërrohet. Mbrojtja kibernetike kryen analiza teknike, për të identifikuar shtigjet dhe fushat që sulmuesit mund të synojnë. Gjithashtu, garanton sigurinë e nevojshme për të drejtuar aktivitetet pa u frikësuar për kërcënime dhe ndihmon në përmirësimin e përdorimit të burimeve strategjike të sigurisë, në mënyrë efektive.

2. Mbrojtja ndaj sulmeve kibernetike

Siguria kibernetike lufton krimin kibernetik, merret me zbulimin e sulmeve dhe përpjekjet e mashtrimit, merret me monitorimin, vlerësimin e rrezikut. Sfidat e sigurisë për sistemet e ndërlidhjes dhe informacionit përfshijnë të gjitha nivelet e strukturave duke filluar nga pajisjet individuale, që përdoren në mjediset zyrtare të punës, deri në sigurimin e sistemeve themelore, të cilat janë kritike për mbarëvajtjen e punës. Disa nga sfidat që karakterizojnë këtë situatë dhe orientimi i tyre për të ardhmen përfshijnë[9]:

- *Interneti dhe pajisjet mobile:* zhvillimi i internetit dhe i sistemeve të reja kompjuterike, sistemet industriale të kontrollit, telefonat mobile, pajisjet magazinuese të lëvizshme (memory stick) dhe tabletat, na bëjnë më shumë efiçent, por edhe më shumë të pambrojtur në mjedisin ku ushtrojmë detyrat funksionale;

- *Rrjetet sociale dhe portalet:* një sfidë e veçantë për shoqëritë e hapura është përdorimi i komunikimit digjital për të ndikuar në mendimin e publikut, për shembull nëpërmjet përpjekjeve të fshehura për të ndikuar në diskutimet mbi mediet sociale dhe duke manipuluar informacionet në portalet e lajmeve. Kjo qasje tashmë ka fituar një rëndësi të veçantë si një element i luftës hibride;

- *Komunikimi dhe transmetimi i informacionit:* rrjeti i MM-së dhe FA-së nuk është i mbyllur në një mjedis të kufizuar. Komunikimet elektronike me struktura të tjera të administratës publike, brenda dhe jashtë vendit, përbëjnë një sfidë më vete për shkak të kushteve, rrezikut të dyanshëm, ligjeve e rregullave të ndryshme, të cilat e bëjnë shumë të vështirë që strukturat e MM-së dhe FA-së të ushtrojnë kontroll mbi to;

- *Krijimi i marketit të krimit kibernetik:* zhvillimi i një marketi të padukshëm, lehtësisht të aksesueshëm, për blerje dhe shitje informacioni, si dhe tregtimin e mjeteve për krimin kibernetik, ka krijuar lehtësira për kriminelët që të shfrytëzojnë këtë mundësi, gjithnjë e më shumë në rritje, për përfitime dhe qëllime keqdashëse.

- *Spiunazhi dhe sabotimi:* objektivat ushtarake janë e do të jenë gjithnjë e më shumë

[8] https://www.consilium.europa.eu/en/policies/cyber-security/.

[9] Strategjia për mbrojtjen Kibernetike 2018-2020. http://www.mod.gov.al/images/PDF/2017/Strategjia_Mbrojtjen_Kibernetike_2018_2020.pdf.

pikësynim i sulmeve (*hacking*) dhe për këtë arsye spiunazhi dhe sabotazhi na bëjnë më ndjeshëm për të rënë pre e sulmeve elektronike ndaj sistemeve të informacionit dhe të komunikimit.

- *Privatësia dhe identiteti:* privatësia personale është gjithashtu e kërcënuar për shkak të metodave të reja të komunikimit dhe mënyrave të përdorimit të sistemeve të informacionit dhe internetit. Abuzimi me identitetin është një sfidë në rritje për çdo individ dhe autoritetet institucional.

- *Anonimati dhe atributet:* hapësira kibernetike nuk ka kufij fizikë. Sulmuesit në fushën kibernetike janë të ndryshëm dhe vështirësia për t'u identifikuar ua bën punën më të lehtë (nga hakerat individual deri në grupet e organizuara kriminale dhe deri në shtete), p.sh. hakerat dhe kriminelët kibernetikë mund të përdorin avantazhin e metodave për të lëshuar sulme të cilat janë të pagjurmueshme dhe të vështira për t'u eliminuar.

- *Asimetria e luftës kibernetike:* në 300 milisekonda, një goditje në tastiere mund të udhëtojë dy herë përreth botës por, nga ana tjetër kërkuesit shkencorë për të identifikuar një sulmues në hapësirën kibernetike mund të shpenzojnë javë të tëra, muaj deri në vite. Kundërmasat janë gjithmonë të vonuara dhe hakerat gjejnë dobësitë dhe i shfrytëzojnë ato për interes të tyre.

- *Kufizimet financiare:* kufizimet financiare janë sfida më madhore e mundshme. Duke konsideruar që mbrojtja kibernetike për shumë vende dhe organizata, është e vendosur si prioritet në koncept dhe strategji, investimet në "mbrojtjen kibernetike" është e nevojshme të jenë në nivelin që i korrespondon riskut aktual.

3. Siguria kibernetike në Shqipëri

Strategjia e Sigurisë Kombëtare (SSK) është dokumenti më themelor planifikues për sigurinë kombëtare në Republikën e Shqipërisë. Qëllimi i saj[10], është të udhëheqë vendin në përmbushjen e përparësive kombëtare të sigurisë nëpërmjet një procesi planifikimi dhe vendimmarrjeje strategjike. Zbatimi i kësaj strategjie kërkon angazhim dhe qasje mbarëkombëtare. SSK thekson idealet dhe vlerat kombëtare dhe kërkon kontributin e çdo shqiptari për të garantuar përmbushjen dhe vazhdimësinë e tyre. Siguria kibernetike varet nga aftësia e shteteve dhe institucioneve për të mbrojtur hapësirën e tyre kibernetike, si në mënyrë kolektive dhe individuale[11].

Hapësira kibernetike, është një fushë në të cilën, si aktorët privatë, edhe ata publikë, civilë dhe ushtarakë, kombëtarë dhe ndërkombëtarë, duhet të veprojnë në të njëjtën kohë dhe të jenë reciprokisht të varur nga njëri-tjetri. Teknikat e përdorura nga sulmuesit, kryesisht janë të ngjashme dhe të dizajnuara për të shfrytëzuar dobësitë e përgjithshme të rrjeteve dhe sistemeve.

Duke u fokusuar te Strategjia për Mbrojtjen Kibernetike 2018-2020, si qëllim kryesor ajo cilëson, mbajtjen e një hapësire kibernetike të besueshme e të sigurt, për Ministrinë e Mbrojtjes dhe Forcat e Armatosura, për realizimin e misionit dhe të detyrave të tyre.

[10] Strategjia e Sigurisë Kombëtare 2014.
http://www.mod.gov.al/images/PDF/strategjia_sigurise_kombetare_republikes_se_shqiperise.pdf.
[11] Po aty.
[12] Strategjia për mbrojtjen Kibernetike 2018-2020.
http://www.mod.gov.al/images/PDF/2017/Strategjia_Mbrojtjen_Kibernetike_2018_2020.pdf.

4. Parimet bazë ku mbështetet strategjia e mbrojtjes kibernetike[12]

- *Zhvillimi:* nëpërmjet zhvillimit të qëndrueshëm dhe sistematik të aftësive, teknologjisë së komunikimit dhe informacionit dhe të masave të sigurisë është e mundur të mbrohemi kundër kërcënimeve kibernetike.

- *Përgjegjësisë:* pakësimi i rreziqeve është i mundur vetëm nëse të gjitha strukturat dhe personeli i MM/FA-së, të përfshira në hapësirën kibernetike, janë të informuar dhe të ndërgjegjësuar për pasojat që rrjedhin nga veprimi ose mosveprimi i tyre në pjesën për sigurinë që u përket atyre dhe në sigurinë e të tjerëve.

- *Bashkëpunimi:* mbrojtja efektive kundër kërcënimeve në hapësirën kibernetike, e pakufizuar nga ndarje administrative me institucione ose struktura të tjera të shtetit, është e mundur vetëm nëpërmjet bashkëpunimit në nivel kombëtar e ndërkombëtar.

- *Ligji dhe standardet:* mbrojta kibernetike efektive realizohet nëpërmjet zbatimit rigoroz të përcaktimeve ligjore, politikave, standardeve dhe udhëzimeve përkatëse.

- *Kapacitetet:* realizimi i mbrojtjes kibernetike efektive arrihet duke pasur burimet e nevojshme njerëzore dhe ato të teknologjisë përkatëse.

- *Strategjitë:* "Strategjia e sigurisë kombëtare" dhe "Strategjia ushtarake" i vlerësojnë sulmet kibernetike si kërcënime, rreziqe dhe sfida jokonvencionale.

4.1 Politika që do të ndiqen

1. Zbatimi i masave të plota organizative dhe teknike të sigurisë kibernetike në sistemet e komunikimit dhe të informacionit (SKI).

2. Rritja e përgjegjësisë së strukturave të MM/FA-së për sigurinë kibernetike.

3. Zhvillimi i nivelit dhe aftësive të specialistëve të sigurisë kibernetike dhe të përdoruesve të SKI-ve.

4. Rritja e bashkëpunimit me strukturat përgjegjëse në nivel kombëtar dhe në kuadrin e NATO-s[13].

Në nivel kombëtar merr rëndësi bashkëpunimi me sektorin publik, si universitetet, dhe me sektorin privat në fushën e kërkimit, zhvillimit dhe trajnimit të personelit. Në nivel ndërkombëtar,[14] objektivi parësor për Ministrinë e Mbrojtjes është bashkëpunim me vendet, që aspirojnë dhe veprojnë në nivele të ngjashme sigurie, zhvillimi i përbashkët i mjeteve, aftësive dhe teknikave. Ministria e Mbrojtjes do të bashkëpunojë me NATO-n për forcimin e mbrojtjes kibernetike, nëpërmjet kontributit në zhvillimin dhe zbatimin e politikave të NATO-s dhe përmirësimit të mbrojtjes së sistemeve dhe rrjeteve të veta, si dhe ato të aleatëve.

5. Dimensioni ndërkombëtar i sulmit kibernetik

Për të luftuar krimin kibernetik, BE ka zbatuar legjislacionin dhe ka mbështetur bashkëpunimin operacional, si pjesë e Strategjisë së Kibernetikës së BE-së.

[13] Po aty.
http://www.mod.gov.al/images/PDF/2017/Strategjia_Mbrojtjen_Kibernetike_2018_2020.pdf
[14] Strategjia për mbrojtjen Kibernetike(CYBER DEFENSE), Ministria e Mbrojtjes
http://www.mod.gov.al/images/PDF/Strategjia_per_Mbrojtjen_Kibernetike.pdf

Strategjia bazohet në pesë parime që do të jenë përparësi për të ardhmen e Bashkimit Evropian. Është shumë e rëndësishme të theksohet njohja që komunikimet zyrtare të BE-së gjithashtu theksojnë: siguria kibernetike është po aq e rëndësishme sa siguria në hapësirën fizike. Pesë parimet e tij (prioritetet) janë si në vijim[15]:

- arritja e qëndrueshmërisë kibernetike,
- reduktimi në mënyrë drastike i krimit kibernetik,
- zhvillimi i politikave dhe aftësive të mbrojtjes kibernetike në lidhje me Politikën e Përbashkët të Sigurisë dhe Mbrojtjes,
- zhvillimi i burimeve industriale dhe teknologjike për sigurinë kibernetike,
- ngritja e një politike koherente ndërkombëtare për hapësirën kibernetike për Bashkimin Evropian dhe promovimi i vlerave thelbësore të BE-së.

Strategjia thekson unitetin e autoriteteve publike dhe të sektorit privat, si dhe zhvillimin e kapaciteteve kibernetike, resurseve dhe efikasitetit. Strategjia ka një rol të veçantë dhe të rëndësishëm për ENISA (Agjencia e Bashkimit Evropian për Rrjetin dhe Sigurinë e Informacionit) për të forcuar elasticitetin kibernetik në të gjithë Shtetet Anëtare. Strategjia[16] thekson se, megjithëse ka përparim në këtë fushë, domethënë krijimi i elasticitetit të koordinuar si një prioritet, ende ekzistojnë boshllëqe serioze në shumë shtete anëtare, kryesisht në aspektin e aftësive kombëtare, koordinimin në trajtimin e incidenteve kibernetike ndërkufitare, ose promovimin e zonave të gatishmërisë së sektorit privat. Në shtator 2017, Komisioni Europian (KE) propozoi propozime të reja për të përmirësuar strukturat e sigurisë kibernetike të Bashkimit Evropian (BE) dhe për të ndërtuar një elasticitet më të madh dhe autonomi strategjike në këtë fushë[17].

Paketa e Kibernetikës së BE-së propozon tri shtylla për veprim: elasticitetin, parandalimin dhe mbrojtjen. Këshilli, e vë theksin në ndërtimin e një autonomie më të madhe strategjike dhe dëshiron të rrisë aftësitë, në aspektin e teknologjisë dhe aftësive, së bashku me ndërtimin e një tregu të fortë, të vetëm, në fushën e sigurisë kibernetike. Lidhur me ndërtimin e elasticitetit më të madh, KE fillimisht këmbëngul për zbatimin e plotë të Direktivës së Sistemeve të Rrjetit dhe Informacionit (NIS), nga shtetet anëtare, si një parakusht thelbësor për elasticitetin kibernetik. Direktiva e NIS është pjesa e parë e legjislacionit të BE-së mbi sigurinë kibernetike. Brenda strategjisë së re dhe ndërtimit të Direktivës së NIS, KE synon së pari të përmirësojë elasticitetin kibernetik të BE-së, duke promovuar, se me një besim të përbashkët, siguria kibernetike është një sfidë e përbashkët shoqërore. KE-ja kërkon që shtetet anëtare, tani, ta përfshijnë sigurinë kibernetike si pjesë të kurrikulave të trajnimit akademik dhe profesional. Ajo, rekomandon gjithashtu përhapjen e fushatave informuese për sigurinë kibernetike, për ta dhënë mesazhin te të gjithë.

Përveç kësaj, për të zvogëluar mungesën e shkathtësive dhe për të ruajtur një autonomi strategjike, KE propozon ngritjen e një qendre kërkimi dhe kompetence të kibernetikës[18] së BE-së, duke përfshirë iniciativa të tilla si skemat e mësimit në sigurinë kibernetike për NVM-të dhe duke u mbështetur në nismat kombëtare. Në nivelin e sektorit të industrisë, KE argumenton në favor të qasjes së "sigurisë sipas projektimit";

[15] https://www.orange.com/en/content/download/44597/1336574/version/2/file/Le%20paquet%20cybersecurite _VA_CLEAN.pdf.
[16] "Cyber security in the European Union". http://www.europarl.europa.eu/eplibrary/Cyber-security-in-the-European%20Union.pdf.
[17] https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-477-F1-EN-MAIN-PART-1.PDF
[18] Po aty.

me fjalë të tjera, pajisjet e projektuara nga toka, deri sa të jenë të sigurta.

5.1 Një vizion global për strategjinë e sigurisë kibernetike dhe bashkëpunimin e mbrojtjes

Ndërsa bota digjitale nuk njeh kufij, KE-ja do t'i japë përparësi shkëmbimit të informacionit ndërkufitar në Evropë dhe më gjerë, si dhe promovimit të një bashkëpunimi ndërkombëtar të forcuar, për të lehtësuar parandalimin e sulmeve kibernetike. KE dëshiron të ndërtojë dhe të mbajë aleanca me vendet e treta, në mënyrë që të promovojë stabilitetin kibernetik global. Në anën tjetër, përmes një "Toolbox për Cyber Diplomacinë"[19], brenda kuadrit të instrumenteve të përbashkët të politikës së jashtme dhe të sigurisë, BE ka deklaruar se ishte e gatshme të përgjigjet me një sërë masash, përfshirë sanksionet, nëse aktorët shtetërorë dhe joshtetërorë duhej të kërcënonin integritetit të hapësirës kibernetike evropiane. Lidhur me bashkëpunimin për mbrojtjen kibernetike, KE do të dëshironte gjithashtu të shihte një bashkëpunim të forcuar midis BE-së dhe NATO-s, nëpërmjet trajnimeve dhe stërvitjeve të përbashkëta, me ndërveprimin e standardeve të sigurisë kibernetike.

5.2 Ruajtja e politikave dhe strategjive koherente në nivel evropian.

Koherenca është një sfidë e madhe për politikat e BE-së në lidhje me sigurinë kibernetike. Koherenca e politikave dhe strategjive duhet të përfshijë të gjitha institucionet dhe organet e BE-së. Të gjithë mbajtësit e informatave në nivel të BE-së koordinojnë dhe planifikojnë ndërtimin e kapaciteteve aktuale dhe të ardhshme në[20]:

- reagimin në internet;
- mbrojtjen e infrastrukturës kritike;
- menaxhimin e krizave;
- mbrojtjen e sigurisë;
- qëndrueshmërinë kibernetike.

6. Zhvillimi i politikave dhe aftësive të kibernetikës në lidhje me kornizën e "Politikës së përbashkët të sigurisë dhe mbrojtjes" (PSDK)

Përpjekjet e sigurisë në internet, në BE, përfshijnë gjithashtu dimensionin e mbrojtjes kibernetike. Për të rritur elasticitetin e sistemeve të komunikimit dhe informacionit që mbështesin mbrojtjen e shteteve anëtare dhe interesat e sigurisë kombëtare, zhvillimi i aftësive kibernetike duhet të përqendrohet në zbulimin, reagimin dhe rikuperimin nga kërcënimet e sofistikuara kibernetike. Përfaqësuesi i Lartë, do të përqendrohet në aktivitetet kryesore në vijim dhe do të ftojë shtetet anëtare dhe Agjencinë Evropiane të Mbrojtjes, të bashkëpunojnë duke u fokusuar te këto çështje[21]:

a) Vlerësimi i kërkesave operacionale të BE-së, për mbrojtjen e internetit dhe promovimi i zhvillimit të aftësive dhe teknologjive të BE-së për të adresuar të gjitha

[19] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013JC0001.
[20] "Cyber defence in the EU" http://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU- FINAL.pdf.
[21] Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks. Directorate-General for External Policies of the Union, Directorate B, Policy Department, European Parliament.

aspektet e zhvillimit të aftësive - duke përfshirë doktrinën, udhëheqjen, organizimin, personelin, trajnimin, teknologjinë, infrastrukturën, logjistikën dhe ndërveprimin.

b) Të zhvillojë kornizën e politikave të BE-së për mbrojtjen e kibernetikës, për të mbrojtur rrjetet brenda misioneve dhe operacioneve të PSDK-së, duke përfshirë menaxhimin dinamik të rrezikut, analizën e përmirësuar të kërcënimeve dhe shkëmbimin e informacionit. Përmirësimi i trajnimit dhe stërvitjeve të mbrojtjes kibernetike për ushtrinë, në kontekstin evropian dhe multinacional, duke përfshirë integrimin e elementeve të mbrojtjes kibernetike në katalogët ekzistues të stërvitjeve.

c) Promovimi i dialogut dhe koordinimit ndërmjet aktorëve civilë dhe ushtarakë në BE - me theks të veçantë në shkëmbimin e praktikave të mira, shkëmbimit të informacionit dhe paralajmërimit të hershëm, reagimit të incidenteve, vlerësimit të rrezikut, ndërgjegjësimit dhe vendosjes së sigurisë kibernetike si prioritet.

d) Sigurimi i dialogut me partnerët ndërkombëtarë, duke përfshirë NATO-n, organizatat e tjera ndërkombëtare dhe qendrat shumëkombëshe të ekselencës, për të siguruar aftësi efektive të mbrojtjes, për të identifikuar fushat për bashkëpunim dhe për të shmangur dyfishimin e përpjekjeve.

7. Koordinimi ndërmjet autoriteteve kompetente, zbatimit të ligjit dhe mbrojtjes në nivelin kombëtar, nivelin e BE-së dhe nivelin ndërkombëtar.

7.1 Niveli kombëtar [22]

Shtetet anëtare duhet të kenë, strukturat për t'u marrë me elasticitetin kibernetik, krimin kibernetik dhe mbrojtjen; dhe ata duhet të arrijnë nivelin e kërkuar të aftësisë për t'u marrë me incidentet kibernetike. Sidoqoftë, duke qenë se një numër i entiteteve mund të kenë përgjegjësi operacionale mbi dimensione të ndryshme të sigurisë kibernetike dhe duke pasur parasysh rëndësinë e përfshirjes së sektorit privat, koordinimi në nivel kombëtar duhet të optimizohet nëpër ministri. Shtetet anëtare duhet të përcaktojnë në strategjitë e tyre kombëtare të sigurisë kibernetike rolet dhe përgjegjësitë e subjekteve të ndryshme kombëtare.

Shkëmbimi i informacionit midis subjekteve kombëtare dhe sektorit privat duhet të inkurajohet, për t'u mundësuar shteteve anëtare dhe sektorit privat që të kenë një pamje të përgjithshme të kërcënimeve të ndryshme dhe të kuptojnë më mirë, prirjet dhe teknikat e reja të përdorura, si për të kryer sulme kibernetike, dhe për të reaguar për ata më shpejt. Duke vendosur plane bashkëpunimi kombëtare për t'u aktivizuar në rastet e incidenteve kibernetike, shtetet anëtare duhet të jenë në gjendje të ndajnë në mënyrë të qartë rolet dhe përgjegjësitë, dhe të zgjedhin veprimet e reagimit.

7.2 Niveli i BE-së[23]

Ashtu si në nivel kombëtar, në nivel të BE-së ka një numër aktorësh që merren me sigurinë kibernetike. Në veçanti, ENISA, Europol / EC3 dhe EDA janë tre agjenci aktive nga perspektiva e NIS, zbatimit të ligjit dhe mbrojtjes, respektivisht. Këto agjenci kanë Bordet e Administrimit ku përfaqësohen shtetet anëtare dhe ofrojnë platforma

[22] National Cyber Security Strategies Good Practice Guide - updated. Good Practice Guide, EU: ENISA. https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

[23] http://www.armyacademy.ro/reviste/rev1_2018/KOVACS.pdf.

për koordinim në nivel të BE.

Koordinimi dhe bashkëpunimi do të inkurajohen midis ENISA, Europol / EC3 dhe EDA në një numër fushash ku ato janë të përfshira bashkërisht, veçanërisht në drejtim të analizës së tendencave, vlerësimit të rrezikut, trajnimit dhe shkëmbimit të praktikave më të mira. Ata duhet të bashkëpunojnë duke ruajtur specifikat e tyre. Këto agjenci së bashku me CERT-EU, Komisionin dhe shtetet anëtare, duhet të mbështesin zhvillimin e një komuniteti të besuar ekspertësh teknikë dhe politikë në këtë fushë.

Kanalet joformale për koordinim dhe bashkëpunim, do të plotësohen nga lidhjet më strukturore. Stafi ushtarak i BE-së dhe ekipi i projektit të mbrojtjes kibernetike të EDA-s, mund të përdoren si vektorë për koordinim në mbrojtje.

7.3 Niveli ndërkombëtar[24]

Komisioni dhe Përfaqësuesi i Lartë sigurojnë, së bashku me shtetet anëtare, koordinimin e veprimeve ndërkombëtare në fushën e sigurisë kibernetike. Duke vepruar kështu, Komisioni dhe Përfaqësuesi i Lartë do të mbështesin vlerat thelbësore të BE-së dhe do të promovojnë një përdorim të qetë, të hapur dhe transparent të teknologjive kibernetike. Komisioni, Përfaqësuesi i Lartë dhe shtetet anëtare angazhohen në dialogun e politikave me partnerët ndërkombëtarë dhe me organizatat ndërkombëtare si Këshilli i Evropës, OECD, OSBE, NATO dhe OKB.

[24] National-level Risk Assessments: An Analysis Report. Survey, Athens: ENISA. https://www.enisa.europa.eu/publications/nlra-analysis-report.

Biblografia

1. http://www.epc.eu/dsm/2/Study_by_Copenhagen.pdf
2. COM(2009) 277, Communication from the Commission to the European Parliament and the Council on "Internet Governance: the next steps"
3. In 2001, the Commission adopted a Communication on "Network and Information Security: Proposal for A European Policy Approach" (COM(2001)298); in 2006, it adopted a Strategy for a Secure Information Society (COM(2006)251). Since 2009, the Commission has also adopted an Action Plan and a Communication on Critical Information Infrastructure Protection (CIIP) (COM(2009)149, endorsed by Council Resolution 2009/C 321/01; and COM(2011)163, endorsed by Council Conclusions 10299/11).
4. Regulation (EC) No 460/2004
5. COM(2010)521. The actions proposed in this Strategy do not entail amending the existing or future mandate of ENISA.
6. Article 13a&b of Directive 2002/21/EC
7. Article 17 of Directive 95/46/EC; Article 4 of Directive 2002/58/EC
8. https://ec.europa.eu/digital-agenda/en/connecting-europe-facility. CEF Budget line 09.03.02 – Telecommunications networks (to promote the interconnection and interoperability of national public services on-line as well as access to such networks).
9. CIP-ICT PSP-2012-6, 325188. It has an overall budget of 15 Million Euro, with EU funding amounting to 7.7 Million Euro.
10. http://www.trustindigitallife.eu/
11. Directive 2011/93/EU replacing Council Framework decision 2004/68/JHA
12. 28 March 2012, the European Commission adopted a Communication "Tackling Crime in a Digital Age: Establishing a European Cybercrime Centre"
13. COM(2012) 196 final
14. Council Conclusions on a Global Alliance against Child Sexual Abuse Online (EU-US Joint Statement) of 7th and 8th June 2012 and Declaration on the launch of the Global Alliance against Child Sexual Abuse Online (http://europa.eu/rapid/press-release_MEMO-12-944_en.htm)
15. Commission Staff Working Document Impact Assessment accompanying the Commission proposal for a Directive on network and information security, Section 4.1.5.2
16. Horizon2020 is the financial instrument implementing the Innovation Union, a Europe 2020 flagship initiative aimed at securing Europe's global competitiveness. Running from 2014 to 2020, the EU's new Framework Programme for research and innovation will be part of the drive to create new growth and jobs in Europe.
17. A renewed EU strategy 2011-14 for Corporate Social Responsibility; COM(2011) 681 final
18. National-level Risk Assessments: An Analysis Report. Survey, Athens: ENISA. https://www.enisa.europa.eu/publications/nlra-analysis-report.
19. National Cyber Security Strategies Good Practice Guide - updated. Good Practice Guide, EU: ENISA. https://www.enisa.europa.eu/publications/ncss-good-practice-guide
20. http://www.armyacademy.ro/reviste/rev1_2018/KOVACS.pdf
21. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013JC0001
22. "Cyber defence in the EU" http://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU- FINAL.pdf
23. https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-477-F1-EN-MAIN-PART-1.PDF
24. https://www.orange.com/en/content/download/44597/1336574/version/2/file/Le%20paquet%20cybersecurite_VA_CLEAN.pdf
25. "Cyber security in the European Union."http://www.europarl.europa.eu/eplibrary/Cyber-security-in-the-European%20Union.pdf.

Terrorizmi kibernetik

■**MSc. Enea SHEQI**
Universiteti i Tiranës, Fakulteti i Drejtësisë
enea.sheqi@yahoo.com

Abstrakt

Përdorimi i internetit në botën e globalizuar krahas të gjithë risive pozitive ka sjellë dhe disa pasoja negative. Krimi kibernetik duket i pashmangshëm, por reagimi ndaj tij është i domosdoshëm dhe i menjëhershëm. Veprat me natyrë terroriste në kohët e fundit janë në rritje dhe po synojnë që të gjejnë forma e mënyra të reja. Përdorimi i hapësirës elektronike për të kryer këto krime, po i shërben edhe më shumë terroristëve në të gjithë botën. Sfida ndaj kësaj vepre është gjithëpërfshirëse dhe reagimi ndaj parandalimit të terrorizmit kibernetik, kërkon bashkëpunim në nivel ndërkombëtar për të luftuar përhapjen e mëtejshme, të këtij krimi të sofistikuar. Në vijim të punimit do të bëhet një analizë e thelluar e terrorizmit kibernetik, formave dhe mënyrave të kryerjes së tij, kuadrit ligjor shqiptar dhe ndërkombëtar në kuadër të luftimit dhe parandalimit të tij, si dhe kërkesave për hartimin e strategjive afatgjata për të mbrojtur rendin dhe sigurinë kombëtare. Gjithashtu, do të bëhet një krahasim në rrafshin ndërkombëtar, për të përfituar nga praktikat më të mira në kuadër të luftës ndaj terrorizmit dhe krimit kibernetik.

Fjalëkyçe:
terrorizmi kibernetik, parandalim, strategji, siguri kombëtare.

1. Hyrje

Terrorizmi kibernetik ndonëse një term tepër i ri dhe mjaft i dëgjuar, ka pasur disa përkufizime të ndryshme nga autorë të ndryshëm. Një përkufizim i cili do të përfaronte disi mendimet në këtë fushë do të ishte: "Terrorizmi kibernetik rrjedh nga konvergjenca e terrorizmit dhe hapësirës kibernetike. Ai nënkupton sulmet dhe kërcënimet e paligjshme ndaj kompjuterëve, sistemeve kompjuterike dhe informacioneve të rezervuara në këto sisteme për të intimiduar një pjesë të shtetit/qeverisë apo njerëzve të saj, me synimin e arritjes së objektivave politike apo sociale. Kështu që një sulm të klasifikohet si pjesë e terrorizmit kibernetik, duhet që t'i jetë drejtuar një personi apo pasurisë, apo të shkaktojë një dëm që sjellë frikë dhe panik. Sulmet kundër infrastrukturës mund të jenë shembuj të terrorizmit kibernetik nëse kanë pasoja mjaft të rënda"[1].

Terrorizmi kibernetik është një term mjaft kontrovers, kjo edhe për shkak të vështirësisë së dallimit të tij nga krimet e tjera kibernetike. Terrorizmi kibernetik gjithashtu po merr përmasa edhe më të mëdha për shkak të disa arsye që lidhen me natyrën e këtij krimi. Ky krim nuk kërkon kosto të lartë, në krahasim me metodat e tjera terroriste. Pra, praktikisht e vetmja gjë që nevojitet është një kompjuter dhe aksesi në internet i tij, për të shkaktuar dëme të mëdha. Gjithashtu, terrorizmi kibernetik ka një rritje në aktivitetin e tij edhe për shkak të anonimitetit që ruan ky krim, duke e bërë të vështirë identifikimin e personave përgjegjës së këtij krimi. Pra, rreziku ndaj autorëve të kryerjes së këtyre veprave, qoftë fizik apo juridik, është tepër i vogël dhe janë gati të paekspozuar ndaj rreziqeve që mund të vijnë nga kjo vepër. Por, një tjetër arsye mjaft e veçantë, e cila përzgjidhet nga ana e autorëve të kësaj vepre penale, është edhe për shkak të

[1] Sarah Gordon, Cyberterrorism? *Symantec Security Response*, f. 4.

numrit tepër të lartë të viktimave dhe të personave të dëmtuar nga ky akt i paligjshëm, në krahasim me terrorizmin e thjeshtë[2].

Siç vihet re, terrorizmi kibernetik ka një lidhje tepër të ngushtë me krimin e terrorizmit. Për sa i përket terrorizmit, edhe pse shtetet e kanë të vështirë të bien dakord për një përkufizim të përbashkët, mund të konsiderohet çdo akt dhune apo kërcënim, i cili ka për qëllim që të shkaktojë frikë tek popullsia civile dhe që është i motivuar politikisht ose ideologjikisht, duke shkaktuar pasoja tek popullsia civile si vdekje apo dëmtime të tjera, me qëllimin për të detyruar qeverinë apo institucione ndërkombëtare për të bërë apo mos bërë një veprim të caktuar.

Terrorizmi kibernetik nuk duhet që të ngatërrohet me disa forma të tjera të krimit kibernetik të cilat mund të kenë ngjashmëri me të si haktivizmi apo ndërhyrja në disa sisteme kompjuterike pa ndonjë qëllim të caktuar, etj. Në çdo rast duhet që të zbatohet kriteri për krimin e terrorizmit kompjuterik, për të bërë një cilësim sa më të saktë të veprës.

2. Aspekte të terrorizmit kibernetik

Terrorizmi kibernetik është një nga format e reja të krimit kibernetik dhe ai ka mjaft pasoja të rënda, duke u bërë një kërcënim real për shumë shtete dhe organizata ndërkombëtare. Pasojat e tyre janë vendimtare, pasi në disa raste të caktuara ato shkatërrojnë një rrjet të tërë të dhënash të nevojshme dhe integrale të një sistemi kompjuterik të një shteti të caktuar. Këto të dhëna, në disa raste mund të jenë sekrete ose të vështira për t'u rikthyer, duke i shkaktuar në këtë mënyrë probleme tepër serioze shtetit në fjalë.

Në raste të tjera krimi i terrorizmit kibernetik shfaqet në formën e sulmeve ndaj infrastrukturës së një shteti e një pjese kritike të saj. Kështu, pasojat që ky sulm ka në ekonomi janë madhore duke shkatërruar për shembull rrjetin e telekomunikimeve, rrjetin elektrik, linjat e transportimit të gazit, pajisjet e ujit dhe rrjetin hidroteknik, apo pjesë të tjera thelbësore për një shtet dhe qytetarët e tyre.

Gjithashtu, krimi kibernetik mund të godasë edhe biznesin, duke i sjellë pasoja tepër të rënda dhe paralizimin e krejt veprimtarisë së tij. Kjo ka një pasojë të drejtpërdrejtë në ekonominë e vendit, por edhe në zhvillimin e përparimin ekonomik të vendit në fjalë. Për shembull, goditja e një sistemi kompjuterik të një banke të caktuar, do të shkaktonte humbje të mëdha ekonomike jo vetëm për subjektin në fjalë, por edhe për vetë shtetin ku kjo bankë operonte dhe subjektet të cilët kishin veprimtari në këtë bankë.

Një ndër pasojat më të rënda të terrorizmit kibernetik, është dhe fakti që shpeshherë ky lloj krimi pasohet me humbjen e jetëve të njerëzve ose dëmtimin e disa prej tyre. Dëmtimi i linjave ajrore nga ana e terroristëve, sigurisht që do të pasohej me humbje të mëdha në jetë njerëzish; krimet në infrastrukturë, po ashtu mund të sillnin panik dhe humbje jetësh, si dhe krimet e tjera.

Disa nga më mënyrat më kryesore të së vepruarit të terroristëve kibernetikë, janë:

- Mënyra e thjeshtë dhe e pastruktuar, është një formë e të vepruarit nga terroristë të cilët veprojnë në mënyrë individuale, duke sulmuar një sistem të caktuar kompjuterik, duke shkaktuar pasoja, edhe pse jo aq të rënda sa ato në mënyrë të organizuar, por me peshë.

[2] John J. Klein, Deterring and Dissuading Cyberterrorism, *Journal of Strategic Security 8, no. 4 (2015): 23-38*, fq. 24.

- Mënyra tjetër e të vepruarit, është ajo e strukturuara, një mënyrë që kërkon një organizim më të lartë se ajo individualja dhe kërkon më shumë njohuri, në mënyrë që vepra penale të kryhet. Kjo mënyrë, shpesh, sulmon disa sisteme kompjuterikë njëkohësisht dhe arrin që të shkaktojë pasoja të rënda njëkohësisht, në mënyrë të kontrolluar.

- Mënyra e koordinuar është metoda më e përparuar e krimit të terrorizmit kibernetik, ku autorët e kësaj vepre, arrijnë të koordinojnë veprimet ndërmjet tyre në mënyrë komplekse dhe të integruar duke u pasuar me pasoja shkatërrimtare. Kjo është metodë e sofistikuar me një kontroll dhe organizim perfekt duke sulmuar në mënyrë të plotë dhe duke arritur shpesh qëllimet[3].

Terroristët e përdorin internetin si një mjet për të kryer veprat e qëllimet e tyre, duke nisur nga fazat e ideimit të veprave penale e deri në zbatimin e tyre. Komunikimi me terroristët e tjerë mundësohet me anë të shërbimeve të internetit, planet dhe strukturimi i tyre po ashtu. Njihen në botë shumë faqe të internetit të cilat janë krijuar posaçërisht për këtë arsye duke, krijuar mjedisin perfekt për të kryer veprën penale. Popullariteti i këtyre faqeve rritet jo vetëm për shkak të sponsorizimit dhe propagandës së kryer nga ana e terroristëve, por edhe për shkak të përpjekjeve të vazhdueshme të qeverive për t'i mbyllur këto faqe interneti[4]. Kështu, kjo është një nga mënyrat më të mira për të nxitur dhunë dhe për të rekrutuar terroristë të ardhshëm që synojnë të kryejnë këto vepra. Gjithashtu kjo është një mënyrë e mirë edhe për të rritur financimet ndaj veprimtarisë së këtyre personave, duke financuar terrorizmin edhe në mënyrë anonime e duke i mundësuar atyre mjete logjistike e burime të tjera të nevojshme për të kryer këto vepra.

Që të jemi përpara veprës së terrorizmit kibernetik është e domosdoshme që të kemi disa elementë që janë:

- sulmi duhet të jetë një sulm i motivuar politikisht, drejt një hapësire kibernetike që ka shkaktuar pasoja të rënda;

- duhet që të shkaktojë frikë ose panik nëpërmjet teknikave kibernetike;

- është një sulm që i është drejtuar një pjese të rëndësishme të infrastrukturës si: asaj financiare, energjetike, rrjetit të ujësjellësve, transportit, apo sektorë të caktuar të qeverive;

- nuk kanë si synim kryesor nxjerrjen e përfitimeve financiare;

- në qoftë se nuk i është drejtuar një pjese esenciale të infrastrukturës, nuk është një sulm që përfshihet në sulmet e terroristëve kibernetik[5].

Motivimi i terroristëve që përdorin hapësirën kibernetike për të kryer një krim, është krijimi i frikës apo krijimi i humbjeve të mëdha ekonomike, e diskriminimi i kundërshtarëve. Për shkak të këtyre motiveve rrezikohen jo vetëm humbjet në jetët njerëzore por, rrezikohet paralizimi i shtetit, për të ngjallur një panik të madh. Një ndër rastet më të bujshme dhe të kohëve të fundit, është dhe dënimi i një shtetasi kosovar në Shtetet e Bashkuara të Amerikës. Ai u dënua në gusht të vitit 2015 nga gjykatat amerikane, për mbështetjen e dhënë ndaj shtetit islamik ISIS, duke ndërhyrë në sistemet kompjuterike amerikane. Ai ndërhyri në këto sisteme, duke mundësuar marrjen e të

[3] https://web.archive.org/web/20140310162011/http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

[4] P. W. Brunst, *Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet,* Chapter 2, f. 71.

[5] Zahri Yunos, *Putting Cyber Terrorism Into Context*, *STAR In-Tech,* 2009, f. 4.

dhënave të rëndësishme e informacioneve sekrete e më pas vënien tyre në dispozicion të shtetit islamik, me qëllimin për t'u shkaktuar sa më shumë dëme Shteteve të Bashkuara të Amerikës. Mijëra informacione sekrete u morën nga punonjësit federalë me qëllimin për t'u përdorur ndaj tyre dhe për të shkaktuar një kërcenim, jo vetëm individual, por edhe kombëtar. Kjo është një ndër çështjet e para, të gjykuara për krimin e terrorizmit kibernetik, - ku ka rëndësinë, si një çështje lider, në goditjen e parandalimit e të terrorizmit dhe ruajtjes së sigurisë kombëtare[6].

Por, në botë janë njohur edhe disa raste të tjera të krimit të terrorizmit kibernetik. Në disa prej tyre, është arritur që të reagohet në nivel kombëtar, e në disa të tjera, pa arritur që të vihen përpara përgjegjësisë autorët. Për shembull, gjatë luftës së Kosovës në vitin 1999, kompjuterët e NATO-s u sulmuan nga e-maile të cilat shkatërronin sistemet kompjuterike. Gjithashtu, shumë organizata dhe institucione publike ndërkombëtare morën viruse me anë të e-maileve, nga persona të paidentifikuar. Pas aksidentit në Ambasadën Kineze, haktivistët kinezë, postuan mesazhin në adresat e internetit të qeverisë amerikane, që nuk do të ndaleshin deri sa lufta të mbaronte, duke marrë disi përsipër autorësinë, por pa u vendosur përpara përgjegjësisë penale.

Nuk mund të rrihet pa përmendur ndërhyrja e bërë në Ukrainë, ku u arrit që të bllokohet dhe të ndërpritet shërbimi i komunikimit në internet, me qëllim mbështetjen e rebelëve për marrjen në kontroll të Krimesë. Gjithashtu, në Ukrainë, në dhjetor të vitit 2016 mbi 250.000 konsumatorë, si pasojë e mungesës së energjisë elektrike pësuan terror dhe panik, ku ngjarja edhe pse shpesh kishte ngjyra politika duke pasur akuza e kundërakuza, nuk u arrit të zbulohej. Është për t'u përmendur edhe rasti i sulmit të Sony Pictures Entertainment, një kompani e cila është e vendosur në Shtetet e Bashkuara të Amerikës, si pasojë e lëshimit të një filmi dedikuar kryetarit të shtetit të Koresë së Veriut. Mendohet se grupi që sulmoi këtë kompani, ishte nga Korea e Veriut, ku u bënë dhe mjaft kërcënime ndaj popullsisë civile, të njëjta me ato të shtatorit të vitit 2001, gjë e cila bëri që Sony, të shtynte nxjerrjen e këtij filmi.

Në vitin 2015, u sulmua edhe Parlamenti Gjerman nga ana e personave të paidentifikuar. Këta, arritën që të sulmonin e të infektonin mbi 20 000 kompjuterë të përdorur nga politikanët gjermanë, ndihmësit e tyre dhe nëpunësit e administratës publike. Ata arritën që të merrnin shumë të dhëna e informata sekrete e më pas, kërkuan një shumë të madhe për t'i rikthyer ato. Kjo vepër mendohet që të jetë kryer nga një grup rebelësh e nacionalistësh, të cilët kërkonin që Berlini të mos mbështeste më Ukrainën. Gjithashtu, edhe sulmi i kryer përpara zgjedhjeve presidenciale në Ukrainë, në vitin 2014, ku u sulmua sistemi i komisionit zgjedhor nga një grup i vendosur në Rusi. Një kaos i vërtetë, e shoqëroi këtë akt, ku qëllimi, ishte mbështetja e kandidatit prorus dhe humbja e atij nacionalist.

Organizata e Kombeve të Bashkuara, ka ndërmarrë disa hapa të rëndësishme për të luftuar terrorizmin kibernetik, në të gjitha format e tij. Janë miratuar disa rezoluta të cilat kërkojnë jo vetëm bashkëpunimin ndërkombëtar, por edhe përmirësimin e sigurisë kibernetike, duke ruajtur të dhënat e duke bërë më të vështirë sulmin ndaj pjesëve të rëndësishme të infrastrukturës. Interpoli, gjithashtu ka krijuar një grup pune në administratën e vet, për të luftuar terrorizmin në përgjithësi dhe, atë kibernetik, si një nga format më të reja të shfaqjes së tij. OECD, nga ana tjetër, vazhdon që të publikojë raporte mbi politikat parandaluese të terrorizmit dhe forcimit të sigurisë kombëtare e

[6] Çështja, Ardit Ferizi vs USA, *Eastern District of Virginia*, 2016.

përkatësisht sistemeve të informacioneve kompjuterike.

Bashkimi Europian, në strategjitë e tij, është i vendosur për të luftuar të gjitha format e terrorizmit dhe pasojat që sjellin këto krime. Konventa mbi krimin kibernetik, e vitit 2002[7], është një ndër hapat kryesorë për luftimin e krimeve kompjuterike, dhe minimizimin e pasojave prej tyre. Edhe pse kjo konventë, në pamje të parë, aplikohet vetëm ndaj krimit kibernetik, ajo indirekt aplikohet edhe ndaj terrorizmit kibernetik, duke shënuar risi në instrumentet ndërkombëtare për identifikimin e një krimi të veçantë. Konventa mbi parandalimin e krimit të terrorizmit gjithashtu është një instrument tepër i rëndësishëm për parandalimin e këtij krimi, duke treguar vendosmërinë e shteteve anëtare për të luftuar të gjitha format e terrorizmit, si dhe ndërhyrjet në legjislacionet vendase për të qenë sa më efikasë në luftën kundër këtij krimi dhe forcimin e bashkëpunimit ndërkombëtar.

Për të luftuar terrorizmin kibernetik është e nevojshme ndërmarrja e disa strategjive, të cilat shërbejnë për parandalimin e tyre. Ndër to, mund të përmendim:

- thithja e praktikave më të mira nga vendet e tjera dhe organizmat ndërkombëtarë në forcimin e sigurisë kombëtare;
- vënia përpara përgjegjësisë ndërkombëtare personave që kryejnë vepra të tilla;
- përmirësimi i legjislacioneve vendase dhe ndërkombëtare, si dhe zhvillimi i strategjive efektive parandaluese;
- krijimi i sistemeve kompjuterike dhe *software* kundër ndërhyrjeve në rrjetet kompjuterike;
- rritja dhe forcimi i bashkëpunimit ndërkombëtar me qëllim parandalimin e kryerjes së këtij krimi dhe shkëmbimit të informacionit;
- forcimi i fushatave ndërgjegjësuese dhe sensibilizuese për të ndaluar rekrutimin e terroristëve kibernetikë;
- nxitja e kërkimit shkencor në këtë fushë, me qëllim identifikimin e problemeve dhe dhënien e opinioneve për zgjidhjen e tyre[8].

3.Terrorizmi kibernetik në Shqipëri

Shqipëria, në legjislacionin e saj, ka arritur që të përafrohet më së miri me atë europian dhe ndërkombëtar. Hapat e ndërmarra legjislative, janë të rëndësishme për luftën ndaj terrorizmit dhe për efikasitetin në parandalimin e tij. Ndër vite, janë krijuar strategji, të cilat kanë rezultuar efektive dhe dita-ditës bashkëpunimi në nivelin kombëtar e atë ndërkombëtar, është rritur duke mundësuar një shkëmbim informacioni e përvojash ndërmjet shteteve, për të qenë të përgatitur ndërmjet çdo situate. Parandalimi i veprave me qëllime terroriste, në vitet e fundit, tregon se vendi ynë mund të preket së shpejti edhe ndaj formave të reja të krimit të terrorizmit e përkatësisht të atij kibernetik.

Veprat me qëllime terroriste, janë të përcaktuara në Kodin tonë Penal në një krè më vete, (Kreu VII), duke treguar e natyrën dhe rëndësinë e këtyre veprave. Kodi ynë, i përcakton kryerjen e veprave me natyrë terroriste, si vepra që kanë për qëllim përhapjen e panikut në popullatë, ose për të detyruar organe shtetërore shqiptare ose të huaja, të kryejë ose të mos kryejnë një akt të caktuar, ose për të shkatërruar apo destabilizuar, në

[7] Konventa në fushën e krimit kibernetik, *Ligji Nr. 8888*, datë 25.4.2002.

[8] Shamsuddin Abdul Jalil, Countering Cyber Terrorism Effectively: Are We Ready To Rumble? *GIAC Security Essentials Certification (GSEC) Practical Assignment Version 1.4b Option 1 June 2003,* f. 8-12.

mënyrë serioze struktura shtetërore politike, kushtetuese, ekonomike, ose sociale të shtetit shqiptar, të një shteti tjetër, institucioni apo organizate ndërkombëtare.[9]

Edhe pse në mënyrë direkt, kodi ynë penal nuk ka arritur të përcaktoj veprën e terrorizmit kibernetik, në mënyrë indirekt mund të themi se ky nen, arrin të zbatohet në brendësi edhe për kryerjen e veprave të terrorizmit, me anë të hapësirës kibernetike. Për shembull, në pikën "c" të këtij neni, përcaktohet se: "shkatërrimi i një avioni në funksionim, i një anijeje apo i një platforme fikse ose shkaktimi i dëmeve të tilla avionit, anijes apo ngarkesës së saj që e bëjnë të pamundur ose rrezikojnë apo mund të rrezikojnë sigurinë e fluturimit a të lundrimit", duke e lënë të hapur, mënyrën se si mund ta kryejnë terroristët në anën objektive të veprës: ku një formë mund të jetë me anë të ndërhyrjes kompjuterike të bërjes së pamundur të udhëtimit a lundrimit.

Gjithashtu, në pikën "dh" të këtij neni, përcaktohet se dënohet edhe shkatërrimi ose dëmtimi i pajisjeve të fluturimit, apo të lundrimit detar, apo ndërhyrja në funksionimin e tyre, kur nga një akt i tillë mund të vihet në rrezik, siguria e avionit apo e anijes. Pra, kur kjo vepër kryhet me anë të hapësirës kibernetike dhe me qëllime terroriste, është vepër e pastër e krimit të terrorizmit kibernetik. Gjithashtu, mund të përfshihet edhe përhapja e informacioneve të cilat dihet se janë të pavërteta, por që vënë në rrezik sigurinë e një avioni në fluturim ose një anijeje në lundrim[10].

Në pikën "k", gjithashtu, është një formë tjetër e kryerjes së këtij krimi, duke dënuar të gjithë ata persona që kryejnë akte të dhunës duke përdorur çdo pajisje, substancë apo armë, kundër një personi në një aeroport të aviacionit civil ndërkombëtar, ose në një avion i cili është vendosur aty, por që nuk është në fluturim, ose ndërprerja e shërbimeve të aeroportit duke përdorur çdo substancë, pajisje apo armë, kur nga ky akt mund të rrezikohet siguria e avionit. Duke lënë në mënyrë të hapur kështu kryerjen e këtij krimi në anën objektive të tij, ku ndër to mund të jetë dhe kryerja e krimit me anë të hapësirës kibernetike.

I rëndësishëm është dhe parashikimi i një forme tjetër të mënyrës së kryerjes së veprës së terrorizmit, por që indirekt përfshihet edhe në veprën e terrorizmit kibernetik. Kështu, shkatërrimi i rëndë dhe në përmasa të mëdha, i pronës publike, infrastrukturës publike, të sistemit të transportit, të sistemit të informacionit të pronës private, duke rrezikuar jetën e personave, përbën një nga format e krimit të terrorizmit[11]. Gjithashtu edhe shkaktimi i ndërprerjes së furnizimit me ujë apo me energji elektrike si dhe me çdo burim tjetër të rëndësishëm për popullsinë, përbën vepër penale[12]. Këto dy format e fundit, përbëjnë edhe format më të zakonshme të kryerjes së terrorizmit kibernetik dhe me të cilat, vijnë edhe pasoja më të rënda.

Një formë tjetër, të cilën e kemi përmendur edhe më lart që mund të kryhet me anë të veprës së terrorizmit kibernetik, është dhe rekrutimi i personave për kryerjen e veprave me qëllime terroriste ose për financimin e tyre, ku në kodin tonë penal parashikohet si një figurë e veçantë e veprës penale[13]. Gjithashtu, përgatitja e udhëzimeve në mënyrë elektronike për kryerjen e veprave penale, apo në mënyrë anonime si dhe përgatitja e tyre për kryerjen e veprave terroriste është e dënueshme në kodin tonë penal[14].

[9] Neni 230 i Kodit Penal të Republikës së Shqipërisë.
[10] Pika "e", neni 230 i Kodit Penal të Republikës së Shqipërisë.
[11] Pika m), neni 230, po aty.
[12] Pika n), neni 230 i Kodit Penal të Republikës së Shqipërisë.
[13] Neni 231 po, aty.
[14] Neni 232 i Kodit Penal të Republikës së Shqipërisë.

Dhënia ose grumbullimi i fondeve, me çdo mjet, në mënyrë të drejtpërdrejtë ose të tërthortë, me qëllimin që ato të përdoren ose duke ditur se ato do të përdoren, plotësisht ose pjesërisht për të kryer vepra me qëllime terroriste, nga një organizatë terroriste, nga një terrorist i vetëm, është gjithashtu një vepër e dënueshme nga ana e legjislacionit tonë[15].

Nxitja, thirrja publike dhe propaganda për kryerjen e veprave terroriste apo shpërndarja e shkrimeve me natyrë terroriste, që synojnë mbështetjen ose financimin e terrorizmit, janë gjithashtu të dënueshme[16]. Nga ana tjetër, gjithashtu dënohet edhe kanosja serioze që u bëhet autoriteteve publike apo një shteti tjetër, ose institucioni, ose organizate ndërkombëtare, për kryerjen e veprave me natyrë terroriste[17].

Sipas nenit 234 pika "a", të Kodit tonë Penal, krijimi ose organizimi, drejtimi dhe financimi i organizatës terroriste, është i dënueshëm me jo më pak se 15 vjet burgim. Gjithashtu, pjesëmarrja në këto organizata, dënohet me burgim nga shtatë deri në 15 vjet.

4. Konkluzione dhe rekomandime

Terrorizmi kibernetik është një term mjaft kontrovers, kjo edhe për shkak të vështirësisë së dallimit të tij nga krimet e tjera kibernetike. Terrorizmi kibernetik rrjedh nga konvergjenca e terrorizmit dhe hapësirës kibernetike. Ai nënkupton sulmet dhe kërcënimet e paligjshme ndaj kompjuterëve, sistemeve kompjuterike dhe informacioneve të rezervuara në këto sisteme për të intimiduar një pjesë të shtetit/qeverisë apo njerëzve të saj, me synimin e arritjes së objektivave politike apo sociale. Kështu, që një sulm të klasifikohet si pjesë e terrorizmit kibernetik, duhet që t'i jetë drejtuar një personi apo pasurisë, apo të shkaktojë një dëm që sjellë frikë dhe panik. Sulmet kundër infrastrukturës, mund të jenë shembuj të terrorizmit kibernetik, nëse kanë pasoja mjaft të rënda. Terrorizmi kibernetik është një nga format e reja të krimit kibernetik dhe ai ka mjaft pasoja të rënda, duke u bërë një kërcënim real për shumë shtete dhe organizata ndërkombëtare. Pasojat e tyre janë vendimtare, pasi në disa raste të caktuara, ato shkatërrojnë një rrjet të tërë të dhënash të nevojshme dhe integrale, të një sistemi kompjuterik të një shteti të caktuar. Kodi ynë, e përcakton kryerjen e veprave me natyrë terroriste, si vepra që kanë për qëllim përhapjen e panikut në popullatë, ose për të detyruar organe shtetërore shqiptare ose të huaja, të kryejë ose të mos kryejnë një akt të caktuar, ose për të shkatërruar apo destabilizuar, në mënyrë serioze struktura shtetërore politike, kushtetuese, ekonomike, ose sociale të shtetit shqiptar, të një shteti tjetër, institucioni apo organizate ndërkombëtare. Edhe pse në mënyrë direkt, kodi ynë penal nuk ka arritur ta përcaktojë veprën e terrorizmit kibernetik, në mënyrë indirekt mund të themi se ky nen arrin të zbatohet në brendësi edhe për kryerjen e veprave të terrorizmit me anë të hapësirës kibernetike.

[15] Neni 230 a), po aty.
[16] Neni 232 a) i Kodit Penal të Republikës së Shqipërisë.
[17] Neni 232 b) po, aty.

Bibliografia

1. Sarah Gordon, *Cyberterrorism?, Symantec Security Response*.
2. John J. Klein, "Deterring and Dissuading Cyberterrorism", *Journal of Strategic Security 8*, no. 4 (2015): 23-38.
3. Shamsuddin Abdul Jalil, *Countering Cyber Terrorism Effectively: Are We Ready To Rumble?* GIAC Security Essentials Certification (GSEC) Practical Assignment Version 1.4b Option 1 June 2003.
4. Zahri Yunos, *Putting Cyber Terrorism Into Context*, STAR In-Tech, 2009.
5. P. W. Brunst, *Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet*, Chapter 2.
6. Kodi Penal i Republikës së Shqipërisë.
7. Konventa në fushën e krimit kibernetik, Ligji Nr. 8888, datë 25.4.2002.
8. Ardit Ferizi vs USA, *Eastern District of Virginia*, 2016.
9. https://web.archive.org/web/20140310162011/http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html


AKADEMIA E SIGURISË
AS

Koncepti i ri i kufijve virtualë dhe kërcënimet e sigurisë publike e kombëtare

MSc. Valeria BARDHAJ
Ministria e Drejtësisë
valeriabardhaj@gmail.com

Abstrakt

Jemi mësuar të lexojmë, diskutojmë apo shkruajmë lidhur me krimet tradicionale të tipit vrasje, vjedhje, rrëmbim personi etj. Me evoluimin e shkencës dhe teknologjisë veçanërisht në lehtësirat që ofron përdorimi i kompjuterit dhe faktin se interneti tashmë është një mjet komunikimi global, vitet e fundit krimet lidhur me mashtrimet, sulmet e viruseve të ndryshme, pornografinë e të miturve, si edhe krimet e urrejtjes janë rritur ndjeshëm. Sot krimi kibernetik cilësohet si një prej problemeve dhe sfidave kryesore të shumë qeverive. Shqipëria është renditur si një prej vendeve ku zhvillimi i teknologjisë po ecën me hapa galopi, për pasojë rrezikshmëria e sulmeve kibernetike është e madhe. Një rrezik i tillë potencial është absolutisht cenim i sigurisë kombëtare dhe asaj publike. Për këtë arsye fokusi i këtij punimit do të lidhet ngushtë me politikat e hartuara me qëllim identifikimin e rreziqeve potenciale, duke u bazuar tek legjislacioni, konventat si dhe strukturat e ngritura nga qeveria për të luftuar këtë krim. Bota virtuale është kthyer tashmë në një nga hapësirat e preferuara të çdokujt, madje edhe qeveritë e kanë cilësuar si një mjet të mirë komunikimi me publikun duke e përdorur për ofrimin e një sërë shërbimesh. Ndonëse digjitalizimi ka ofruar mori lehtësirash nga ana tjetër është rritur rreziku i sulmeve pirate. Këto sulme dëmtojnë shkëmbimin e të dhënave, sistemin bankar, apo edhe sektorin publik. Partnerët ndërkombëtarë evidentuan se Shqipëria nuk ishte gati për të përballuar një fenomen të tillë, ndaj një prej kushteve kryesore për integrimin në Bashkimin Evropian lidhej drejtpërdrejtë me hartimin e politikave mbi sigurinë kibernetike (Kapitulli 24; Drejtësia, Liria dhe Siguria). Madje, si anëtare e NATO-s, me të drejta të plota, Shqipëria ka për detyrë zgjerimin e mbrojtjes kibernetike për rjetet dhe infrastrukturat kombëtare. Krimi kibernetik ka karakteristika shumë më të fuqishme në përhapje dhe tejet të ndërlikuara (krahasuar këtu me krimet tradicionale), të cilat sjellin vështirësi në zbatimin e ligjit. Ndaj në përmbyllje ky punim do të fokusohet kryesisht një sërë rekomandimesh dhe praktikash të suksesshme mbi ndërgjegjësimin e shtetit në tërësi, institucioneve ligjzbatuese dhe qytetarëve mbi rreziqet që sjell krimi kibernetik.

Fjalëkyçe:
siguria kombëtare, siguria kibernetike, legjislacion, digjitalizim.

1. Krimi kibernetik në përmasat kombëtare

1.1 Hyrje

Shpeshherë e përcaktomë krimin kibernetik të ndarë nga krimet tradicionale, të zakonshme, mirëpo ky krim kryhet nga të njëjtët kriminel për të njëjtat arsye. Praktikisht ata kanë të njëjtat motive si kriminelët tradicionalë, si vandalizmi, keqdashja ose hakmarrja, fitimi monetar përmes nxjerrjes ose shitjes së të dhënave të marra në mënyrë të paligjshme, terrorizmit, etj.

Në gjuhën e zakonshme krimi është një veprim i paligjshëm, pra një veprim në kundërshti me rregullat dhe ligjet e një shteti. Krimi është i dënueshëm. *Veprat penale ndahen në krime dhe në kundërvajtje penale. Dallimi i tyre bëhet në çdo rast në dispozitat e pjesës së posaçme të Kodit Penal*[1].

Termi "krim" nuk ka ndonjë përkufizim të pranuar universalisht, në të drejtën moderne penale, por për qëllime të caktuara janë dhënë përkufizime statutore. Kriminologjisti Paul Tappan e përcakton termin *krim* si një veprim i qëllimshëm apo mosveprim në shkelje të ligjit, i kryer pa mbrojtje ose justifikim dhe i sanksionuar nga shteti si kundërvajtje[2].

Nga ana tjetër autorë të ndryshëm e kanë përcaktuar *krimin kibernetik* si shkelje e ligjit penal duke përdorur si mjet njohuritë e teknologjisë së informacionin për kryerjen e një veprimtarie të paligjshme. Me krim kibernetik i referohemi shkeljeve që kanë të bëjnë me veprimtarinë kriminale që përfshin vepra penale si mashtrimi, aksesi i

[1] Ligj nr. 7895, datë 27.1.1995, Kodi Penal i Republikës së Shqipërisë.

[2] Who Is the Criminal?, Paul W. Tappan, f.18 (https://www.corwin.com/sites/default/files/upm-binaries/25522_Chap02.pdf).

paautorizuar, pornografia e fëmijëve dhe vjedhja e të dhënave etj. Pra, shkurtimisht themi se *krimi kibernetik* i referohet veprave penale të kryera duke shfrytëzuar internetin ose një rrjet tjetër kompjuterik si komponent i veprës penale.

Krimi kibernetik po rritet me ritme shumë të shpejta në ditët e sotme. Shumë kriminelë rriten duke shfrytëzuar komoditetin, shpejtësinë, si dhe anonimitetin e përdorimit të internetit, me qëllim kryerjen e aktiviteteve të ndryshme kriminale. Sot ne njohim lloje të ndryshme sulmesh kibernetike që kanë sjellë pasoja fatale për biznese, qeveri apo edhe individë, të cilët kanë humbur pronat e tyre apo shuma të mëdha parash, madje së fundmi kemi dëgjuar raste që për shkak të krimit kibernetik, të rinj në mbarë botën janë bërë pjesë e lojërave të ndryshme nëpërmjet internetit/rrjeteve sociale duke i çuar kështu në humbjen e jetës/vetëvrasje.

1.2 Historik i shkurtër i krimit kibernetik ndër vite

Bota në të cilën jetojmë, tashmë ka arritur një shkallë tejet të lartë komunikimi dhe shkëmbimi informacioni, përmes përdorimit të internetit. Përmes teknologjisë së informacionit dhe botës virtuale, gjithkush ka mundësi të përfitojë informacionin dhe shërbimin e nevojshëm duke kursyer kohë dhe para.

Mirëpo, nga ana tjetër rritet rreziku i sulmeve kibernetike, duke i dhënë kështu një mundësi të artë kriminelëve të kësaj fushe të zaptojnë të dhënat personale, si dhe të kryejnë veprimtari të tjera kriminale përmes përdorimit të internetit.

- *Në vitin 1960* është përdorur për herë të parë fjala "hacker". Ky term u përdor për të përshkruar veprimtarinë e modifikimit të një produkti ose procedure, pra për të ndryshuar funksionin e tij normal për të rregulluar një problem. Termi u përdor nga disa individë që ishin të pasionuar pas trenave të MIT (Massachusetts Institute of Technology). Ata zbuluan mënyra për të ndryshuar funksione të caktuara të trenit pa riinxhinierimin e pajisjes në tërësi. Ky lloj inovativ i krimit ishte një çështje e vështirë për zbatimin e ligjit, për shkak të mungesës së legjislacionit për të ndihmuar në ndjekjen penale, si dhe mungesën e hetuesve të kualifikuar në këtë fushë[3].

- *Në vitin 1970* një grup hakerash i quajtur "phreakers", duke imituar dhe kopjuar operatoret telefonik zbuluan kodet e sakta nëpërmjet të cilave do të mund të përfitonin shërbim telefonik falas jashtë zonës së mbulimit nga operatori telefonik[4].

- *Në vitin 1986* Policia e Gjermanisë Perëndimore shkatërroi një rrjet të spiunazhit kompjuterik që punonte me agjentët e inteligjencës sovjetike, të cilët vidhnin fjalëkalimet kompjuterike ushtarake të Shteteve të Bashkuara, *software* dhe të dhëna të tjera. Sipas policisë mendohet se hakerët mund të kishin vjedhur një sasi të madhe së të dhënave kërkimore të avancuara, të dobishme për agjentët sovjetikë. Ndërhyrjet e hakerëve gjermanë u zbuluan në vitin 1986 nga dr. Clifford Stoll, një astronom dhe ekspert i sigurisë kompjuterike[5].

- *Në mesin e viteve 1990,* mashtrimi i kartave të kreditit ishte një problem me rritje të shpejtë për përdoruesit e këtyre kartave, si dhe për zbatimin e ligjit. Një raport i FBI-së i vitit 1997, përllogarit se në të gjithë botën humbjet e mashtrimeve bankare në kartat Visa dhe Master-Card janë rritur nga 110 milionë dollarë në vitin 1980, në rreth 1.63 miliardë dollarë deri në 1995[6].

[3] https://www.floridatechonline.com/blog/information-technology/a-brief-history-of-cyber-crime/
[4] Po aty.
[5] https://www.nytimes.com/1989/03/03/world/west-germans-raid-spy-ring-that-violated-us-computers.html
[6] "Future of Bank Cards - Part I (Fraud),"The Nilson Report, No. 568, March, 1994; Burimi dytësor: https://leb.fbi.gov/file-repository/archives/june-1997.pdf

- *Fundi i viteve 1990 dhe deri në 2000,* mashtrimi nëpërmjet kartës së kreditit u ndërthur me atë të vjedhjes së identitetit. Grupe të strukturuara kriminale ose individë të veçantë filluan të vidhnin identitetin e personave të caktuar, duke krijuar kështu identitete paralele me qëllim marrjen e kredive bankare, blerjen e makinave me kredi në emër njerëzve të tjerë, të cilët mbeteshin debitorë në banka të ndryshme[7].

- *Pas viteve 2000* e deri në ditët e sotme, kemi një përdorim më të gjerë të internetit, botës virtuale, gjë që sjell përdorimin e kësaj bote nga ana e shkelësve të ligjit për një sërë veprimtarish të paligjshme. Nëse pas viteve 2000 hakerat lëshonin një sërë virusesh, të cilët sillnin probleme në *hardware* apo *software* (të tilla si virusi *"Trojan",* materialeve *spam* siç ishte rasti i virusit *"I Love You",* po ashtu site të ndryshme, të cilët përmes një reklame bindnin qytetarët të bënin pagesa të ndryshme për përfitimin e *Green Card* amerikane etj.).

- *Sot* krimi nëpërmjet internetit i tejkalon kufijtë e imagjinatës. Në ditët e sotme përmes rrjeteve sociale dhe sajteve të ndryshme po rritet numri i të rinjve që mashtrohen me qëllim prostitucionin, po rritet numri i të rinjve që vetëflijohen për shkak të lojërave të ndryshme virtuale, siç ishte rasti i "Balenës blu", si dhe raste të shumta të pornografisë së të miturve.

Krimi kibernetik do të vazhdojnë të jetë i pranishëm në shoqërinë tonë, pavarësisht nga përpjekjet më të mira të qeverisë, policisë dhe sistemit të drejtësisë penale për të luftuar këtë fenomen.

1.3 Situata aktuale, e krimit kibernetik në Shqipëri

Përmasat e krimit kibernetik nga një vit në tjetrin janë në rritje. Po ashtu krimi kibernetik po konsolidohet në grupe të strukturuara, të cilat formohen sipas veprimtarisë kriminale. Vihet re një prirje organizimi në grupime të vogla, që krijohen dhe lidhen në bazë të njohjeve kryesisht *online*, por dhe shoqërore. Anëtarët e këtyre grupeve vijnë nga zonat e populluara urbane, por edhe nga qytetet e vogla. Ka një ndërthurje të veprimtarive kriminale *online* me ato *offline*. Mosha e anëtarëve të luhatet nga 18 në 35 vjeç[8].

Më poshtë paraqitet një tabelë sqarimi i të cilës vijon:

Sipas statistikave të AKEP, vitet e fundit përdorimi i internetit në Shqipëri është rritur me 65%, shifër kjo që rrit ndjeshëm rrezikun e krimeve në vendin tonë. Por, sipas një raporti të prokurorisë, sqarohet se në vitin 2015 në numrin total të krimeve të raportuara në Prokurorinë e Përgjithshme, kjo vepër penale përbën 0.4% të numrit total të veprave, ndërsa në 2016 ka një rritje tejet të vogël duke kapur vlerën 0.46% të totalit.

Sipas raportit të prokurorisë duke krahasuar vitin 2016 në vitin 2017, vihet re një ulje të treguesve të ndjekjes penale konkretisht ulje 4% e numrit të procedimeve të regjistruara, ulje e numrit të procedimeve dërguar në gjykatë, nga 13 procedime në vitin 2016 në 4 procedime dërguar në gjykatë në vitin 2017 ose ulje 69%, ulje e numrit të të pandehurve të regjistruar në vitin 2017, përkundrejt këtij totali në vitin 2016, nga 16 në 4 ose 75 %, po kaq është edhe ulja e numrit së të pandehurve, të cilët janë dërguar në gjykatë, dhe 36%, është ulja e numrit së të pandehurve të dënuar për vepra penale kundër krimit kompjuterik.

[7] http://www.mekabay.com/overvieës/history.pdf

[8] Krimi i organizuar, vlerësimi i riskut në Shqipëri, Fabian Zhilla, Besfort Llamallari, f. 11.

Po sipas këtij raporti, duke krahasuar vitin 2015 me vitin 2016 ka një rritje të treguesve të ndjekjes penale me 7.4% të numrit të procedimeve të regjistruara, 2.2 herë rritja e numrit të procedimeve dërguar në gjykatë. Po ashtu, edhe numri të pandehurve të dënuar, është rritur me 2.2 herë, krahasuar me vitin 2015.

Ndërsa, nga vitin 2015 në vitin 2017, kemi të regjistruar katër procedime penale më shumë, por nga ana tjetër është ulur numri i personave të dënuar për vepra penale në fushën e kibernetikës.

Sipas raportit të Prokurorisë së Përgjithshme, vepra penale "Mashtrimi kompjuterik" zë 63% të totalit të procedimeve mbi krimin kibernetik.

KRIMI KIBERNETIK	2015					2016					2017				
	Nr. Proc Regj	Nr. Proc ne gjykim	Nr. Pand Regj	Nr. Pand per gjykim	Nr. Pand denuar	Nr. Proc Regj	Nr. Proc ne gjykim	Nr. Pand Regj	Nr. Pand per gjykim	Nr. Pand denuar	Nr. Proc Regj	Nr. Proc ne gjykim	Nr. Pand Regj	Nr. Pand per gjykim	Nr. Pand denuar
Neni 74/a Shpërndarja kompjuterike e materialeve komp. pro genocitit ose krimeve kunder njerëzimit	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Neni 84/a Kanosja me motive racizmi dhe ksenofobie nëpërmjet sistemit kompjuterik	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0
Neni 119/a Shpërndarja e materialeve raciste ose ksenofobie nëpërmjet sistemit kompjuterik	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
Neni 119/b Fyerja me motive racizmi ose ksenofobie nëpërmjet sist. kompj.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Neni 143/b Mashtrimi kompjuterik	60	2	3	2	4	51	7	10	10	7	73	1	2	1	0
Neni 186/a Falsifikimi kompjuterik	18	2	1	2	0	23	1	2	1	1	16	0	0	0	1
Neni 192/b Hyrja e paautorizuar kompjuterik	8	0	0	0	0	4	1	0	1	0	11	1	1	1	2
Neni 293/a Përgjimi i paligjshëm i të dhënave kompjuterik	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
Neni 293/b Ndërhyrja në të dhënat kompjuterike	64	2	1	2	1	64	4	4	4	3	33	2	0	2	4
Neni 293/c Ndërhyrja në sistemet kompjuterike	3	0	0	0	0	3	0	0	0	0	4	0	0	0	0
Neni 293/ç Keqpërdorimi i pajisjeve	0	0	0	0	0	1	0	0	0	0	1	0	1	0	0
TOTALI	136	6	6	6	5	146	13	16	16	11	140	4	4	4	7

Burimi: Raporti Vjetor mbi Gjendjen e Kriminalitetit Viti 2016, 2017, Prokuroria e Përgjithshme

Në këtë grup veprash penale bëjnë pjesë mashtrimet kompjuterike, hyrja e paautorizuar në të dhëna të rezervuara, falsifikimi i të dhënave, apo përgjimi i paligjshëm i të dhënave kompjuterike. Sipas të dhënave zyrtare të Prokurorisë së Përgjithshme, peshën më të madhe në këtë grup krimesh e zënë mashtrimet kompjuterike, të pasuar nga ndërhyrja e jashtëligjshme në të dhënat e rezervuara. Po ashtu nga të dhënat zyrtare të Policisë së Shtetit mbi krimin kibernetik, të rregulluar sipas Kodit Penal të Republikës së Shqipërisë, rezultojnë se në periudhën janar-dhjetor 2014 janë evidentuar 180 vepra penale, janë zbuluar 76, me 86 autorë, nga të cilët 74 janë në gjendje të lirë, 10 të arrestuar dhe 2 në kërkim. Për periudhën janar-dhjetor 2013, janë evidentuar 108 vepra penale nga të cilat janë zbuluar 63 prej tyre, me 69 autorë, nga të cilët 58 janë në gjendje të lirë, 9 arrestuar dhe 2 në kërkim[9].

Të pandehurit, janë të gjithë meshkuj të rritur, mbi moshën 18 vjeçare. Në lidhje me arsimin e të pandehurve, rezulton se 62,5% e tyre janë me arsim të mesëm, 25% me arsim të lartë, 12,5% me arsim deri 9-vjeçar. Rezulton se 87,5 % e të pandehurve, kanë vendbanimin në qytet dhe 12,5% në fshat. Ndërsa lidhur me gjendjen gjyqësore së të pandehurve, vërehet se 75% e tyre, janë të padënuar më parë dhe 25% janë të dënuar për vepra të ndryshme.

Sipas hulumtimeve nga Komisioni Evropian, 8% e përdoruesve të internetit në BE, janë përballur me vjedhjen identiteti dhe 12% kanë vuajtur nga ndonjë formë mashtrimi në internet[10].

Sipas progres-raportit të BE-së për vitin 2017, mbi krimin kibernetik, për vendin tonë është përcaktuar si nevojë zhvillimi i një strategjie kombëtare të sigurisë kibernetike. Në këtë raport thuhet se është bërë përparim i mirë në komunikimet elektronike me miratimin e ligjit për zhvillimin e rrjeteve të komunikimeve elektronike me shpejtësi të lartë dhe sigurimin e të drejtës së rrugës. Ligji është plotësisht në përputhje me aktet nënligjore. Për sa i përket fushës së shërbimeve informatike, po zbatohet strategjia ndërsektoriale e agjendës digjitale shqiptare për 2015-2020, si dhe plani për zhvillimin e brezit të gjerë. Ligji për sigurinë kibernetike u miratua në shkurt 2017 dhe është pjesërisht në linjë me Direktivën për sigurinë e rrjetit dhe sistemeve të informacionit[11].

2. Bota virtuale, lehtësitë dhe rreziqet

Përdorimi i internetit dhe rrjeteve sociale tashmë për këdo është një nevojë e pazëvendësueshme. Veçse një mjet ndihmës ku me një klik mund të gjesh miliona informacione të nevojshme, përdorimi i internetit është një kërcënim i madh për të gjithë botën, madje edhe për vendet si SHBA, Gjermani, Kanada, etj., të cilat njihen si vende të zhvilluara teknologjike.

Interneti është në revolucion gjatë gjithë kohës. Janë dy faktorë kryesorë që kanë shënuar evolucion kohët e fundit, pikërisht rrjetet sociale dhe teknologjia e lartë e telefonave celularë (*smartphones*). Këto dy risi kanë ndryshuar mënyrën se si njerëzit përdorin internetin.

Në vitin 1995, në botë numëroheshin 16 milion përdorues të internetit. Sipas statistikave, deri në dhjetor të vitit 2017, kjo shifër arrin 4,156 milion përdorues në të

[9] Dokumenti i Politikave për Sigurinë Kibernetike 2015-2017.

[10] https://www.europol.europa.eu/sites/default/files/documents/socta2013.pdf, EU serious and organised crime threat assessment, f. 28.

gjithë botën. Ndërkohë, në vendin tonë, nga tabela e mëposhtme, e cila është raport i AKEP-it, rezulton se nga viti 2013 deri në 2017 numri i përdoruesve të internetit është rritur me 65%.

TABELA 1.1: TREGUESIT KRYESORË TË VOLUMIT TË SHËRBIMEVE CELULARE 2013-2017

Viti	2013	2014	2015	2016	2017	Ndryshimi 2017/2016
Numri i përdoruesve të telefonisë celulare:						
– *Sipas kartave SIM*	5,282,350	4,928,784	4,777,885	5,160,060	5,392,964	**4.5%**
– *Përdorues aktivë*	3,685,983	3,406,772	3,442,665	3,360,888	3,460,171	**3.0%**
Numri përdoruesve me akses broadband 3G/4G:						
– *Totali*	1,231,259	1,576,877	2,049,072	2,739,550	3,345,045	**22.1%**
– *Përdorues aktivë*	1,231,259	907,975[1]	1,297,281	1,686,354	2,030,978	**20.4%**
Thirrje telefonike dalëse të përdoruesve celularë (minuta)	6,769,300,966	7,301,024,035	7,381,147,348	6,793,769,155	6,619,674,715	**-2.6%**
Thirrje hyrëse kombëtare	335,122,643	596,861,301	1,388,340,601	2,522,840,417	2,893,847,082	**14.7%**
Thirrje hyrëse ndërkombëtare	655,124,571	464,550,758	420,253,147	300,227,063	168,753,020	**-43.8%**
Numri mesazheve SMS të dërguara nga përdoruesit	1,689,200,882	1,826,346,190	1,598,702,865	1,610,322,977	1,400,142,526	**-13.1%**
Volumi total i të dhënave të transmetuara në rrjete celulare (GB)	2,529,549	6,269,940	12,740,073	26,753,639	45,901,117	**71.6%**

Burimi: Të dhëna të dërguara nga operatorët, përpunimi AKEP

Rritja e numrit të përdoruesve të aksesit *broadband* nga rrjetet celulare 3G/4G në vitet e fundit, është shoqëruar edhe me rritjen e volumit së të dhënave të transmetuara në rrjetet celulare, si dhe në përdorimin mesatar për përdorues së të dhënave. Në vitin 2017, ritmi i rritjes së trafikut së të dhënave në rrjetet celulare u ngadalësua në 72%, por kjo vjen pas normave të rritjes 103-148% në 2014-2016. Në periudhën 2013-2017 volumi i trafikut së të dhënave në rrjetet celulare, është rritur më shumë se 18 herë[12].

Sa më shumë të përdoret internet nëpërmjet telefonave, aq më i madh është rreziku i sulmeve të kibernetike. Ndërmjet transferimit së të dhënave, i japim mundësi kriminelëve, për të aksesuar fjalëkalimet e kartave të kreditit gjatë blerjeve *online*, apo fjalëkalimet e llogarisë tonë bankare gjatë përdorimit të shërbimit *online banking*, po ashtu i japim mundësinë të vjedhin adresat në rrjetet sociale, si dhe të përcjellin viruse në sajtet më të frekuentuara nga përdoruesit.

Qeveria, apo edhe kompani të ndryshme, humbasin miliona pará nga sulmet kibernetike, madje edhe të dhëna personale të rëndësishme janë arritur të merren përmes sulmeve pirate. Më poshtë, po paraqes disa raste konkrete ku hakerat kanë sulmuar qeveri të ndryshme.

- *Qeveria kanadeze, në janar të vitit 2011,* referoi një sulm kibernetik kundër agjencive dhe institucioneve të ndryshme në vend. Përmes adresave të email-it hakerat shpërndanë viruse të ndryshme, të cilat në momentin që klikoheshin mblidhnin të dhëna mbi fjalëkalimet dhe kontaktet e nëpunësve civil.

Të dhënat e mbledhura u përdorën nga kriminelët për të dërguar emaile *spam* tek mijëra punonjës të institucioneve të tjera qeveritare, duke i infektuar kështu kompjuterin dhe përhapur virusin më gjerë.

Departamentet e prekura ishin Bordi i Thesarit, Departamenti i Financave Federale,

[12] https://akep.al/images/stories/AKEP/publikime/raporte/Raporti%20Vjetor%202017%20AKEP.pdf

si dhe agjencia DND (Department of National Defence), që këshillonte Forcat e Armatosura Kanadeze mbi shkencën dhe teknologjinë. Pasi u zbulua ky sulm, zyrtarët kanadezë të sigurisë kibernetike mbyllën të gjithë aksesin që këto departamente kishin në internet, në mënyrë që të ndalonin transferimin e informacionit nga kompjuterët e hakuar. Kjo i la mijra nënpunsë të administratës publike pa qasje në internet.

Pas hetimeve u arrit të konstatohej që IP e virusit ishte Kineze, por kurrë nuk u vërtetua nëse kriminelët ishin kinez apo të ndonjë kombësie tjetër. Mbi këtë ngjarje Kryeministri Stephen Harper, deklaroi se, qeveria hartoi një strategji për zhvillimin e sistemeve të mbrojtjes, pasi çakerrat bëhen më të sofistikuar çdo ditë. Nga ana tjetër qeveria kineze ka mohuar përfshirjen në sulme dhe ka deklaruar, se pretendimet janë të pabaza[13].

- *Në korrik 2012,* në shpalosjen e programit të mbrojtjes kibernetike, zëvendëssekretari i Mbrojtjes së SHBA-së, bëri me dije se një kontraktori të Mbrojtjes (një kompani që nënshkruan një kontratë, me një qeveri federale të Shteteve të Bashkuara, për prodhimin e materialit ose për kryerjen e shërbimeve, për mbrojtjen kombëtare) iu hakuan 24 000 skedarë nga një sulm kibernetik[14].

- *Në maj të vitit 2015*, Bunderstagu Gjerman u prek nga një sulm kibernetik[15]. Disa parlamentarë gjermanë morën një *email* në të njëjtën kohë, ku adresa e dërguesit përfundonte me @un.org, duke e bërë atë të dukej sikur ishte nga Kombet e Bashkuara. Në të vërtetë ky email ishte nga hakerët, nga një server që sistemi mbrojtës i Bundestag nuk e njeh si problematik. E-maili kishte si lëndë, konfliktin mes Ukrainës dhe Rusisë, ndërsa në *attachmet* përmbante një buletin të supozuar të OKB-së. Ata që klikuan përfunduan në një faqe interneti që dukej si një faqe e OKB-së, por në të vërtetë i instalonte viruse në mënyrë të fshehtë në kompjuterin e marrësit të postës, të ashtuquajturin *Trojan*.

Ky sulm shkaktoi dëme të rënda, duke detyruar autoritetet gjermane të mbyllnin sistemin kompjuterik për disa ditë, me qëllim riparimin e rrjetit. Qeveria gjermane akuzon qeverinë ruse si shkaktare të këtij sulmi, por realisht ende nuk ka një autor për ngjarjen. Siç shihet edhe më sipër e-maili është një prej formave më të preferuara të komunikimit në botë, në administratën publike, institucionet shtetërore. Miliarda email-e shkëmbehen në të gjithë botën çdo ditë. Ashtu si çdo formë tjetër e komunikimit, siç u vu re edhe nga rastet e studimit më sipër, email-i keqpërdoret nga elementët kriminalë. Lehtësia, shpejtësia dhe anonimiteti relativ i email-it, e kanë bërë atë një mjet të fuqishëm për kriminelët.

Rastet e mësipërme paraqitën sulmet nga *Trojans* (apo *worms*) që janë dizajnuar për të infektuar kompjuterët ose për të instaluar vetveten në një kompjuter, pa lejen e përdoruesit. Megjithatë, mënyrat sesi veprojnë viruse të tilla shumë ndryshe nga tjetri. Një virus tipik bën dy gjëra, së pari, ai kopjon veten në programe të painfektuara më parë dhe së dyti, ekzekuton udhëzime të tjera që krijuesi i virusit ka përfshirë në të. Kodi keqdashës është çdo program *software* i projektuar për të lëvizur nga kompjuteri në kompjuter dhe nga rrjet në rrjet, në mënyrë që të modifikojë qëllimisht sistemet kompjuterike pa pëlqimin e pronarit ose të operatorit.

Të dhënat që rrjedhin përmes përdorimit të internetit nga sektori publik dhe privat,

[13] https://en.wikipedia.org/wiki/2011_Canadian_government_hackings.
[14] https://www.nato.int/docu/revieë/2013/cyber/timeline/en/index.htm
[15] https://www.reuters.com/article/us-germany-cyber/german-parliament-foiled-cyber-attack-by-hackers-via-israeli-website-idUSKBN1701V3

janë të larta. Në mbarë botën, mbi 700 milionë të dhëna personale u kompromet uan në vitin 2015, duke shkelur privatësinë e mbi 70 milionë individëve[16].

Tashmë qeveri të ndryshme në botë kanë marrë masa ndaj këtyre fenomenëve duke përqafuar strategji të reja për mbrojtjen e të dhënave të tyre, si më poshtë:

- *Instalimi i antiviruseve:* të gjithë përdoruesit e *windowsit* duhet të instalojnë antiviruse të licencuar në kompjuterët e tyre. Këto antiviruse përditësohen shpesh, gjatë gjithë ditës, duke siguruar mbrojtje në kohë kundër një game të gjerë kërcënimesh.

- *Instalimi i mbrojtjes në kohë reale "anti-spyware".*

- *Mbajtja e aplikacioneve anti-malëare të përditësuara:* programet antivirus dhe anti-*spyware* kërkojnë përditësime të rregullta dhe përditësime të bazës së të dhënave. Pa këto përditësime kritike, programet anti-*malware* nuk janë në gjendje të mbrojnë kompjuterët nga kërcënimet që i kanosen përmes viruseve.

- *Skanimet ditore:* këto skanime ditore janë tejet efektive në zbulimin, izolimin dhe largimin e "infektimit"që fillimisht i largohen vëmendjes së softuerit të sigurisë.

- *Çaktivizimi i imazheve "preview" në "Outlook":* marrja e viruseve përmes kodit grafik të një imazhi është një formë tjetër e sulmeve kibernetike. Përmes çaktivizimit të këtij opsioni parandalohen sulmet e viruseve të tilla.

- *Përdorimi i "firewall" me bazë në harduer: firewall* është një sistem i sigurisë së rrjetit që monitoron dhe kontrollon trafikun e rrjeteve hyrëse dhe dalëse në bazë të rregullave të paracaktuara të sigurisë. Një *firewall* i besueshëm është i domosdoshëm, pasi mbron kompjuterët nga një shumëllojshmëri e gjerë e shfrytëzimeve nga kriminelë të fushës. Për fat të keq, një *firewall* i bazuar në softuer i përfshirë me *Windows* nuk është i mjaftueshëm për të qenë i mbrojtur nga një numër sulmesh robotike që prekin të gjitha sistemet e lidhura me internetin. Për këtë arsye, të gjitha kompjuterët e lidhur me internet duhet të sigurohen nga një *firewall* me bazë në harduer (Harduer përfshin çdo pajisje që është e lidhur në kompjuterin dhe që kontrollohet nga mikroprocesori. Kjo përfshin pajisjen që është lidhur në kompjuterin kur ai u prodhua, si edhe pajisjen periferike e cila shtohet më pas)[17].

- *Vendosja e mbrojtjes DNS, Domain Name System (DNS):* është quajtur ndryshe numëratori telefonik i internetit. Njerëzit i qasen informatave në internet përmes emrave të *domain*-it, si bbc.co.uk ose fbi.gov. DNS përkthen emrat e *domain*-ve në adresa IP kështu që shfletuesit mund të ngarkojnë burimet e internetit. Çdo pajisje me akses në internet ka një adresë të veçantë IP, të cilën motorët e kërkimit e përdorin për të gjetur pajisjen. Jemi hasur shpesh me sulmeve e DNS-ve të infektuara, ku një server i DNS-së i kompromet uar, ju drejton në një server *Web* të paautorizuar. Për këtë arsye vendosja e një mbrojtjeje për DNS-në, është tejet e nevojshme.

- *"E-government"*

Në ditët e sotme, qeveritë po i drejtohen masivisht dhënies së shërbimeve *online*. Është e qartë se zbatimi i e-qeverisë jo vetëm që kursen burimet, përpjekjet dhe paratë, por gjithashtu mund të rrisë ndjeshëm nivelet e cilësisë së shërbimit dhe uljen e kohës së shpenzuar në departamentet qeveritare.

E-government përmirëson shërbimet përmes kuptimit më të mirë të kërkesave të qytetarëve, duke përmirësuar shërbimet përmes transparencës, saktësisë dhe lehtësimit të informacionit që shkëmbehet midis qeverisë dhe qytetarëve. Ajo që ka rëndësi shumë për qytetarët është efikasiteti i shërbimeve që ofrohen. Efektiviteti i qeverisë matet me

[16] https://www.gemalto.com/press/pages/gemalto-releases-findings-of-2015-breach-level-index.aspx
[17] https://sq.wikipedia.org/wiki/Harduer_kompjuterik

cilësinë e ndërveprimeve të tij me qytetarët. Përpunimi i dokumenteve në një sistem tradicional qeveritar, është një detyrë e vështirë që konsumon shumë burime; koha e kaluar në dokumentet nuk krijon shumë vlerë për qytetarët. Kjo çështje bëhet edhe më e rëndësishme, kur marrim parasysh faktin, se qytetarët kërkojnë më shumë nga shërbimet publike. Me krijimin e një pike të centralizuar të komunikimit përmes e-qeverisjes, qeveritë mund të arrijnë efikasitet të lartë operacional.

Nga ana tjetër, kriminelët e kibernetikë, përmes sulmeve pirate kanë lehtësi në ndërhyrjen në bazat e të dhënave të sektorëve qeveritarë, në mënyrë që të përdorin informacionin e tyre. Përpos shumë dëmeve që sjell një sulm kibernetik, ai zvogëlon efektivitetin e një qeverie dhe kështu besimin e qytetarëve në qeveri. Veçmas kësaj studiues të ndryshëm argumentojnë se pavarësisht nga shumë përfitime që mund të arrihen përmes shkëmbimit së të dhënave apo shërbimeve *online,* mirëmbajtja e sistemeve është e kushtueshme edhe e vështirë dhe neglizhimi i mirëmbajtjes lehtëson punën e kriminelëve të kësaj fushe.

Përpos të gjithave shërbimi *e-government* po përqafohet masivisht nga shumë qeveri në botë, pasi përfitimet janë të mëdha. Është një sistem transparent dhe fikas, duke reduktuar kohën, zhdukur ryshfetin dhe korrupsionin. Sistemet e *e-qeverisjes* ndryshojnë nga një shtet në tjetrin, ndaj edhe sulmet kibernetike janë të ndryshme, por deri më tani, vendi ynë nuk është përballur me të tilla sulme, por kjo nuk do të thotë se sulme të tilla duhet të na gjejnë të papërgatitur.

3. Bashkëpunimi ndërkombëtar dhe politikat mbi sigurinë kibernetike

3.1 Bashkëpunimi në nivel kombëtar dhe ndërkombëtar për garantimin e sigurisë kibernetike

Krimi kibernetik ka dimension ndërkombëtar. Teknologjitë kompjuterike, krijohen për të ndryshuar dhe përmirësuar efikasitetin e proceseve të punës, në çdo aspekt të jetës, por bota e krimit nuk e përjashton veten, duke përfituar apo krijuar përfitime, përmes digjitalizimit dhe evoluimit të teknologjisë.

Përmes organizmave të ndryshëm ndërkombëtar për mbrojtje dhe siguri, u konstatua se vetëm duke u bashkuar në një e duke unifikuar ligje, dhe duke pasur objektiva të përbashkëta, mund të luftohet një fenomen si krimi kibernetik, i cili vepron me një shpejtësi të jashtëzakonshme.

Në vitin 2004, me vendim të Kuvendit të Republikës së Shqipërisë, ratifikohet "Konventa për krim në fushën kibernetike". Kjo konventë. mbështetur në nenin 42 të "Convention of Cyber Crime", 23.11.2001, Budapest, lëshuar nga Këshilli i Europës, rezervon të drejtën për të ngarkuar me përgjegjësi penale të gjithë autorët që kryejnë krime të kësaj natyre. Konventën e kanë nënshkruar gjithsej 58 vende, ku prej të cilave, 28 me ratifikim. Për sa i përket Shqipërisë, konventa u nënshkrua më 2001, u ratifikua më 15.9.2004, ndërsa hyri në fuqi më 1.1.2005.

Kjo konventë kishte për qëllim luftën kundër krimit kibernetik, si dhe një unitet mes vendeve, për të bashkëpunuar dhe shkëmbyer informacion në luftën ndaj këtij fenomeni, ndërmjet shteteve anëtare të BE. Konventa ishte një mjet i nevojshëm për të ndaluar kryerjen e veprimeve të paligjshme dhe ndëshkimin me ligj të autorëve, si dhe mbi nevojën për të siguruar një balancë të përshtatshme ndërmjet interesave të zbatimit të

ligjit dhe respektimit së të drejtave themelore të njeriut, sikurse është parashikuar në Konventën e Këshillit të Europës, të vitit 1950, për Mbrojtjen e të Drejtave të Njeriut dhe Lirive Themelore.

Shqipëria është pjesë e "Konventës së Këshillit të Evropës mbi ndihmën e përbashkët ligjore në çështjet penale", të vitit 1959, gjithashtu ratifikoi protokollin e parë dhe të dytë të "Konventës evropiane për ndihmën e ndërsjellët në çështjet penale", si dhe "Konventën mbi ekstradimin".

Vendi ynë bashkëpunon me shtetet e tjera në bazë të dispozitave të KPP ("Marrëdhëniet juridiksionale me autoritetet e huaja") dhe mbi bazën e ligjit nr. 10193, datë 3.12.2009 "Për marrëdhëniet juridiksionale me autoritetet e huaja në çështjet penale".

Një nga sfidat ndërkombëtare është mbrojtja nga krimi kibernetik dhe qëndrimi i shteteve lidhur me përbërjen dhe parandalimin e këtij krimi. Pjesa dërmuese e infrastrukturës së sotme si sistemet financiare, rrjetet elektrike, ujësjellësit, sistemi i kujdesit shëndetësor, sistemi bankar, sistemet e kontrollit të trafikut ajror detar tokësor etj., janë të lidhura me internetin, ndaj mbrojtja e këtyre sistemeve nga sulmet kibernetike, është çështje e sigurisë publike në rang kombëtar, ashtu sikundër është edhe në rang ndërkombëtar, pasi një pjesë e mirë e këtyre sistemeve, janë të lidhura dhe ndikojnë ndërkombëtarisht.

3.2 NATO dhe BE, si asistues me mekanizma të veçantë kundër krimit kibernetik

Bashkimi Evropian ka ndërmarrë një mori masash mbi mbrojtjen nga sulmet kibernetike, duke u kthyer në një prej lobuesve më të fuqishëm, për mbrojtjen e vendeve anëtare të BE-së, si dhe për të asistuar e ndihmuar shtete të tjera të botës, që hasen me këtë fenomen. BE-ja e cilëson krimin kibernetik si një nga fenomenet më negative në botë, i cili goditjen e shpërndan në të gjithë globin, jo vetëm në një shtet.

BE-ja ka ngritur një strukturë të posaçme për mbrojtjen ndaj këtij lloj krimi: "The European Cybercrime Centre (EC3)"[18]. Kjo qendër, e vendosur pranë strukturave të Europol-it, është pika kyçe e BE-së, në luftën kundër krimit kibernetik, ku me anë të reagimeve të shpejta, në rast të ndodhjes së krimeve *online* kontribuojnë në ndërtimin e kapaciteteve operacionale dhe analitike, për hetime dhe bashkëpunim me partnerët ndërkombëtarë, me qëllim forcimin e ligjit kundër krimit kibernetik në vendet anëtare, si dhe, garantimin e sigurisë së qytetarëve.

Në Deklaratën e Kryetarëve të shteteve dhe të qeverive, pjesëmarrës në samitin e NATO-s, në Strasburg, më 4 prill 2009, krahas të tjerash u theksua se: "Ne mbetemi të angazhuar të fuqizojmë sistemet e komunikimit dhe të informacionit që janë të rëndësisë vendimtare për Aleancën, kundër sulmeve *cyber*, duke qenë se aktorë shtetërorë dhe joshtetërorë mund të përpiqen të shfrytëzojnë padrejtësisht besimin në rritje të Aleancës dhe aleatëve në këto sisteme"[19].

Vendi ynë, do të bashkëpunojë me NATO-n për forcimin e mbrojtjes kibernetike, nëpërmjet kontributit, në zhvillimin dhe zbatimin e politikave të NATO-s dhe përmirësimit të mbrojtjes së sistemeve dhe rrjeteve të veta, si dhe ato të aleatëve. Trajnimi i specialistëve, mbetet një drejtim i rëndësishëm, për të formuar kapacitetet e nevojshme

[18] https://www.europol.europa.eu/content/megamenu/european-cybercrime-centre-ec3-1837.

[19] Deklarata e Kryetarëve të shteteve dhe të qeverive, pjesëmarrës në Samitin e NATO-s në Strasburg, 4 prill. 2009.

për mbrojtjen kibernetike. Për këtë, do të synohet pjesëmarrja e vijueshme në veprimtaritë që organizon NATO-ja, për mbrojtjen kibernetike, duke u trajnuar në struktura të mirëfillta, si: Qendra e Ekselencës për Mbrojtjen Kibernetike apo njohja e përvojave të vendeve të tjera të NATO-s, që kanë ngritur struktura të veçanta për këtë qëllim. Specialistët e trajnuar jashtë vendit do të shfrytëzohen për organizimin e trajnimeve në nivelin e MM/FA[20].

3.3 Garantimi i sigurisë publike përmes zbatimit të ligjit

Qëllimi i zbatimit të ligjit dhe hartimit të strategjive ka të bëjë me mbrojtjen e shtetit dhe në veçanti qytetarit, nga kërcënimet dhe rreziqet që janë të brendshme dhe të jashtme.

Ka disa ligje që rregullojnë ndjekjen penale të krimeve kompjuterike në Republikën e Shqipërisë, si:

- Ligji nr. 8888 i datës 25.4.2002 "Për ratifikimin e konventës për krimin kibernetik", është reflektuar në Kodin Penal.

- Ligji nr. 9262, i datës 29.7.2004, "Për ratifikimin e protokollit shtesë të konventës për krimin kibernetik, për penalizimin e akteve me natyrë raciste dhe ksenofobe të kryera nëpërmjet sistemeve kompjuterike", sërish është reflektuar në Kodin Penal përkatësisht.

- Ligji nr. 9859, datë 21.1.2008, "Për disa shtesa dhe ndryshime në ligjin nr. 7895, datë 27.1.1995", "Kodi Penal i R.Sh".

- Ligji nr. 10023, datë 27.11.2008, "Për disa shtesa dhe ndryshime në ligjin nr. 7895, datë 27.1.1995", "Kodi Penal i Republikës Së Shqipërisë.

- Ligji nr. 10054, datë 29.12.2008, "Për disa shtesa dhe ndryshime në ligjin nr. 7905, datë 21.3.1995.

- Ligj, nr. 144/2013, dt. Aktit: 2.5.2013, dt. miratimit: 2.5.2013, Fletore Zyrtare nr. 83, faqe 3526.

- Ligj nr. 144/2013, "Për disa shtesa dhe ndryshime në ligjin nr. 7895, datë 27.1.1995", "Kodi Penal i Republikës së Shqipërisë", i ndryshuar.

Për të garantuar siguri kombëtare është tejet i nevojshëm hartimi i një dokumenti, ku të evidentohen dhe përcaktohen strategjitë e sigurisë së informacionit dhe infrastrukturës kritike të tij. Është primare hartimi i strategjive kombëtare për të garantuar mbajtjen e një mjedisi operimi elektronik të sigurt, të qëndrueshëm dhe të besueshëm për vendin dhe qytetarët.

Këshilli i Ministrave, më datë 2.12.2015, miratoi me VKM-në nr. 973, "Dokumentin e politikave për sigurinë kibernetike 2015-2017", i cili ka për qëllim rishikimin dhe koordinimin e detyrimeve që lindin nga angazhimet e marra për një hapësirë kibernetike të sigurt, me qëllim që të sigurohet përmbushja e përgjegjësive nga të gjithë aktorët, në mënyrë të koordinuar[21].

Objektivat strategjike që do të ndiqen për përmbushjen e këtij vizioni, dhe respektimin e parimeve të mësipërme, janë:

- plotësimi i kuadrit ligjor në fushën e sigurisë kibernetike,
- forcimi i kuadrit institucional,
- rritja e ndërgjegjësimit për sigurinë kibernetike,

[20] Strategjia për Mbrojtjen Kibernetike, Ministria e Mbrojtjes, nëntor 2014.
[21] http://www.akce.gov.al/rreth-nesh/raportidokumentittepolitikave.pdf

- identifikimi dhe mbrojtja e infrastrukturave kritike të informacionit,
- krijimi dhe implementimi i kërkesave minimale të sigurisë kibernetike,
- forcimi i partneritetit me struktura të tjera përgjegjëse të fushës brenda dhe jashtë vendit,
- rritja e nivelit të njohurive, aftësive dhe kapaciteteve për ekspertizë në fushën e sigurisë kibernetike[22].

Zbatimi i ligjit luan një rol thelbësor në arritjen e objektivave kibernetike të vendit tonë duke hetuar një gamë të krimeve kibernetike, si vjedhja e të dhënave, mashtrimi, pornografinë *online*, etj., si dhe duke garantuar kapjen dhe vënien përpara organeve ligjzbatuese të personave përgjegjës. Për zyrtarët e zbatimit të ligjit në shumë raste kanë munguar mjetet e nevojshme për të trajtuar krimit; ligjet e vjetra nuk janë mjaft të përshtatshme për këto lloj krimesh, po ashtu edhe ekspertët e fushës, kërkojnë trajnime të vazhdueshme, pasi ky lloj krimi evoluon "me shpejtësinë e dritës".

Për shkak se interneti është një rrjet global, rregulli brenda shteteve të veçanta nuk mund të sigurojë mjetin dhe efektshmërinë e duhur, në luftën kundër kërcënimit kibernetik. Meqenëse çdo vend vendos vetë, nëse do të bashkëpunojë për procedurat kriminale që lidhen me sulmet kibernetike, zgjidhjet e ligjshme për mbrojtjen e hapësirës kibernetike, funksionojnë vetëm kur zbatohen nga çdo vend, dhe kur ka bashkëveprim ndërmjet vendeve, mbi bazën e një marrëveshje ligjore përkatëse, dy ose shumëpalëshe.[23]

4. Rekomandime

1. Fëmijët, të rriturit, të gjithë qytetarët e republikës së Shqipërisë duhet të edukohen dhe informohen mbi të mirat dhe rreziqet e botës virtuale.

2. Kompanitë celulare duhet të krijojnë filtra që mbrojnë fëmijët nga përdorimi i internetit në faqe me rrezikshmëri të lartë.

3. Shihet nevoja e hartimi të një ligji të veçantë për krimin kibernetik ku të jenë të evidentuara të gjitha format e tij.

4. Nevojitet më shumë bashkëpunim dhe koordinim midis grupeve të ndryshme të interesit për hartimin e një legjislacioni të ri mbi krimin kibernetik.

5. Të specializohen prokurorët, efektivët e policisë dhe gjyqtarët, për këtë lloj krimi.

6. Rritja e numrit të ekspertëve në fushën e hetimit dhe ndjekjes penale të krimit kibernetik duke i dhënë mundësinë të trajnohen brenda dhe jashtë vendit.

7. Të nënshkruhet një memorandum bashkëpunimi në fushën e krimit kibernetik, midis të gjitha agjencive ligjzbatuese.

8. Fuqizimi i institucioneve ligjzbatuese duke i krijuar kapacitetet e nevojshme për të reaguar menjëherë në çdo rast emergjent.

9. Nevojitet të merren masa për ndarjen dhe qarkullimin e të dhënave dhe informacionit në mënyrë më të sigurt, si brenda institucioneve publike ashtu edhe atyre private, me qëllim parandalimin dhe luftën kundër krimit dhe garantimin e politikave të duhura të sigurisë[24].

10. Të forcohet mbrojtja e sistemeve të operimit në administratën publike, si dhe nëpërmjet AKSH-it të ndalohet lundrimi në sajte të ndryshme *online*.

[22] "Dokumenti i politikave për sigurinë kibernetike, 2015-2017", f. 21.
[23] Krimi kibernetik dhe legjislacioni ndërkombëtar, Etleva Haka.
[24] Krimi kompjuterik, strategjia dhe siguria kombëtare, Nertil Bërdufi.

Bibliografia

1. Strategjia për mbrojtjen kibernetike 2018-2020.
2. Strategjia për Mbrojtjen Kibernetike, Ministria e Mbrojtjes.
3. Convention on Cybercrime, 23.XI.2001.
4. Strategies for the promotion of broadband services and infrastructure: a case study on Albania, Board CommisionUnderstanding cybercrime: Phenomena, challenges and legal response, ITU publication, Prof. Dr. Marco Gercke
5. Cyber Crime and Cyber Security: A White Paper for Franchisors, Licensors, and Others by Bruce S. Schaeffer, Henfree Chan Henry Chan and Susan Ogulnick
6. Situating the Public Police in Networks of Security within Cyberspace by David Wall
7. Effects of Cybercrime on State Security: Types, Impact and Mitigations with the Fiber Optic Deployment in Kenya, IBIMA Publishing Journal of Information Assurance & Cybersecurity http://www.ibimapublishing.com/journals/JIACS/jiacs.html
8. A Study on Child Online Safety in Albania, World Vission
9. The law enforcement challenges of cybercrime: are we really playing catch-up?, Dr. Ben Hayes, Dr. Julien Jeandesboz, Dr. Francesco Ragazzi, Dr. Stephanie Simon, Prof. Valsamis Mitsilegas, Eurepean Parliament
10. Cybersecurity Guide for State and Local Law Enforcement,National Consortium for Advanced Policing
11. A to Z of Cyber Crime Asian School of Cyber Laws
12. Digitalizing Albanian Government, role of internet in managing government communication, Eva Londo
13. Policing Cybercrime, Petter Gotschalk
14. Cybercrime: A National Security Issue? By Lior Tabansky
15. International Journal of Juridical Sciences, www.juridicaljournal.univagora.ro ISSN 1843-570X, E-ISSN 2067-7677 No. 1 (2015), pp. 62-66
16. Towards a More Resilient Cyberspace: The Case of Albania, Rovena BAHITI and Jona JOSIFI
17. Vendim nr. 973, datë 2.12.2015, "Për miratimin e dokumentit të politikave për sigurinë kibernetike 2015-2017".
18. Ligji nr. 8322, datë 2.4.1998 "Për ratifikimin e Konventës së Këshilllit të Europës për ekstradimin dhe të dy protokolleve shtesë".
19. Ligj nr .9918, datë 19.5.2008 (i ndryshuar) "Për komunikimet elektronike në Republikën e Shqipërisë".
20. Ligji nr. 102/2012, "Për disa ndryshime dhe shtesa në ligjin nr. 9918, datë 19.5.2008 'Për komunikimet elektronike në Republikën e Shqipërisë' ".
21. Ligji nr. 7905, datë 21.3.1995, "Kodi i Procedurës Penale i Republikës së Shqipërisë", i ndryshuar.
22. Krimi i organizuar, vlerësimi i riskut në Shqipëri, Fabian Zhilla, Besfort Lamallari.
23. Raport i Prokurorisë së Përgjithshme, viti 2015, 2016, 2017.
24. http://www.pp.gov.al/web/Raporte_te_Prokurorit_te_Pergjithshem_353_1.php#.W65ZEWgzaM-

Adresa interneti

1. https://lawaspect.com/traditional-crime-cyber-crime/
2. https://www.pgitl.com/explore/article/what-is-the-difference-between-cyber-crime-and-traditional-crime
3. http://cco.ndu.edu/Portals/96/Documents/books/Beyond%20Convergence/BCWWO%20Chap%2013.pdf?ver= 2016-10-25-125 402-513
4. http://univagora.ro/jour/index.php/aijjs/article/viewFile/1910/605
5. http://www.cybercrimejournal.com/ibrahimmarcusIJCCJuly2009.pdf
6. https://waset.org/publications/9999296/curbing-cybercrime-by-application-of-internet-users-identification-system-iuis-in-nigeria
7. http://www.akce.gov.al/wp-content/uploads/2016/04/Dokumenti%20i%20 Politikave%20per%20 Sigurine%20Kibernetike% 202015-2017.pdf
8. https://www.independent.co.uk/news/uk/crime/mafia-cybercrime-booming-and-with-it-a-whole-service-industry-says-study-9763447.html
9. https://www.floridatechonline.com/blog/information-technology/a-brief-history-of-cyber-crime/
10. file:///C:/Users/Valeria/Downloads/Cyber%20crime.pdf
11. https://www.corwin.com/sites/default/files/upm-binaries/25522_Chap02.pdf
12. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.470.3895&rep=rep1&type=pdf
13. http://anali.ius.bg.ac.rs/Annals%202006/Annals%202006%20078-086.pdf
14. https://www.scmagazine.com/cybercrime/topic/47218/
15. https://bohatala.com/cybercrime-types-cybercrime/
16. http://www.crossdomainsolutions.com/cyber-crime/
17. http://www.akce.gov.al/wp-content/uploads/2016/04/Dokumenti%20i%20 Politikave%20per%20 Sigurine%20Kibernetike% 202015-2017.pdf
18. https://www.pgitl.com/explore/article/what-is-the-difference-between-cyber-crime-and-traditional-crime
19. https://lawaspect.com/traditional-crime-cyber-crime/
20. https://home.kpmg.com/xx/en/home/insights/2016/05/five-ways-for-governments-to-tighten-up-cyber-security.html

21. https://www.business.gov.au/risk-management/cyber-security
22. https://www.accenture.com/us-en/insight-ways-government-prepare-cybercrime
23. http://knowledge.wharton.upenn.edu/article/mobile-devices-and-cybercrime-is-your-phone-the-weakest-link/
24. https://www.techrepublic.com/blog/10-things/10-ways-to-avoid-viruses-and-spyware/
25. http://www.panorama.com.al/krimi-kibernetik-50-biznesmeneve-shqiptare-iu-vodhen-2-5-mln-euro/
26. http://www.scan-tv.com/me-pak-krim-kibernetik-prokuroria-147-procedime-ne-2017-dominon-mashtrimi-kompjuterik/
27. http://www.gsh.al/2018/07/09/krimi-kibernetik-flet-eksperti-semanaj-shqiperia-e-rrezikuar/
28. http://top-channel.tv/2017/01/05/rreziku-nga-krimi-kibernetik-dhe-mashtrimet-policia-kujdes-femijet/
29. http://www.mod.gov.al/images/PDF/2017/Strategjia_Mbrojtjen_Kibernetike_2018_2020.pdf
30. https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20180417-albania-report.pdf
31. https://www.osce.org/sq/skopje/121225?download=true
32. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3


AKADEMIA E SIGURISË
AS
1971

Siguria dhe terrorizmi kibernetik

■**Dr. (proc.) Nënkolonel Flora DAKO**
Shtabi i Përgjithshëm i Forcave të Armatosura të RSH-së
flora.dako@aaf.mil.al

Abstrakt

Në ditët e sotme, informacioni, i trajtuar në të gjitha format e mundshme, elektronike apo tradicionale, përbën një pasuri të vërtetë si për individët ashtu dhe për organizmat private apo shtetërore dhe konsiderohet si një burim strategjik rreth të cilit zhvillohet ajo që sot quhet shoqëria e informacionit. Mënyra e marrjes dhe dhënies së informacionit ndryshon nga një vend në tjetrin për vetë faktin e mundësive të implementimit të modeleve dhe mënyrave të reja të komunikimit. Shikojmë që në një distancë kohore një vjeçare, teknologjia dhe informacioni ndryshon me një progres të madh të paparashikueshëm. Këtë mund ta quajmë pa frikë një kërkesë apo nevojë drastike e shoqërisë për ndryshime që pasojnë njëra-tjetrën, por pa menduar ndikimin që këto ndryshime të vazhdueshme kanë në sigurinë e jetës tonë dhe të fëmijëve tanë. Në teknologjinë e telekomunikacionit në të gjithë globin më i përdoruri është interneti, i cili shërben si burim të dhënash për çdo pyetje apo pikëpyetje që ne kemi. Por në shumë raste kërkimi ka rezultuar fatal në shkatërrimin e të dhënave personale, të organizatës apo dhe të një shteti, dhe kjo nëpërmjet manipulimit, fshirjes, modifikimit dhe survejimit të informacioneve që qarkullojnë në rrjetet e komunikimit. Kështu, siguria e informacionit është e lidhur direkt me sovranitetin e individit, grupeve shoqërore apo të një shteti, e cila realizohet nga mbrojtja e infrastrukturave kritike, e sistemeve dhe e rrjeteve, e pasurive kulturore të kombit, e të mirave materiale dhe jo materiale, pra në mbrojtjen e vlerave. Nëse ne marrim njohuri dhe kemi një kulturë në mënyrën se si duhet të përballemi me ndryshimet në komunikimin online, atëherë do të jemi më të përgatitur dhe më të aftë për të shmangur veprimet shkatërruese të çdo lloj informacioni që ne disponojmë, që nga ai personal e deri tek ai kombëtar.

Fjalëkyçe:
komunikim, siguri, terrorizëm, mbrojtje, strategji kibernetike.

1. Hyrje

Përdorimi i kompjuterëve si mjet për të prodhuar informacion të rremë apo që planifikojnë dhe kontrollojnë krime, të cilat mund të kryhen në një ardhme, tashmë është bërë pothuajse i modës për grupet terroriste në të gjithë globin. Mënyra tradicionale, ose ajo e flijimit personal, tashmë po kursehet dhe ndodh më rrallë se sa në vitet e mëparshme, dhe duke përdorur, metodat më të sofistikuara që shkatërrojnë jetë të njerëzve të pafajshëm dhe mbrojnë jetët e kriminelëve.

Nga vetë emri "terrorizëm kibernetik" kuptohet çdo sjellje e kryer nëpërmjet veprimeve elektronike të cilat drejtohen ndaj sigurisë së sistemeve kompjuterike dhe të dhënave të përpunuara prej tyre. Kuptohet që këto veprime janë të paligjshme dhe cenojnë rëndë sigurinë personale, të një grupi të caktuar shoqëror dhe të një vendi në tërësi. Kjo varet nga shkalla e impaktit që sulmi kibernetik ka dhe në kalkulimet e bëra nga grupet terroriste për arritjen e një goditje të caktuar[1].

Të gjitha llojet e krimeve apo të mashtrimeve, shkelin sigurinë njerëzore dhe kombëtare, duke filluar që nga bixhozi i paligjshëm, skemat piramidale, mashtrimi me karta krediti dhe lloje të tjera të aktiviteteve të paligjshme. Në dallim nga krimet tradicionale, krimi kibernetik është një krim global. Këto lloj krimesh, kryhen përmes hapësirave dhe rrjeteve kompjuterike dhe nuk ndalojnë në kufijtë konvencionale shtetërorë. Ato mund të parapërgatiten nga kudo dhe kundër një përdoruesi kompjuteri në një vend çfarëdo të globit. Përveç rritjes së shkallës së aktivitetit kriminal në shkeljet me natyrë të krimeve kompjuterike, ka një tendencë për t'iu shmangur kategorive

[1] US Department of Justice, Computer Crime and Intellectual Property Section (CCIPS), *CCIPS Documents And Reports*, https://www.justice.gov/criminal-ccips/ccips-documents-and-reports.

tradicionale të shkeljeve.

Në vendin tonë deri para pak viteve nuk ka pasur ligje të mirëfillta për krimet kibernetike, por duke parë aktet e shumta terroriste në disa vende të botës, dhe ligjvënësit tanë kanë filluar të ndërgjegjësohen ndaj këtij rreziku të pashmangshëm, i cili rrezikon gjithnjë e më shumë sigurinë e jetës. Duke qenë dhe pjesë e Forcave të Armatosura dua të përmend dhe analizoj një dokument të rëndësishëm të prodhuar nga Ministria e Mbrojtjes, i cili është "Strategjia për mbrojtjen kibernetike 2018-2020". Ky dokument është dhe udhërrëfyes për masat që duhen marrë për parandalimin e sulmeve terroriste nëpërmjet teknologjive të reja kompjuterike, të cilat po vijnë e bëhen gjithnjë e më shumë të sofistikuara.

Duke njohur se sa shumë krime mund të kryhen dhe duke bërë një analizë nga ekspertët e fushës, atëherë mund të jemi në gjendje të dimë se sa duhet të shpenzojmë në lidhje me sigurinë.

2. Format dhe tiparet e krimit kibernetik

Teknologjitë e reja sot janë në ndryshim të vazhdueshëm dhe për rrjedhojë dhe rreziqet e lidhura me këtë teknologji evoluojnë në të njëjtën mënyrë me një shpejtësi të paparashikueshme. Krimi kibernetik ka të bëjë me veprimtarinë kriminale të zhvilluar në rrjetin kompjuterik. Duke e përkufizuar në mënyrën më precize mund të themi se krimi kibernetik është përdorimi i kompjuterit / internetit për të shkaktuar terror tek të tjerët, pa dallim moshe e besimi. Me fjalë të tjera terrorizmi kibernetik është një ndërthurje e terrorizmit dhe hapësirës kompjuterike. Ai është përkufizuar si një sulm i paramenduar, më shumë me ndikim politik, i motivuar kundër informacionit, sistemeve a programeve kompjuterike, dhe të dhënave të cilat pasojnë në dhunë, kundër shënjestrave nga grupeve ndërkombëtare apo agjentë klandestinë[2]. Sulmet që shkaktojnë vdekje, dëmtime trupore, shpërthime, rënie avionësh, kontaminim uji apo humbje të ndryshme ekonomike, mund të jenë shembuj. Sulme të rrezikshme mund të kryhen ndaj infrastrukturës dhe të jenë krime kompjuterike, në varësi të impaktit të tyre.

Duke analizuar sulmet e viteve të fundit në vende të ndryshme dhe në vende që konsiderohen të zhvilluara dhe me një zhvillim të vazhdueshëm në ekonomisë dhe sigurisë, duhet të kuptojmë mirë këtë nocion dhe në të vërtetë ka një dallim të nocionit krim kibernetik nga krimi informatik, sepse krimi kibernetik kryhet duke pasur në funksion dhe shërbim kompjuterin. Pra, duket që krimi kibernetik është një nënkategori e krimit kompjuterik, ku kompjuteri shërben si "lëndë e parë" për realizimin e një projekti dhe sulmi terrorist.

Duke e parë që interneti është një nga rrjetet më të përdorur sot, ne arrijmë të kuptojmë dhe të evidentojmë që qenia në rrjet na ekspozon ndaj rrezikut të një sulmi të mundshëm. Zgjidhja nuk do të ishte largimi nga interneti, sepse më pas do kishim zhdukje të konkurrencës në fusha të ndryshme, dhe kjo do të pengonte konkurrencën dhe për rrjedhojë paralizojnë zhvillimin global. Një aspekt tjetër që duhet trajtuar për të kuptuar fenomenin e krimit kibernetik, është dhe teknologjia e përdorur e cila mbetet pak a shumë jotransparente për përdoruesin. Historikisht, rrjeti komunikues u zhvillua

[2] Adam Gorlick, "Obama at Stanford: Industry, government must cooperate on cybersecurity", February 13, 2015, *President Barack Obama addressing the White House Summit on Cybersecurity and Consumer Protection at Stanford* .
http://news.stanford.edu/ne%C3%ABs/2015/february/summit-main-obama-021315.html

si një mjet i fushës ushtarake për t'u përdorur më pas nga fushat e tjera për të lehtësuar komunikimin ndërmjet tyre.

Nëse sot dëgjojmë apo flasim për sulm kibernetik, kuptohet që ky është një veprim absolutisht i matur, i paramenduar dhe i parapërgatitur në mënyrën më të sofistikuar të mundshme për të ndërhyrë në sisteme dhe të dhëna personale apo shtetërore pa pasur akses dhe autoritet ligjor.

Format më të dukshme dhe të evidentuara të krimit kibernetik në kohën e sotme janë:

- krim kibernetik ndaj individit
- krim kibernetik ndaj pronës
- krim kibernetik ndaj organizatës
- krim kibernetik ndaj shoqërisë[3].

Përballë shteteve dhe organizatave ndërkombëtare, eksitojnë një numër i konsiderueshëm i organizatave terroriste, ose afërsisht sa dyfishi i shteteve anëtare të Kombeve të Bashkuara. Terrorizmi i sotëm është një rrezik jo vetëm rajonal por edhe global. Rrezikshmëria sipas këtij klasifikimi varet nga shpërndarja gjeografike e organizatave terroriste. Për t'i dhënë përgjigje pyetjes në se jemi të kërcënuar globalisht apo rajonalisht, duhen marrë në konsideratë dhe analizuar shumë faktorë, disa prej të cilëve po i radhisim më poshtë:

- gjeografia e shtrirjes së shteteve të etiketuara "terroriste", aleancat dhe marrëdhëniet e tyre të ngushta politike, ekonomike e ushtarake me faktorë dhe aktorë politikë rajonalë;
- lidhjen e faktorëve rajonalë me shtete që kanë adoptuar programe për prodhimin dhe tregtimin, dhe pse jo, trafikimin e armëve bërthamore apo të dëmtimit në masë;
- nivelin e bashkëpunimit ndërkombëtarë të faktorëve rajonalë në funksion të ndërprerjes së burimeve financiare të dyshimta dhe "pastrimit të parave të pista"; rajonet dhe vatrat e militarizuara në ekstrem dhe me premisa krizash serioze me motivim etniko-nacional, politik e religjioz.

Prania e këtij rreziku eminent dhe real të sigurisë globale, shtron përpara shteteve dhe institucioneve të sigurisë një detyrë të madhe. Së pari ajo që kërkohet mendoj se është t'i vësh përballë këtij terrorizmi global një përpjekje globale. Për këtë kërkohet bashkëpunim dhe integrim të përpjekjeve të të gjithë shteteve, pra mirëfunksionimin normal të një koalicioni antiterrorizëm. Së dyti, lufta kundër terrorizmit duhet goditur në rrënjët e tij. Për ta bërë këtë, duhet të studiohen metodat, shkaqe e krijimit dhe të funksionimit të terrorizmit. Kjo gjithashtu kërkon bashkëpunim ndërshtetëror e ndërinstitucional[4].

3. Kërcënimet kibernetike ndaj sigurisë së vendit

Krimi tradicional mund të cenojë sigurinë e brendshme të një vendi, po ashtu edhe krimi kibernetik mund të këtë pasoja të rënda në këtë aspekt. Po krimi ekonomik nuk përbën një fushë që do të cenonte rëndë sigurinë kombëtare të një shteti sovran? Çfarë vendi zë fenomeni i korrupsionit dhe lufta kundër tij në strategjinë e sigurisë së brendshme? Një gjë është e sigurt dhe për këtë shifrat na japin të drejtë krimi ekonomik

[3] Jimmy Sproles, Will Byars, "Examples of Cyber Terrorism", *Paper for Computer Ethics Class,* 1998.
[4] Kolë Krasniqi, *Terrorizmi Ndërkombëtar,* Prishtinë, 2010.

po e zhvendos gjithnjë e më shume fushën e tij të veprimit në aktivitete *online*, si mënyra më e lehtë dhe më fitimprurëse. Le të përmendim këtu rastin e Bankës së Sicilisë në vitin 2000, ku një grup prej 20 personash, natyrisht me njohuri specifike në fushën e informatikës dhe të lidhur me disa familje mafioze, arritën të krijonin një klon të servisit *e-banking* të bankës. Kështu, arritën në këtë mënyrë të përvetësonin shumën prej 400 milion $ të vëna në dispozicion nga Komuniteti Europian për zhvillimin rajonal. Le të kujtojmë që para disa viteve gati 500 shtetas shqiptarë u mashtruan me një skemë vjedhjeje, tashmë të njohur si ajo e lotarisë, dhe falën kursimet e tyre kush e di se ku e kujt? Kush janë përgjegjësitë në këtë ngjarje?

Ka kohë ku qeveria shqiptare vendosi që tani aplikimet për tendera do të bëhen nëpërmjet internetit dhe në mënyrë të përqendruar. Kjo natyrisht do të thotë shërbim më cilësor e më i shpejtë. Po cilat janë rreziqet që një iniciativë e tillë të bjerë pre e sulmeve të personave të interesuar për destabilizim e përfitim? Sa jemi të përgatitur për të përballuar këto sulme dhe mbi të gjitha nëse sulmi fatkeqësisht del me sukses, çfarë jemi gati të humbim dhe çfarë ka vlerë më të madhe? Pa u përgjigjur këtyre pyetjeve, nuk mund të imagjinojmë masat teknike që duhen marrë. Le t'i kthehemi pak çështjeve më tradicionale të sigurisë kombëtare si për shembull mbrojtja e kufirit, parandalimi i kriminalitetit transnacional, apo dhe mbrojtja e infrastrukturave kritike siç janë burimet e energjisë, të ujit të pijshëm, kontrollit të mallrave ushqimorë apo mjekësorë, etj. Pavarësisht që këto që përmendëm mund të jenë shumë të ndryshme në natyrën e tyre, një gjë i bashkon në epokën ku jetojmë, – menaxhimi nëpërmjet teknologjive kompjuterike[5].

Dëmi do të ishte i njëjtë si ai i një eksplozivi në një nga infrastrukturat, ashtu dhe dhënia e një komande të gabuar në sistemin e drejtimit. Dëmi do të ishte i njëjtë si kalimi natën i një krimineli dhe futja e tij në territorin tonë, ashtu dhe fshirja e të dhënave të tija kompromet uese në kompjuterët apo serverët e policisë. Dëmi do të ishte po i njëjtë si futja e mallrave të skaduar apo të rrezikshëm, në territorin tonë, ashtu dhe falsifikimi i të dhënave në lidhje me këto mallra. Terrorizmi kibernetik është një nocion shumë i përfolur dhe shqetësues vitet e fundit. Dhe këtu spekulimet janë të shumta: disa e quajnë demagogji, disa e quajnë realitet. Në fakt është e vërtetë, me internetin nuk mundesh të vrasësh njerëz direkt. Po indirekt? A nuk ekzistojnë vallë me miliona *website* të financuara kush e di nga kush që bëjnë një propagandë aktive në favor të kësaj apo asaj organizate? Më keq akoma, a nuk ekzistojnë me qindra *website* që të mësojnë se si të fabrikosh bomba artizanale? Kundër kujt do të përdoren? Komenti mbi këtë realitet do të ishte i tepërt, ajo çfarë nevojitet është kundërpërgjigja e organeve të specializuara pra interneti duhet të konsiderohet si infrastrukturë kritike e denjë për tu mbrojtur.

Për të shkuar përtej kufijve të Shqipërisë kujtojmë luftën e Kosovës, ku NATO-ja u përball disa ditë me bllokimin e llogarisë së postës elektronike dhe të faqes së internetit. Një valë sulmesh masive trejavore ndaj rrjetit kompjuterik, tregoi se shoqëritë anëtare të NATO-s, tejet të varura nga komunikimi elektronik, ishin gjithashtu shumë të cenueshme në frontin kompjuterik. Disa e konsideronin si nga ngrirje të këtij funksionimi nga ana e autoriteteve të NATO-s, në mënyrë që të mos kishte rrjedhje informacioni, por kjo ishte një e vërtetë dhe kërkonte një kundërveprim teknik të zgjuar të specialistëve të NATO-s, që në atë kohë ishte paksa e kufizuar.

Duke shkuar më tej, u deshën ngjarjet e 11 shtatorit për të ndryshuar atë perceptim.

[5] Luan Hoxha, *Lufta Informative*, Kolegji i Mbrojtjes, Akademia e Forcave të Armatosura të RSH.

Dhe madje ishin të nevojshme incidentet në Estoni në verën e vitit 2007 për të përqendruar më në fund vëmendjen e plotë politike për këtë burim në rritje të kërcënimeve ndaj sigurisë publike dhe stabilitetit shtetëror. Që atëherë, spiunazhi kompjuterik është bërë një kërcënim pothuajse i vijueshëm. Incidente të ngjashme kanë ndodhur pothuajse në të gjitha shtetet e NATO-s dhe më dukshëm vitet e fundit përsëri në Shtetet e Bashkuara. Këtë herë u prekën më shumë se 72 shoqëri, përfshirë 22 zyra qeveritare dhe 13 kontraktues të fushës së mbrojtjes.

Kujtojmë konfliktin Gjeorgji-Rusi, u kryen sulme masive mbi faqet e internetit të qeverisë dhe të shërbimeve kompjuterike në Gjeorgji, duke i dhënë një formë më konkrete termit të luftës kompjuterike. Këto veprime nuk kanë shkaktuar dëme fizike. Por, sidoqoftë, ato dobësuan qeverinë gjeorgjiane gjatë një fazë të vështirë të konfliktit. Ato gjithashtu ndikuan në aftësinë e saj për të komunikuar publikun kombëtar dhe ndërkombëtar.

Duke shkuar më tej, në verën e vitit 2010, u përhap lajmi se rreth 45 000 sisteme kontrolli të punës të "Siemens"-it në të gjithë botën ishin infektuar nga një virus *trojan* i përshtatur, që mund të manipulonte proceset teknike me rëndësi të veçantë për centralet bërthamore në Iran. Edhe pse vlerësimi i dëmeve mbetet ende i paqartë, kjo tregoi rrezikun e mundshëm të programeve të kamufluara në sistemet kompjuterike të rëndësisë së veçantë që administrojnë furnizimin me energji apo rrjetet e trafikut. Për herë të parë, këtu u dha prova se sulmet kompjuterike përmbajnë në vetvete mundësinë për të shkaktuar dëme të njëmendta fizike dhe për të rrezikuar jetën e njerëzve.

Gjithë këto raste dhe analizat e bëra nga ekspertë të fushës së sigurisë dhe mbrojtjes, i hapën rrugën vendimeve kryesore të marra në Lisbonë, në vitin 2010 për të shqyrtuar në vijimësi mbrojtjen kompjuterike si një çështje të pavarur në rendin e ditës të NATO-s. në këtë takim u hodh edhe rishikimi i konceptit të mbrojtjes dhe sigurisë brenda vendeve të NATO-s. Me vendimet e Lisbonës, në nëntor 2010, Aleanca më pas përgatiti me sukses truallin për një shqyrtim të vetëdrejtuar dhe të bazuar në fakte të çështjes. Duke vepruar në këtë mënyrë, NATO-ja, jo vetëm që është duke kryer një ripërtëritje aq shumë të nevojshme të strukturave, si: aftësia kundërvepruese e NATO-s ndaj incidenteve kompjuterike, por gjithashtu, e bashkuar, si një aleancë, po përgatitet për të përballuar sfidat mjaft të dallueshme dhe në rritje ndaj mbrojtjes kompjuterike[6].

Në përshtatje me Konceptin e ri Strategjik të NATO-s, politika e rishikuar e NATO-s mbi *mbrojtjen kompjuterike* i përcakton kërcënimet kompjuterike si një burim të mundshëm për mbrojtjen e përbashkët, në përputhje me nenin 5 të NATO-s. Për më tepër, politika e re, - dhe *Plani i Veprimit* për zbatimin e saj, – i mbështet shtetet e NATO-s me udhëzime të qarta dhe me një listë përparësish, të miratuara mbi mënyrën e çuarjes përpara të mbrojtjes të Aleancës, përfshirë fuqizimin e bashkërendimit brenda NATO-s, si dhe me partnerët ndërkombëtarë.

Kompjuterët, institucionet shtetërore, kompanitë, individët, organizatat civile, strukturat që kryejnë funksione, makineritë dhe komplekset që drejtohen me sisteme informatike dhe interneti, janë objekt i sulmeve kibernetike. Sistemet kompjuterike të cilat i kemi dëgjuar shpesh në vitet e fundit, pra sistemet e botës virtuale, nënkuptojnë pafundësinë e quajtur hapësirë kibernetike. Njerëzit që përdorin këto mjete dhe të gjitha makineritë me bazë kompjuterin, ndodhen nën presionin e vazhdueshëm të sulmeve serioze kibernetike. Sot, siguria e informacionit, përbën pjesën më të madhe të

[6] https://www.nato.int/docu/review/2011/11-september/Cyber-Threads/AL/index.htm

sigurisë kombëtare të një vendi. Të gjitha përfundimet dhe proceset e së shkuarës, që përftoheshin me terror, tashmë mund të arrihen me sulme kibernetike. Pra, prej kohësh në grupet e terrorizmit është shtuar dhe terrorizmi kibernetik. Por, nuk duhet harruar që sulmet kibernetike botërore janë të pamundura të organizohen nga një grup njerëzish, të pavarur nga shtetet që kanë rivalitete botërore. Tashmë, bota kibernetike është një fushë e re lufte. Hapësira, është pika lidhëse e luftërave kibernetike.

Duke marrë si shembull rastin e Turqisë, vihet re se ajo është në qendër të këtyre sulmeve. Bashkë me internetin janë rritur edhe sulmet kibernetike. Interneti kërkohet të shpërndahet në të gjithë botën pa pagesë. Sot, numri i përdoruesve të internetit në botë, është 3.8 miliard dhe interneti tashmë, është një ndërmjetës shumë i rëndësishëm i politikës së jashtme. Në qoftë se gjithë bota do të pajisej me internet, atëherë sulmi kibernetik që mund të ndodhte, do të ishte edhe më i efektshëm.

Internetin, sikurse energjinë elektrike, po e ofrojnë si një formë joshje për lehtësimin e jetës, veçse interneti, po ashtu si energjia, nuk është vetëm lehtësues, por ka dhe anën e marrjes nën kontroll. Sulmet kibernetike dhe përgjimet e kompjuterëve është e mundur të realizohen edhe në mungesë të internetit. Shembull për këtë janë linjat elektrike, të cilat ofrojnë edhe mundësinë e përgjimit, edhe atë të ndërlidhjes; p.sh. pjesa më e madhe e sulmeve kibernetike drejt Turqisë nuk ndodhin vetëm nëpërmjet internetit sikurse supozohet, por realizohen edhe mes linjave elektrike.

Turqia, përveç Qipros, ka lidhje elektrike me të gjitha vendet fqinje. Sistemi elektrik që bënë të mundur lidhjet ndërkombëtare ose rajonale njihet me emrin interkonjeksion. Turqia është e lidhur me rrjetet elektrike të Irakut, Sirisë, Iranit, Gjeorgjisë, Bullgarisë, Greqisë, Azerbajxhanit, Rusisë dhe Armenisë nëpërmjet sistemit interkonjeksion. Brenda këtyre vendeve, Siria është vendi që i ka bërë më tepër sulme Turqisë nëpërmjet linjave elektrike, por autor i këtyre sulmeve nuk është as Siria dhe as qeveria e Asadit. Përdorimi i shtetasve të huaj si bazë dhe identitet të rremë, është një taktikë e vjetër dhe Turqia për "inxhinierët e rrugëve", "inxhinierët e bujqësisë" dhe "inxhinierët e digave" në Siri, ka mjaftueshëm informacion.

4. Kapacitetet kombëtare për mbrojtjen kibernetike

Nga qeveria shqiptare janë marrë masa dhe janë ndërgjegjësuar nga rreziku kibernetik që po kanos sot botën në zhvillim. Janë një sërë dokumentesh që institucionet tona të sigurisë bazohen për të realizuar punën e tyre të vështirë, e cila kërkon jo vetëm ekspertizë të fushës së sigurisë, por dhe inxhinierë dhe programues të zotë.

Dua të përmend një dokument shumë të rëndësishëm dhe me vlera, Strategjia për Mbrojtjen Kibernetike 2018-2020 e Ministrisë së Mbrojtjes, e cila është përgatitur dhe mbështetur në një sërë dokumentesh të rëndësishme si: Dokumentin "NATO Enhanced Cyber Defence Policy" (Samiti i Wellsit, shtator 2014), i cili konsideron mbrojtjen kibernetike si pjesë të detyrave kryesore të Aleancës për mbrojtjen kolektive, duke konfirmuar që në hapësirën kibernetike zbatohet ligji ndërkombëtar; Vendimet e Samitit të Varshavës (qershor 2016), i cili rikonfirmoi mandatin mbrojtës të NATO-s dhe njohu hapësirën kibernetike si një "domain" operacional, në të cilin NATO-ja duhet të mbrojë veten me efektivitet ashtu siç vepron në ajër, tokë dhe det; Programi i NATO-s "Cyber Defence Pledge", i cili përfshin miratimin e vendeve të Aleancës që të zgjerojnë mbrojtjen kibernetike për rrjetet dhe infrastrukturat kombëtare, të cilat konsiderohen si një çështje me prioritet në të cilën çdo vend aleat, në respekt të përgjegjësive të tij, të përmirësojë

qëndrueshmërinë dhe aftësinë për t'u përgjigjur shpejt dhe me efektivitet ndaj sulmeve kibernetike[7].

Çdo vend Aleat është dhe do të jetë përgjegjës për të mbrojtur rrjetet e tij kombëtare, të cilat janë të nevojshme të jenë të përshtatshme me ato të NATO-s dhe të njëri-tjetrit, si dhe të zgjerohet shkëmbimi i informacionit për mbështetje të përbashkët në parandalimin, zvogëlimin dhe rigjenerimin nga sulmet kibernetike. Strategjia e Sigurisë Kombëtare 2014-2020 "Për vendosjen dhe respektimin e standardeve më të larta në drejtim të ruajtjes dhe mbrojtjes së informacionit në të gjitha trajtat e ekzistencës së tij, duke përqendruar përpjekje të veçanta për mbrojtjen nga sulmet kibernetike"; VKM nr. 303, datë 31.03.2011 "Për krijimin e njësive të teknologjisë së informacionit e të komunikimit në Ministritë e linjës dhe Institucionet e varësisë"; ligji nr. 2/2017 "Për Sigurinë Kibernetike".

Ashtu si në territorin e vendit tonë edhe jashtë tij në misione, personeli i mbrojtjes (MM/FA) përdorin internetin (*cloud computing*), pajisje teknologjike dhe media të lëvizshme (p.sh. *thumb drives*, *USB flash drives* etj.). Sfida më e madhe në lidhje me përdorimin e tyre, është ndërgjegjësimi dhe paralajmërimi i personelit që i përdor ato. Shumica e sulmeve kibernetike kanë ndodhur nga gabimet njerëzore, për rrjedhojë "kërcënimet e brendshme" janë reale[8].

Mbrojtja kibernetike është vlerësuar në çdo moment dhe prioritetet e Ministrisë së Mbrojtjes janë të qarta, të cilat i përmendim më poshtë:

- zbatimi i masave të plota organizative dhe teknike të sigurisë kibernetike në *sistemet e komunikimit dhe të informacionit* (SKI);
- rritja e përgjegjësisë së strukturave të MM/FA-së për sigurinë kibernetik, zhvillimi i nivelit dhe aftësive të specialistëve të sigurisë kibernetike dhe të përdoruesve të SKI-ve;
- rritja e bashkëpunimit me strukturat përgjegjëse në nivel kombëtar dhe në kuadrin e NATO-s[9].

Të njëjtat masa vlejnë dhe për institucionet e tjera shtetërore e private në vendin tonë. Pra, asnjëherë mbrojtja kibernetike nuk duhet parë si e shkëputur nga një institucion në tjetrin. Ajo duhet të vlerësohet si një e tërë dhe të trajtohet me seriozitet në mënyrë që mos të biem prè e sulmeve, të cilat mund të shkaktojnë dëme të parikuperueshme dhe me kosto të lartë.

5. Përfundime

Krimi kibernetik tashmë është një shqetësim i vazhdueshëm dhe që ka përfshirë gjithë globin. Në shumicën e rasteve mbrojtja kibernetike trajtohet e shkëputur, duke dhënë edhe zgjidhje të veçanta për probleme të shkëputura. Elementi siguri, qoftë ky në kuptimin tradicional të fjalës apo në atë kibernetik ose virtual duhet vendosur e ideuar në themelin e strukturës të cilën duam të mbrojmë. Për këtë nevojitet një strategji gjithëpërfshirëse. Nëse strategjia do të përfshijë dhe sektorin shtetëror dhe atë privat. Në këtë mënyrë do kemi asetet dhe të përcaktojmë se cilat janë rreziqet që na kanosen, cilat janë zhvillimet që në nuk i dimë akoma, dhe sa është raporti dhe efekti përfundimtar i këtyre rreziqeve që na kanosen. Duke bërë një analizë të tillë gjithëpërfshirëse, bashkë

[7] Ministria e Mbrojtjes, *Strategjia për Mbrojtjen Kibernetike* 2018-2020, f. 4
[8] Po aty, f. 11.
[9] Po aty, f. 8.

sektori shtetëror dhe ai privat, atëherë do jemi në gjendje të marrim masat në kohë dhe të parandalojmë rrezikun.

Me rritjen e shkallës së zhvillimit dhe shkëmbimit të informacionit është rritur dhe rreziku i sulmeve kibernetike. Nëse nga njëra anë kemi ata grupe njerëzish që planifikojnë sulmin nëpërmjet komandave të ndryshme kompjuterike, nga ana tjetër duhet të kemi njerëz po kaq të përgatitur që të pengojnë sulme të tilla. Kjo kërkon një bashkëpunim institucional, kombëtar, po ashtu dhe ndërkombëtar.

Bibliografia

1. *Kushtetuta e Shqipërisë*, Tiranë 1998, (e ndryshuar).
2. Kolë Krasniqi, *Terrorizmi Ndërkombëtar* , Botim i dytë, Prishtinë, 2010.
3. Jimmy Sproles, Will Byars, "Examples of Cyber Terrorism", Paper for Computer Ethics Class, 1998.
4. Luan Hoxha, *Lufta Informative*, Kolegji i Mbrojtjes, Akademia e Forcave të Armatosura të RSH.
5. US Department of Justice, Computer Crime and Intellectual Property Section (CCIPS), CCIPS Documents And Reports, https://www.justice.gov/criminal-ccips/ccips-documents-and-reports
6. Adam Gorlick, "Obama at Stanford: Industry, government must cooperate on cybersecurity", February 13, 2015, President Barack Obama addressing the White House Summit on Cybersecurity and Consumer Protection at Stanford
http://news.stanford.edu/ne%C3%ABs/2015/february/summit-main-obama-021315.html
7. https://www.nato.int/docu/review/2011/11-september/Cyber-Threads/AL/index.htm
8. Ministria e Mbrojtjes, Strategjia për Mbrojtjen Kibernetike 2018-2020.


AKADEMIA E SIGURISË
1971


AKADEMIA E SIGURISË
AS
1975

~ Sesioni II ~

Hetime profesionale të krimeve kibernetike

Krimi kibernetik dhe sistemi i sigurisë

■**MSc. Marco SARACCHI**[1]
Ekspert për hetimet kibernetike/të inteligjencës
marcosaracchi@libero.it

■**Dr. Bajram Ibraj**[2]
Drejtor i komanduar/Rektor Kolegji ISPE
bajramibraj@yahoo.com

■**MSc. Patrizio Mazzacane**[3]
Ekspert për sigurinë kibernetike
patrizio.mazzacane@gmail.com

Abstrakt

Abstrakt

Procesi procedural (vademecum operativo) për luftën kundër krimit kibernetik sipas standardeve europiane GDPR EU 679/2016, është sipas standardeve ndërkombëtare: ISO 27002:2007, ISO 27001:2005, NERC, NIST, BSI IT, ISO 15408. Termi krim informatik, identifikon një aktivitet kriminal të karakterizuar nga përdorimi i teknologjisë informatike si pajisjeve fizike dhe ato virtuale (programet), për kryerjen e një ose më shumë krimeve. Bëhet fjalë për një aktivitet kriminal që përfshin strukturën e teknologjisë së informacionit, përfshirë aksesin e paligjshëm (të paautorizuar), përgjimin (me pajisje teknike të transmetimeve së të dhënave informatike jopublike, kundër, nga apo brenda të një sistemi informativ), ndërhyrje ndaj të dhënave (dëmtim, fshirje, ndryshim, alternim apo suprimim i të dhënave informatike), sisteme ndërhyrjeje (ndërhyrje me funksionin e një sistemi informatik përmes transmetimit, dëmtimit, fshirjes, shkatërrimit, alternimit apo suprimimit të të dhënave informatike), vjedhja e identitetit dhe mashtrimi elektronik.

Fjalëkyçe:

krimi kibernetik, ekzaminimi kompjuterik, "hacking", informacione "web", përputhshmëria IT, "phishing".

1. Hyrje

Tipologjitë kryesore të kryera përmes përdorimit të hapësirës kibernetike, janë si në vijim: vjedhje identiteti, pastrimi elektronik i të ardhurave të paligjshme, terrorizmi kibernetik, mashtrime në platformat *E-commerce,* klonim i kartave bankare, shpifje *online*, dialer (numërtim telefonik me vlerë të shtuar), dhunimi i llogarisë, aksesi abuziv në email, aksesi abuziv në sistemet informatike, transferta bankare në destinacion të panjohur (*Phishing*), falsifikimi në dokumentet informatike, dëmtim i të dhënave dhe programeve, sabotimi informatik, akses abuziv tek masat e sigurisë të sistemit, përgjim i paautorizuar, riprodhim dhe tregtim i programeve të mbrojtura, riprodhim dhe tregtim i paautorizuar i imazheve, videove dhe audiove, alterim i paautorizuar i të dhënave apo programeve, spiunazh informativ i kuptuar si zbulim informacioni i lidhur me sekrete industriale apo tregtare, përdorim i paautorizuar i një kompjuteri apo një rrjeti kompjuterik, përdorimi i paautorizuar i një programi kompjuterik i mbrojtur, tregtia e kodeve të aksesit i përfituar në mënyrë ilegale, shpërndarja e viruseve, programeve të

[1] Marco Saracchi, Itali, Liceo Scientifico Tecnologico dhe Master Shkencor në Kriminologji. Ekspert i pajisur me licence për hetimet kibernetike dhe të inteligjencës. Zyrtar i Mbrojtjes së të Dhënave GDPR EU/679 & Detektiv Ndërkombëtar. Bashkëadministrator dhe ortak i kompanisë „RADAR" SHPK, në Tiranë për: siguri kibernetike, Web intelligence, investigime, teknologji per siguri, computer forencic, çdo operacion të ngjashëm të lejuar nga legjislacioni shqiptar.

[2] Dr. Drejtues (Gjeneral Major) Bajram Ibraj, Shkenca Politike dhe Marrëdhënie Ndërkombëtare. Kolegji ISPE – Studime Evropiane për të Ardhme Evropiane, Prishtinë, Kosovë. Drejtor i komanduar/Rektor Kolegji ISPE. Pedagog- E Drejta Penale e Përgjithshme në Kolegjin Universitar të Biznesit, Tiranë.Drejtor i Sigurisë Fizike në Intesa Sanpaolo Bank Albania.

[3] Patrizio Mazzacane, Shkolla e lartë dhe Master shkencor në Administrim dhe Biznes.Bashkëadministrator dhe ortak i kompanisë „RADAR"SHPK, në Tiranë për: siguri kibernetike, Web intelligence, investigime, teknologji per siguri, computer forencic, çdo operacion të ngjashëm të lejuar nga legjislacioni shqiptar.

këqija, *keylogger and cryptolocker*. Zëvendësimi i identitetit me profile të rreme në rrjetet kryesore (es. *Facebook, Instagram, Linkedin*), sabotim informatik me qëllim zhvatjen për restaurimin e sistemit, në ngarkim dhe në shkarkim së të dhënave ilegale, personale dhe/ose të palejuara nga ligji, *E-commerce* ilegal (p.sh. material pedopornografik, armë, drogë, karta bankare të klonuara, valuta-*crypto*, pasaporta false, patenta false etj.), pedopornografi, bulizmi kibernetik, përndjekja kibernetike, *spam*, etj.[4]

2. Krimet kibernetike kryesore

1. Sulme ndaj infrastrukturave kritike: ky lloj krimi informatik kryhet deri në fund, për të dëmtuar sistemet e mëdha informatike të ndërmarrjeve private dhe shtetërore.

2. Terrorizmi kibernetik: sipas përkufizimit të FBI-së, terrorizmi kibernetik është një sulm i paramenduar me sfond politik nga grupe lokale apo agjentë klandestinë, kundër mjeteve të informimit, të dhënave dhe programeve të informatizuar, që përkthehet si dhunë kundër objektivave të paaftë për të luftuar.

3. Të drejtat e autorit: nuk është gjë tjetër veçse mbrojtja e të dhënave të autorit, në fakt zhvillimi i teknologjisë dhe futja e internetit në shekullin e XX, futja e riprodhuesve dhe në veçanti të kompjuterit dhe rrjetit të internetit, ka zbehur një nga themelet e të drejtës së autorit në sensin klasik, domethënë që kostoja dhe vështirësia për të riprodhuar dhe për të përhapur në territor shfaqjet opera, i trajtohej nga korporata e redaktorëve, SIAE. Ajo ka bërë të vështirë tutelën e të drejtës së autorit në formën tradicionale dhe ka krijuar hapësira të reja për autorët.

4. Mashtrimi kompjuterik: mashtrimi kompjuterik që konsiston në shndërrimin e përpunimit së të dhënave, me qëllimin për të nxjerrë përfitim të padrejtë.

5. Dhunimi i të dhënave personale: konsiston në sigurimin padrejtësisht së të dhënave personale apo delikate. Në fakt, rrjeti është në gjendje të ofrojë një gamë të gjerë informacioni e shërbimesh, po në të njëjtën kohë, mund të përbëjë një vend të rrezikshëm për privatësinë tonë, sepse vetë mjeti, nuk është konceptuar për të shkëmbyer dhe trajtuar të dhëna delikate.

6. "Spamming": është një nga fenomenet më të bezdisshme të internetit, i cili konsiston në dërgimin e të njëjtit mesazh, email, me përmbajtje publicistike, qindra dhe mijëra personave, duke u justifikuar se posta elektronike është falas. Përveç dhunimit të standardit, për përdorimin e rrjetit dhe mbingopjen e tij me mesazhe të pavlera, *spamming* në Itali shkel ligjin për privatësinë e personave dhe të subjekteve të tjerë, duke marrë parasysh trajtimin e të dhënave personale. Në një kontekst të ngjashëm, mbajtja e anonimatit, rezulton shpesh e vështirë, dhe me riprodhimin e llogarive *online* dhe spostimit të ndërmarrjeve në internet, rezulton më e thjeshtë për keqbërësit të hyjnë në informacionet tona të rezervuara.

7. Pajisjet spiune: bëhet fjalë për programe të cilat pasi instalohen, shpeshherë në mënyrë mashtruese në kompjuterët personale të viktimës, sigurohet që të dërgojë të

[4] Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.
Warren G. Kruse, Jay G. Heiser (2002). *Computer forensics: incident response essentials*. Addison-Wesley. p. 392. ISBN 0-201-70719-5.
- Halder, D., & Jaishankar, K. (2011) Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9.

dhëna personale (faqe të vizituara, llogaritë e postës elektronike, shijet, etj.) tek ndërmarrje që për rrjedhojë do t'i ripërpunojnë dhe rishesin[5].

Ekziston edhe një metodë që quhet *social engineering*, nëpërmjet së cilës, mashtruesit arrijnë të marrin informacione personale tek viktimat përmes teknikave të ndryshme psikologjike; bëhet fjalë për një lloj manipulimi që i bën përdoruesit të lëshojnë spontanisht të dhënat e veta konfidenciale.

3. Veçoritë e ndryshme të "Dark Web", sipas vendeve të ndryshme, nga "Trend Micro"[6]

Një fenomen negativ që po tjetërson shoqërinë me përhapjen masive tek të rinjtë e rrjeteve sociale, forumeve dhe *chat*-eve është ngacmimi [bulizmi] kibernetik, një formë e ndryshme nga ngacmimi [bulizmi] tradicional në jetën reale, përdorimi i mjeteve elektronike (*mezzi elettronici*) i jep ngacmimit kibernetik disa karakteristika përkatëse:

8. Anonimiteti i abuzuesit: në realitet ky anonimat është iluziv - çdo komunikim elektronik lë pothuajse gjithmonë gjurmë. Ndërkohë për viktimën është e vështirë të arrijë vetë tek abuzuesit përkatës; për më tepër përveç faktit të anonimatit te ngacmuesi kibernetik, gjëra të pahijshme tek llogaria e viktimës (shpeshherë të përshkruara në mënyrë publike, të tjerat në mënyrë vetëm të dukshme por të pagjurmueshme) mund të tjetërsohen nga një numër i madh njerëzish.

9. Vështirësi për të gjetur: nëse *cyberbullying* zhvillohet përmes SMS-ve, mesazheve të menjëhershme ose *email*, ose në një forum privat në internet, për shembull, është një

[5] FTC Report (2005). "[1]".
SPYWARE ""Archived copy" (PDF). Archived from the original (PDF) on November 1, 2013. Retrieved 2016-02-05."
Basil Cupa, Trojan Horse Resurrected: On the Legality of the Use of Government Spyware (Govware), LISS 2013, pp. 419–428.
FAQ – Häufig gestellte Fragen Archived May 6, 2013, at the Wayback Machine.
"Spam". *Merriam-Webster Dictionary* (definition & more). 2012-08-31. Retrieved 2013-07-05.
- Monty Python (2009-01-13), *Spam - Monty Python's The Flying Circus*, retrieved 2017-01-11.
"The Definition of Spam". *The Spamhaus Project*. Retrieved 2013-09-03.
"Developer Policy Center – Intellectual Property, Deception, and Spam". *play.google.com*. Retrieved 2016-05-01.
"Spam". *Merriam-Webster Dictionary* (definition & more). 2012-08-31. Retrieved 2013-07-05.

[6] https://www.lettera43.it/it/articoli/scienza-e-tech/2016/03/05/dark-web-mappa-del-crimine-informatico/163911/.

vështirësi për t'i gjetur dhe për t'i korrigjuar ato.

10. Dobësimi i etikës: dhe dy karakteristika të mëparshme, të kombinuara me aftësinë për të qenë "një person tjetër" *online* (shih RPGs), mund të dobësojë dyshime etike: njerëzit shpesh bëjnë dhe thonë gjëra në internet që ata nuk do të bënin ose nuk do të thoshin në jetën reale.

11. Mungesa e afateve hapësirë-kohë: Ndërsa ngacmimi tradicional zakonisht ndodh në vende dhe në kohë të caktuara (për shembull, në kontekstin e shkollës), *cyberbullying* përfshin viktimën çdo herë që të lidheni në medium elektronik që përdoret nga *cyberbully*. Ashtu si në ngacmimet tradicionale, megjithatë, dhunuesi dëshiron të synojë ata që konsiderohen "të ndryshëm", p.sh. për paraqitjen, droje, orientimit seksual apo politik, veshje, etj. Rezultat i ngacmimit të tillë është erozioni i çdo vullneti të bashkimit dhe izolimi konsekuent, duke nënkuptuar dëme psikologjike, të tilla si depresioni ose, më keq, dhe idetë e qëllimet vetëvrasëse[7].

4. Konsiderata

Në bazë të përvojave tona të trajtuara deri më tani, janë llojet kryesore të krimeve kompjuterike që kryhen në nivel ndërkombëtar. Ky lloj i krimit ka karakteristikën për të dëmtuar personin fizik, por në realitet kjo ndodh në fund të një cikli që e sheh si objektiv kryesor infrastrukturën dhe kompanitë. Prandaj ka krime që u drejtohen drejtpërsëdrejti individëve, ndërkohë që krime të tjera u drejtohen shoqërive që administrojnë kompani, grupe njerëzish dhe interesat e njerëzve. Prandaj, pavarësisht krimeve kundër kompanive, ato ndikojnë - në fund të fundit – te njerëzit.

Kjo është arsyeja pse veprimi është i nevojshëm, para së gjithash me procedurat e sigurisë dhe protokolleve të sigurisë kibernetike të organizuara mirë dhe të strukturuara në mënyrë specifike ne avantazh të korporatave dhe kompanive që operojnë në sektorët kryesorë.

Ndihemi të detyruar të japim një kontribut të rëndësishëm, në këtë rast, në ruajtjen e mënyrave me të cilat ruajmë dhe mbrojmë të dhënat, në vend që të përshkruajmë në detaje karakteristikat e një sulmi kibernetik dhe karakteristikat e *cyber*-krimeve. Këto janë arsyet që na bindën të hartojmë një protokoll të sigurisë kompjuterike menjëherë të përdorshëm pavarësisht nga sektorët profesionistë dhe privatë në të cilët përdoret.

Ne mendojmë, se është e rëndësishme të kemi mjetet për të luftuar krimin kibernetik, dhe këtu, na lejoni t'u japim të gjithë pjesëmarrësve një protokoll standard dhe shumë efektiv, për sigurinë e infrastrukturave informatike. Protokolli është në përputhje me standardet e rregullores evropiane 679/2016 GDPR, me dispozitat e Garantit të Privatësisë në kontekstin europian dhe ndërkombëtar, dhe me standardet kryesore të përdorura nga qeveritë, për të mbrojtur rrjetet kompjuterike në përdorim.

[7] consultato il 12 luglio 2017.
- Sheri Bauman, Ph.D., *Cyberbullying: a Virtual Menace* (PDF), in *University of Arizona*(archiviato dall'url originale il 28 febbraio 2016).
- Parry Aftab, What is Cyberubullying Exactly, in stopcyberbullying.org.
- Collana Genuensis, *Bullismo & Co*, Youcanprint, 2015, ISBN 9788891194503.
- *Indagine conoscitiva sulla condizione dell'infanzia e dell'adolescenza in Italia 2011*(PDF), su *azzurro.it*, 2011. URL.
- Cyberbullismo - Polizia di Stato Archiviato il 15 aprile 2013 in Internet Archive.
Facebook e codice penale, quando i leoni da tastiera miagolano, su *ilfattoquotidiano.it*. URL consultato il 5 marzo 2018.

Ky dokument përshkruan hapat themelore procedurale, në fushën e sigurisë kompjuterike, duke ilustruar dispozitat ekzistuese dhe rregullat e sjelljes që duhet të ndiqen në menaxhimin e duhur dhe trajtimin e informacionit të klasifikuar në kuadër të kompanive dhe të shoqërive. Këto janë procedurat që përdor si DPO *Data Protection Officer* (*person kontakti për mbrojtjen e të dhënave*) me qëllim mbrojtjen e të dhënave. Si fillim duhet të pajiseni me një organizatë të sigurisë, në thelb një organ mbikëqyrësi i brendshëm, i cili duhet të përshtatet për kategoritë e informacionit të klasifikuar që duhet të trajtohet si edhe me madhësinë dhe karakteristikat e infrastrukturës dhe menaxhimit të kompanisë objekt ndërhyrje. Ligjet në drejtim të mbrojtjes së të drejtës për privatësi i japin përfaqësuesit ligjor të ndonjë kompanie përgjegjësinë për mbrojtjen dhe ruajtjen e informacionit të përpunuar, në nivel qendror dhe periferik.

1. Përfaqësuesi ligjor mund t'i delegojë personave me kërkesa specifike, persona të cilët quhen *persona kontakti* dhe *zyrtarët për mbrojtjen e të dhënave (DPO)* dhe delegohen në ushtrimin e detyrave dhe funksioneve që lidhen me administrimin e sigurisë dhe rrezikut.

2. *Zyrtari për mbrojtjen e të dhënave* (DPO), përkatësisht personi i kontaktit për mbrojtjen e të dhënave, drejton, koordinon dhe kontrollon të gjitha aktivitetet që kanë të bëjnë me mbrojtjen e informacionit, dokumenteve dhe materialeve të klasifikuar dhe/ose konfidencial, të trajtuara brenda kompanisë.

Ai pastaj i jep përfaqësuesit ligjor këshilla për interpretimin dhe zbatimin e ligjeve aktuale dhe standardeve të brendshme procedurale, duke formuluar udhëzime për miratimin e masave të nevojshme për të mbrojtur të dhënat e kompanisë.

3. Pranë secilës prej selive operacionale të kompanisë, caktohet një oficer i caktuar i sigurisë, i cili është një *Risk Officer* në "varësinë" e DPO-së.

Aktivitetet e shoqërisë, në ndjekjen e qëllimeve dhe statuteve të shoqërisë, kryejnë një sërë detyrash sipas udhëzimeve dhe procedurave të hartuara nga ODV-të, të cilat sipas makro zonave që i përkasin, do të menaxhohen, organizohen dhe zbatohen sipas metodave dhe strukturave të ndryshme që kërkojnë monitorim dhe veprime parandaluese të ndryshme. Në varësi të llojit të aktivitetit të kryer, llojit të klientelës të cilës i është adresuar, llojit së të dhënave dhe informacionit të përpunuar, sistemet dhe infrastrukturat duhet të jenë gjithmonë nën kontrollin e drejtpërdrejtë dhe verifikimin e vazhdueshëm të ODV dhe DPO[8].

Më poshtë është një përshkrim i terminologjisë që normalisht përdoret për standardet procedurale:

Informacione të klasifikuara: informacion i klasifikuara është çdo informacion, akt, veprimtari, dokumentacion, material ose çdo gjë tjetër, për të cilin është caktuar një klasifikim konfidencialiteti.

Dokument i klasifikuar: dokument i klasifikuar është paraqitja grafike, fotokinematografike, elektromagnetike, informatike ose në çdo formë tjetër të informacionit të klasifikuar.

Materiale të klasifikuara: materiale të klasifikuara janë çdo objekt, prototip, komponent elektro-mekanik, pajisje, armë, pajisje, softuer operativ, materiale për infrastrukturën e rrjetit dhe teknologjitë së informacionit, konfidencialiteti i të cilave duhet të garantohet për shkak se është garantues i privatësisë së shoqërisë.

Informacione jo të klasifikuara të kontrolluara: informacione jo të klasifikuara të

[8] DPO:https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en, Qui di seguito riporto una descrizione della terminologia di norma utilizzata per gli standard procedurali.

kontrolluara, janë informacione që kërkojnë masa minimale të mbrojtjes, qasja e të cilave lejohet vetëm për ata që kanë nevojë t'i trajtojnë ato.

Shkelje: shkelje janë shkelje të sigurisë pas veprimeve ose mosveprimeve në kundërshtim me një dispozitë mbi mbrojtjen e informacionit të klasifikuar, që mund të dëmtojë vetë informacionin.

Vënie në rrezik: vënie në rrezik, kemi kur informacioni është aksesuar pjesërisht ose tërësisht nga persona të paautorizuar ose me nivel të pamjaftueshëm në aspektin e sigurisë dhe kur informacioni është kompromentuar.

Kujtojmë se, në sferën ndërkombëtare, këto janë klasifikimet për fushat, aktivitetet e të cilave përfshijnë ekzekutimin e punëve, furnizimin e mallrave dhe shërbimeve, ndërtime, studime dhe projekte, të cilave u atribuohet një shkallë e lartë konfidencialiteti, si dhe pjesëmarrjen në tendera, që kanë për qëllim dhënien e kontratave të klasifikuara për të cilat kërkohen kualifikime të veçanta për qëllime sigurie[9].

5. Mbrojtja kibernetike dhe, siguria e sistemeve dhe rrjeteve objektive

Kjo veprimtari është një përpjekje për të krijuar një programim të shpërndarë që ka për qëllim verifikimin e sigurisë informatike të sistemeve dhe rrjeteve për të mbrojtur sigurinë si dhe imazhin e vetë kompanisë.

5.1 Organizimi

Verifikimet do të bëhen çdo muaj, në baza vjetore do të jenë përafërsisht 12 vlerësime tekniko-informatike dhe të sistemeve të cilat do të përdoren edhe për monitorimin e teknologjive inovative në të gjithë sektorët e ndërlidhur me përdorimin e sistemeve dhe platformave të TIK-ut në mënyrë që të identifikohen profile eventuale të ndjeshme.

Vlerësimet e bëra me të gjithë përgjegjësit e infrastrukturës kritike, do të ndahen përmes platformave të posaçme institucionale dhe/ose të dedikuara ekzistuese duke realizuar n.12 audite me DPO Personi i kontaktit për mbrojtjen e të dhënave personale dhe përgjegjësinë e IT-së.

Çdo përdorues do të konsiderohet i tillë, vetëm për sa i përket zotërimit të specifikave të kredencialeve të autenticitetit dhe duhet të përgatisë çdo javë për përgjegjësinë e IT-së, një raport që përmban masat e përdorura dhe një përshkrim, të aktiviteteve të kryera sipas procedurave.

5.2 Verifikime inspektuese

Verifikimet inspektuese mujore, kanë qëllimin të forcojnë aftësitë e sigurisë kibernetike, duke zhvilluar procedura për monitorimin e volumit të trafikut dhe, për ndërlidhjen e ngjarjeve, me qëllim zbulimin e menjëhershëm të anomalive të lidhura me gjendje kërcënuese. Verifikimet inspektuese parashikojnë zbatimin e operativitetit të strukturave të caktuara për mbrojtjen e hapësirës kibernetike, duke predispozuar asete, të identifikuara në linjat e komandimit, përmes përgatitjes, mbrojtjes dhe mbështetjes së tyre, duke përcaktuar standarde specifike për vlerësimin dhe formatin e komunikimit të analizave të brendshme të lidhura me infrastrukturën e menaxhuar, si

[9] https://www.sicurezzanazionale.gov.it/sisr.nsf/cosa-facciamo/tutela-delle-informazioni/segreto-di-stato.html.

dhe ndjeshmërinë e identifikuar.

5.3 Fazat procedurale

Të tre fazat procedurale janë të strukturuara, në mënyrë që të garantojnë një sinergji korrekte dhe efektive, nëpërmjet instrumenteve të analizës, zbatimit të procedurave dhe mbrojtjes së të gjithë infrastrukturës informatike.

1. ATIP (*Konstatim teknik informatik paraprak*), - ka për qëllim të përcaktojë kërkesat minimale të mbrojtjes kibernetike në aspektin instrumental dhe procedural, për mbrojtjen e infrastrukturës, së të dhënave të internetit dhe për menaxhimin e të dhënave të ndjeshme.

2. POPC (*Plan operativ për mbrojtjen kibernetike*), - përcakton kriteret për të cilat çdo tremujor kryhen operacionet teknike të verifikimit, mirëmbajtjes dhe përditësimit së të gjitha sistemeve si të brendshëm, dhe të jashtëm, ato të internetit me të dhënat mbi trafikun në hyrje dhe dalje, gjithashtu edhe sistemet e autenticitetit dhe dobësitë e tyre.

3. PODI (*Procedura operative e mbrojtjes informatike*), - grumbullon të gjitha teknikat e mbrojtjes që përdoren për ruajtjen e sigurisë dhe parandalimin e kërcënimeve[10].

*5.4 Sekuenca në ATIP (*Konstatim teknik informatik paraprak*)* [11]

Analiza: parimet e autentifikimit [vërtetimit]; fjalëkalimi; sfida - përgjigja (mbrojtja kundër sulmeve të sistemit); vërtetimi *client/server;* shërbimet e vërtetimit të përdoruesve *remot*; siguria në aksesin në Web (SSL); siguria e lidhje (SSH); siguria në *email* (PGP, S/MIME); pronësia e protokolleve të vërtetimit.

*5.5 Sekuenca në POPC (*Plan operativ për mbrojtjen kibernetike*)*

Analiza dhe verifikimi: *software*; sistemet e informacionit; ndërfaqet e përdoruesit; përpunimi i imazhit; përpunimi i medieve audio-video; metodat e autenticitetit të sistemit; *firewall*; server; cenueshmëria e sistemit; testimi i depërtimit në rrjet; trafiku i të dhënave në internet, shërbimet dhe lidhjet; lidhje me rrjetet sociale; mospërputhja e shërbimeve të ofruara nga ofruesi në *Web*; informacioni i disponueshëm për publikun; identifikimi i sistemeve/rrjeteve/shërbimeve të ekspozuara nga jashtë; informacion që del nga kompania dhe përfundon në motorët e kërkimit; informacion i ndjeshëm dhe menaxhimi sipas ligjeve në fuqi; përpunimi i të dhënave sipas normativave aktuale.

PODI, lista e procedurave operative të mbrojtjes informatike, është hartuar dhe strukturuar sipas udhëzimeve të përdorura për ndërtimin e aplikacioneve të sigurta në *Web*: garantimi i sigurisë nuk kërkon që përdoruesi të marrë vendime; kërkimi i një justifikimi komercial për të gjitha *input-et* dhe *output*-et e aplikacionit; të vendosësh në karantinë dhe vlerësimi i të gjitha *input*-eve që përfshijnë përmbajtjen e aplikacionit; kufizimi i mirëbesimit (tek sistemi dhe përdoruesit); kriptimi i të dhënave; sigurohuni që të gjitha bashkëveprimet të ndodhin në anën e serverit; të strukturosh në nivele sigurie; është më mirë të tregohet vetëm shërbimi dhe jo përbërësit e tij; aktivizimi i alarmeve.

Sa i përket sigurisë kompjuterike, mbrojtja parandaluese arrihet përmes masave tekniko-organizative dhe funksionale që synojnë të sigurojnë saktësinë e të dhënave

[10] https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf.

[11] https://www.businessinternational.it/Eventi/3820/Enterprise-Risk-Management-Meeting.

(integritetin), konfidencialitetin e të dhënave (kriptimin), qasjen fizike dhe/ose logjike vetëm për përdoruesit e autorizuar (vërtetimi), përdorimi i të gjitha shërbimeve të ofruara për ata përdorues në kohë dhe në mënyrën e parashikuar nga sistemi (disponueshmëria), dhe së fundi, mbrojtjen e sistemit nga sulmet e softuer *malware* për të garantuar kërkesat e mësipërme.

Mjetet e përdorura në PODI (*Procedura operative të mbrojtjes informatike procedurat*), - sipas standardeve ISO, - të zbatuara nga kompania jonë, janë të organizuara në 10 zona kontrolli:

1. *Politikat e sigurisë:* ofrojnë udhëzime për menaxhimin dhe mbështetjen për informacionin e sigurisë.

2. Siguria organizative: kontrolli i sigurisë së informacionit brenda kompanisë; të ruajë sigurinë dhe lehtësinë e proceseve të organizmit të informacioneve edhe kur ato aksesohen nga palë të treta; monitorojnë sigurinë e informacionit kur është dhënë përgjegjësia për përpunimin e informacionit.

3. *Kontrolli dhe klasifikimi i aseteve:* mbajnë mbrojtjen e strukturës organizative dhe sigurojnë që struktura e informacionit të ketë një nivel të duhur mbrojtjeje.

4. *Siguria e personelit:* zvogëlimi i rreziqeve nga gabimet, vjedhjet, mashtrimet apo abuzimet nga operatorët; të sigurojë që përdoruesit janë në dijeni të kërcënimeve dhe shqetësimeve të mundshme në lidhje me sigurinë e informacionit dhe janë të pajisur për të mbështetur politikën e sigurisë së kompanisë gjatë punës së tyre normale; për të minimizuar dëmet nga ngjarjet dhe mosfunksionimet e sigurisë dhe për të mësuar nga ngjarje të tilla.

5. *Siguria fizike dhe e ambienteve:* parandalimi i hyrjeve, dëmtimi dhe ndërhyrja e personave të paautorizuar brenda rrjedhës së informacionit të biznesit; të parandalojë humbjen, dëmtimin ose strukturën e sistemit dhe ndërprerjen e aktiviteteve ekonomike; për të parandaluar manipulimin ose vjedhjen e informacionit.

6. *Menaxhimi i komunikimit dhe operacioneve:* të sigurojë funksionimin e duhur dhe lehtësinë e përpunimit të informacionit; minimizimi i rrezikut dhe dështimeve të sistemit; të mbrojë integritetin e softuerit dhe të informacionit; të ruajë integritetin dhe vlefshmërinë e proceseve të përpunimit të informacionit dhe komunikimit; garanton mbrojtjen e informacionit në rrjet dhe mbrojtjen e infrastrukturave mbështetëse; të parandalojë dëmtimin e aseteve dhe ndërprerjet e veprimtarisë ekonomike; parandalon humbjen, modifikimin ose abuzimin e informacionit të shkëmbyer midis organizatave.

7. Kontrolli i qasjeve: për të kontrolluar qasjen në informacione; për të parandaluar qasjen e paautorizuar në sistemet e informacionit; për të përcaktuar mbrojtjen e shërbimeve të rrjetit; për të parandaluar hyrjen e paautorizuar në kompjuter; për të zbuluar aktivitete të paautorizuara; për të konstatuar sigurinë e informacionit kur përdoren telerrjetet dhe rrjetet celulare.

8. *Zhvillimi dhe mirëmbajtja e sistemit:* të garantojë që siguria është ndërtuar brenda operacioneve të sistemit; për të parandaluar humbjen, modifikimin ose keqpërdorimin e të dhënave të përdoruesve brenda sistemeve të aplikimit; për të mbrojtur konfidencialitetin, origjinalitetin dhe integritetin e informacionit; për të siguruar që aktivitetet e projektit dhe aktivitetet mbështetëse të zhvillohen në mënyrë të sigurt; të ruajë sigurinë e softuerit dhe të dhënave të sistemit.

9. *Menaxhimi i vazhdimësisë operacionale:* ndërprerjet dhe neutralizimi i ndërprerjeve ndaj aktiviteteve ekonomike dhe proceseve kritike të biznesit, nga efektet e defekteve.

10. *Përshtatshmëria:* shmangia e mosrespektimit të ligjeve civile, penale dhe çfarëdo kriteri lidhur me sigurinë;

Fazat operative të mësipërme janë në përputhje me udhëzimet e siguruara nga "Sistemi i menaxhimit të sigurisë në teknologjitë e informacionit" (*Information Security Management System*, ISMS)[12].

Duke konsideruar përvojat tona dhe rastet në të cilat kemi punuar, ne rekomandojmë ndërmarrjen e hapave të mëposhtëm për të garantuar për një shkallë më të lartë të sigurisë duke u mbrojtur nga krimet kibernetike:

1. *Antivirus:* kontrolli i përditësimeve dhe funksioneve të skanimit në kohë reale.

2. *Antispyware:* kontrolli i përditësimeve dhe funksioneve të skanimit në kohë reale.

3. *Firewall:* verifikimi i instalimit dhe funksionimit të duhur sipas procedurave të kontrollit të qasjes duke verifikuar të gjithë trafikun që kalon përmes tij.

4. *Nënshkrimet digjitale dhe kriptografia:* verifikimi i mekanizmave për të mbrojtur dokumentet dhe të dhënat e ndjeshme nga qasja e paautorizuar.

5. "*Backup":* verifikimi i rikuperimit korrekt së të dhënave dhe ruajtja e tyre sipas kohës dhe metodave të përcaktuara.

6. *Sistemi i zbulimit të ndërhyrjeve (IDS):* verifikimi i funksionalitetit të sistemeve softuerike dhe *hardware* për të identifikuar qasjen e paautorizuar në kompjuterë.

7. *Rrjeti i zbulimit të ndërhyrjeve në sistem (NIDS):* verifikimi i teknologjisë së informacionit, *software* apo *hardware*, i dedikuar për të analizuar trafikun e një ose më shumë segmenteve të një LAN-i, me qëllim të zbulimit të anomalive në rrjedhat e ndërhyrjeve të mundshme kompjuterike.

8. *Sistemi i autentifikimit [vërtetimit]:* verifikimi dhe testimi i softuerit për vërtetim të sigurt.

Ajo që u theksua në prezantimin e mësipërm, korrespondon pjesërisht me atë që duhet përdorur. Ndërkohë, shumë teknika dhe standarde procedurale janë lënë jashtë qëllimisht për të mbrojtur më mirë integritetin e procedurave të zbatuara normalisht nga i nënshkruari për të mbrojtur një sistem të veçantë që siguron mbrojtjen e përmbajtjes dhe proceset në avantazh të klientit dhe në dëm të hakerëve dhe kriminelëve kibernetikë.

Jemi kufizuar në trajtimin e një mënyre të përgjithshme dhe joshteruese, me çështjen e krimit kibernetik dhe procedurave themelore, për mbrojtjen e sigurisë dhe privatësisë përmes përdorimit të procedurave të IT-së, për mbrojtjen kibernetike.

Ekziston një mënyrë e zhytur, ajo e *deep web*, që është grupi i burimeve të informacionit të *www* (*world wide web*) që nuk indeksohet nga motorët e kërkimit normal.

Për të shpjeguar sasinë e të dhënave të pranishme në *deep web*, ne përdorim metaforën *iceberg*, ku pjesa mbi ujë i korrespondon të gjitha faqeve të internetit të indeksuar nga motorët e kërkimit: të ashtuquajturit *web* të aksesueshëm; ndërsa pjesa thelbësore e ajsbergut është zhytur dhe i korrespondon *deep web*-it.

[12] De Santis, Giulia; Lahmadi, Abdelkader; Francois, Jerome; Festor, Olivier. "Modeling of IP scanning activities with Hidden Markov Models: Darknet case study". *IEEE.ORG*. IEEE. Retrieved 16 April 2018.|1|1.
Wood, Jessica (2010). "The Darknet: A Digital Copyright Revolution" (PDF). *Richmond Journal of Law and Technology*. 16 (4): 15–17. Retrieved 25 October 2011.
Mansfield-Devine, Steve (December 2009). "Darknets". *Computer Fraud & Security*. 2009(12): 4–6. doi:10.1016/S1361-3723(09)70150-2.
Miller, Tessa (10 January 2014). "How Can I Stay Anonymous with Tor?". *Life Hacker*. Retrieved 7 June 2015.

Sipas një hulumtimi mbi madhësinë e rrjetit të kryer në vitin 2000 nga *Bright Planet*, një organizatë në SHBA, *web*-i përbëhet nga mbi 550 miliardë dokumente dhe 18 milionë GB, ndërsa indekset *Google* vetëm 2 miliardë, ose më pak se një për qind.

Kryesisht merremi me aktivitete hetuese në internet, ose *web intelligence*. Nga këtu kanë origjinën krime botërore dhe përmes softuerëve të anonimitetit dhe dinamikës teknologjike, ku nga shumë komplekse janë kryer shumë lloje krimesh, si tregtia e armëve, riprodhimi i dokumenteve të rreme si karta identiteti dhe pasaporta, tregtimi i kartave të kreditit të klonuara, shitja e drogës, mund të bëhen vrasje në internet, etj., por mbi të gjitha mënyra e pagesës është anonime: mund të paguani përmes një *Cryptovalute* - për shembull *Bitcoin*[13].

6. Bashkëpunimi ndërkombëtar

Thelbësore për punën e shërbimit policor, si dhe shërbimit të postës dhe komunikimit është pjesëmarrja në forume të rëndësishme ndërkombëtare. Kontaktet dhe shkëmbimet e informacionit me bashkëbiseduesit ndërkombëtarë janë një element themelor në aspektin e efektivitetit operacional.

Interneti nuk ka një territor të vetëm, por veprimet kriminale mund të kryhen nga e gjithë bota. Duke pasur parasysh këtë, është thelbësore që të zgjerohet rrjeti i kontakteve me policinë e vendeve te tjera për një shkëmbim të frytshëm me kolegët për çështje të përbashkëta dhe për të siguruar një shkëmbim të vazhdueshëm të informacionit në fazën operacionale, me përditësimin e vazhdueshëm të teknikave hetimore dhe inovacioneve teknologjike.

Një rol aktiv në diskutimet për çështje e hetimit të temave politiko-hetuese është bërë me pjesëmarrjen e nëngrupit *High Tech Crime* të G8 dhe Komisionit për Politikën e Informatikës dhe Komunikimeve (ICCP) të Organizatës për Bashkëpunim Ekonomik

---

[13] Hamilton, Nigel. "The Mechanics of a Deep Net Metasearch Engine". CiteSeerX 10.1.1.90.5847./
Devine, Jane; Egger-Sider, Francine (July 2004). "Beyond google: the invisible web in the academic library". *The Journal of Academic Librarianship*. 30 (4): 265–269. doi:10.1016/j.acalib.2004.04.010. Retrieved 2014-02-06.
Raghavan, Sriram; Garcia-Molina, Hector (11–14 September 2001). "Crawling the Hidden Web". *27th International Conference on Very Large Data Bases*.
1. "deep Web". *WhatIs.com*. Retrieved 20 June 2018.
2. "Surface Web". *Computer Hope*. Retrieved 20 June 2018.
3. Wright, Alex (2009-02-22). "Exploring a 'Deep Web' That Google Can't Grasp". *The New York Times*. Retrieved 2009-02-23.
Andy Greenberg (20 April 2011). "Crypto Currency". Forbes.com. Archived from the original on 31 August 2014. Retrieved 8 August 2014.
Cryptocurrencies: A Brief Thematic Review Archived 25 December 2017 at the Wayback Machine.. *Economics of Networks Journal*. Social Science Research Network (SSRN). Date accessed 28 August 2017.
Schueffel, Patrick (2017). *The Concise Fintech Compendium*. Fribourg: School of Management Fribourg/ Switzerland. Archived from the original on 24 October 2017.
McDonnell, Patrick "PK" (9 September 2015). "What Is The Difference Between Bitcoin, Forex, and Gold"
Cryptocurrencies: A Brief Thematic Review Archived 25 December 2017 at the Wayback Machine.. *Economics of Networks Journal*. Social Science Research Network (SSRN). Date accessed 28 August 2017.
1.Schueffel, Patrick (2017). *The Concise Fintech Compendium*. Fribourg: School of Management Fribourg/ Switzerland. Archived from the original on 24 October 2017.
2.McDonnell, Patrick "PK" (9 September 2015). "What Is The Difference Between Bitcoin, Forex, and Gold". NewsBTC. Archived from the original on 16 September 2015. Retrieved 15 September 2015.
3.Allison, Ian (8 September 2015). "If Banks Want Benefits of Blockchains, They Must Go Permissionless". NewsBTC. Archived from the original on 12 September 2015. Retrieved 15 September 2015.
4.Jump up^ "Cryptocurrency FAQ - What is Distributed Ledger Technology?". CryptoCurrency Works. Retrieved 21 May 2018.

[14] http://www.commissariatodips.it/profilo/collaborazione-internazionale.html.

dhe Zhvillim (OCSE).

Shërbimi është gjithashtu pika ndërkombëtare e kontaktit për emergjencat me karakter informatik brenda rrjeteve të vendosura në G8 dhe në Këshillin e Evropës dhe që veprojnë 24/7. Si pjesë e aktiviteteve që kanë për qëllim luftimin e pornografisë së fëmijëve në linjë, shërbimi policor i komunikimeve, merr pjesë në mbledhjet e *task forcës së krimit elektronik* (ECTF), Koalicioni Evropian Financiar (KEF) dhe është pjesë e rrjetit të policisë të quajtur *Task Force Virtual Global* (VGT).

Mos harroni, në fund, pjesëmarrjen në *European Working Party on Information Technology Crime* e cila mblidhet rregullisht në Lion nga Sekretariati i Përgjithshëm i Interpolit, nga komiteti *High Tech Crime i Europolit*, Komitetit dhe disa grupeve tematike të punës të Komisionit Evropian[14].

Ne besojmë se është e nevojshme të forcohet ndërveprimi midis ekspertëve në sektorët: informatikë, hetim, qeveritarë dhe joqeveritarë, në mënyrë që të kuptohet më mirë, si dhe, të jemi në gjendje të luftojnë këtë fenomen vazhdimisht në zhvillim: *kiberkrimin*.

7. Konkluzione

1. Krimet kompjuterike janë karakterizuar nga dematerializimi, duke tejkaluar idenë e territorit kombëtar dhe nivelin e lartë të teknologjisë. Disiplina e këtyre veprave është e përmbajtura në ligjin nr. 547, të vitit 1993, që ka sjellë ndryshime në Kodin Penal, duke ndëshkuar penalisht sjelljet kriminale më të përhapura në industrinë e kompjuterëve si aksesi i paautorizuar, dëmtimi, mashtrimi kompjuterik, informacione të rreme, spiunazhi, atentatet ndaj objekteve për përdorim publik, posedimi dhe zbulimi i paautorizuar i kodeve të hyrjes dhe dhuna mbi asetet informatike.

2. Ligji nr. 48, i 18 marsit 2008, ratifikon "Konventën e Këshillit të Evropës mbi krimin kibernetik" e cila ka përfaqësuar marrëveshjen e parë të veçantë ndërkombëtare mbi këtë çështje. Miratimi i këtij ligji të ri, ka dhënë një mundësi për të përshtatur Kodit Penal me krimet kompjuterike pas kontributeve të ligjit 547/1993, që ishte ndërhyrja e parë në këtë çështje.

Bibliografia

1. GDPR EU/679/2016: https://eugdpr.org/
2. Cyber crime real time mapping: https://www.roccobalzama.it/cyberthreat-real-time-map-la-mappa-del-crimine-informatico-in-tempo-reale.
3. Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.
4. Warren G. Kruse, Jay G. Heiser (2002). *Computer forensics: incident response essentials*. Addison-Wesley.
5. Halder, D., & Jaishankar, K. (2011) Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global.
6. FTC Report (2005). "[1]".
7. SPYWARE ""Archived copy" (PDF). Archived from the original (PDF) on November 1, 2013. Retrieved 2016-02-05."
8. Basil Cupa, Trojan Horse Resurrected: On the Legality of the Use of Government Spyware (Govware), LISS 2013, pp. 419–428.
9. FAQ – Häufig gestellte Fragen Archived May 6, 2013, at the Wayback Machine.
10. "Spam". *Merriam-Webster Dictionary* (definition & more). 2012-08-31. Retrieved 2013-07-05.
11. Monty Python (2009-01-13), *Spam - Monty Python's The Flying Circus*, retrieved 2017-01-11.
12. "The Definition of Spam". *The Spamhaus Project*. Retrieved 2013-09-03.
13. "Developer Policy Center – Intellectual Property, Deception, and Spam". *play.google.com*. Retrieved 2016-05-01.
14. "Spam". *Merriam-Webster Dictionary* (definition & more). 2012-08-31. Retrieved 2013-07-05.
15. https://www.lettera43.it/it/articoli/scienza-e-tech/2016/03/05/dark-web-mappa-del-crimine-informatico/163911/.
16. https://www.lettera43.it/it/articoli/scienza-e-tech/2016/03/05/dark-web-mappa-del-crimine-informatico/163911/. consultato il 12 luglio 2017.
17. Sheri Bauman, Ph.D., *Cyberbullying: a Virtual Menace* (PDF), in *University of Arizona*(archiviato dall'url originale il 28 febbraio 2016).
18. Parry Aftab, What is Cyberbullying Exactly, in stopcyberbullying.org.
19. Collana Genuensis, *Bullismo & Co*, Youcanprint, 2015.
20. *Indagine conoscitiva sulla condizione dell'infanzia e dell'adolescenza in Italia 2011*(PDF), su *azzurro.it*, 2011. URL.
21. Cyberbullismo - Polizia di Stato Archiviato il 15 aprile 2013 in Internet Archive.
22. *Facebook e codice penale, quando i leoni da tastiera miagolano*, su *ilfattoquotidiano.it*. URL consultato il 5 marzo 2018.
23. https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en, Qui di seguito riporto una descrizione della terminologia di norma utilizzata per gli standard procedurali.
24. https://www.sicurezzanazionale.gov.it/sisr.nsf/cosa-facciamo/tutela-delle-informazioni/ segreto-di-stato.html.
25. https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale -cyber-2017.pdf.
26. https://www.businessinternational.it/Eventi/3820/Enterprise-Risk-Management-Meeting.
27. https://www.businessinternational.it/Speaker/Index/16171.
28. https://whatis.techtarget.com/definition/information-security-management-system-ISMS. ; https://www.itgovernance.co.uk/blog/what-is-an-isms-and-9-reasons-why-you-should-implement-one/.
29. De Santis, Giulia; Lahmadi, Abdelkader; Francois, Jerome; Festor, Olivier. "Modeling of IP scanning activities with Hidden Markov Models: Darknet case study". *IEEE.ORG*. IEEE. Retrieved 16 April 2018.|1|1.
30. Wood, Jessica (2010). "The Darknet: A Digital Copyright Revolution" (PDF). *Richmond Journal of Law and Technology*. 16 (4): 15–17. Retrieved 25 October 2011.
31. Mansfield-Devine, Steve (December 2009). "Darknets". *Computer Fraud & Security*. 2009(12): 4–6. doi:10.1016/S1361-3723(09)70150-2.
32. Miller, Tessa (10 January 2014). "How Can I Stay Anonymous with Tor?". *Life Hacker*. Retrieved 7 June 2015.
33. Hamilton, Nigel. "The Mechanics of a Deep Net Metasearch Engine". CiteSeerX 10.1.1.90.5847./
34. Devine, Jane; Egger-Sider, Francine (July 2004). "Beyond google: the invisible web in the academic library". *The Journal of Academic Librarianship*. 30 (4): 265–269. doi:10.1016/j.acalib.2004.04.010. Retrieved 2014-02-06.
35. Raghavan, Sriram; Garcia-Molina, Hector (11–14 September 2001). "Crawling the Hidden Web". *27th International Conference on Very Large Data Bases*.
36. "deep Web". *WhatIs.com*. Retrieved 20 June 2018.
37. "Surface Web". *Computer Hope*. Retrieved 20 June 2018.
38. ^Wright, Alex (2009-02-22). "Exploring a 'Deep Web' That Google Can't Grasp". *The New York Times*. Retrieved 2009-02-23.

39. Andy Greenberg (20 April 2011). "Crypto Currency". Forbes.com. Archived from the original on 31 August 2014. Retrieved 8 August 2014.
40. Cryptocurrencies: A Brief Thematic Review Archived 25 December 2017 at the Wayback Machine.. *Economics of Networks Journal.* Social Science Research Network (SSRN). Date accessed 28 August 2017.
41. Schueffel, Patrick (2017). *The Concise Fintech Compendium*. Fribourg: School of Management Fribourg/ Switzerland. Archived from the original on 24 October 2017.
42. McDonnell, Patrick "PK" (9 September 2015). "What Is The Difference Between Bitcoin, Forex, and Gold". NewsBTC. Archived from the original on 16 September 2015. Retrieved 15 September 2015.
43. Allison, Ian (8 September 2015). "If Banks Want Benefits of Blockchains, They Must Go Permissionless". NewsBTC. Archived from the original on 12 September 2015. Retrieved 15 September 2015.
44. Jump up "Cryptocurrency FAQ - What is Distributed Ledger Technology?". CryptoCurrency Works. Retrieved 21 May 2018.
45. http://www.commissariatodips.it/profilo/collaborazione-internazionale.html.

Ligjet

1. Dekreti Legjislativ 15 janar 1992 n. 50: "Zbatimi i Direktivës 85/577 / EEC për kontratat e negociuara larg ambienteve tregtare".
2. Dekreti Legjislativ 29 dhjetor 1992 n. 518: "Zbatimi i Direktivës 91/250 / KEE për mbrojtjen ligjore të programeve kompjuterike".
3. Ligji i 23 dhjetorit 1993 n. 547: "Ndryshimet dhe plotësimet e dispozitave të Kodit Penal dhe të Kodit të Procedurës Penale në lidhje me krimin kibernetik".
4. Direktiva e BE-së 95/46 / EC e 24 tetorit 1995: mbi mbrojtjen e individëve në lidhje me përpunimin e të dhënave personale dhe lëvizjen e lirë të këtyre të dhënave. Neni. 32 i Direktivës parasheh transpozimin e saj nga Shtetet Anëtare "më së voni në mbarimin e vitit të tretë pas miratimit të tij" (23 tetor 1998).
5. Ligji i 31 dhjetorit 1996 n. 675: "Mbrojtja e personave dhe subjekteve të tjera në lidhje me përpunimin e të dhënave personale".
6. Dekreti Legjislativ i 22 Majit 1999 n. 185: "Zbatimi i Direktivës 97/7 / EC mbi mbrojtjen e konsumatorëve në lidhje me kontratat në distancë".
7. Ligji 18 Mars 2008 n. 48: "Ratifikimi dhe zbatimi i Konventës së Këshillit të Evropës mbi krimin kibernetik, nënshkruar në Budapest më 23 nëntor 2001 dhe për përshtatjen e rregullave të brendshme".
8. Artikuj nga 1469-bis deri 1469-sexies të Kodit Civil në lidhje me legjislacionin mbi kushtet e padrejta në kontratat e konsumatorëve.

Sistemet biometrike dhe mbrojtja e tyre me anë të modeleve sintetike:

matja dhe krahasimi, mes teknikave automatike dhe atyre perceptuese të sulmuesve

■**Prof. Asc. Dr. Edlira MARTIRI**
Universiteti i Tiranës
edlira.martiri@unitir.edu.al

Abstrakt

Në mjedise të sigurisë së nivelit të lartë, mbrojtja e të dhënave dhe parandalimi i rrjedhjes së informacionit mbetet një nga sfidat kryesore. Për shembull, në sistemet biometrike, informacioni i saj më i ndjeshëm, modeli, vazhdimisht shkëmbehet, transferohet, përpunohet ndërmjet dhe prej blloqeve përbërës të një sistemi informacioni që menaxhon materialin biometrik. Në këtë sistem, identifikuesi personal i secilit subjekt, si p.sh. emri, ID, apo ndonjë element tjetër, si dhe karakteristika biometrike e tij, ruhen në modulin e bazës së të dhënave. Pyetja që shtrojmë në këtë punim është: në vend që të kemi vetëm një karakteristikë biometrike të mirëfilltë për një përdorues, a mund të ruajmë një bashkësi modelesh,ku vetëm një është e vërteta dhe të tjerat janë sintetike për ta maskuar atë? Nëse një ndërhyrës i mundshëm, i përfton këto modele duke përvetësuar materialin e bazës së të dhënave, a është ai në gjendje t'i rindërtoje dhe dallojë modelin sintetik nga i vërteti? Për këtë pyetje ne përpiqemi të gjejmë përgjigje në këtë punim. Paraqesim një skemë për mbrojtjen e modeleve biometrike, e për të testuar që këto dy lloje janë për sulmuesin të padallueshëm, ne supozojmë një sulm mbi to. Se sa i suksesshëm është sulmuesi, rindërtojmë imazhet e përftuara dhe i klasifikojmë ato nëpërmjet dy teknikave: vizuale dhe automatike. Për të parën kemi ndërtuar një platformë, ku testues njerëzorë mund të klasifikojnë një sërë imazhesh të rindërtuara si nga modelet reale ashtu dhe sintetike. Nga pikëpamja e sulmuesit, eksperimentet na treguan se, krahasuar me klasifikuesin automatik, testuesit njerëzorë dhanë rezultate më të mira perceptuese dhe dalluese të modeleve.

Fjalëkyçe:
modelet sintetike biometrike, rrjedhje e bazës së të dhënave, klasifikim njerëzor, dallimi i fytyrës, PCA.

1. Hyrje

Një sistem biometrik shërben për të lejuar ose mohuar një subjekt të aksesojë një zonë të caktuar të lidhur me të. Ai përbëhet nga disa komponentë kryesorë, duke filluar që nga: (1) lexuesi (skaner, mikrofon, kamera, etj) i biometrikës, (2) ekstraktuesi i vetive, që konverton biometrikën e kapur nga lexuesi në një format të përpunueshëm nga makina, (3) moduli i ruajtjes (p.sh. bazë të dhënash) që ruan të gjitha biometrikat e përpunuara dhe të mbrojtura, (4) krahasuesi, që vlerëson biometrikën e re të sapolexuar dhe e krahason atë me çfarë ka të ruajtur në bazën e të dhënave, (5) moduli i vendimmarrjes, i cili në bazë të rezultatit që kthen krahasuesi (vlerësimi i krahasimit në pikë, e kalon ose jo një vlerë prag), merr një vendim nëse subjekti duhet apo jo të aksesojë më tej sistemin. Duhet të theksojmë që një sistem biometrik ka dy mënyra në të cilën operon: *identifikim* apo *verifikim*.

Pavarësisht metodave, duhet të ketë gjithmonë një *proces regjistrimi* ku çdo subjekt arkivohet bashkë me të dhënat e tij personale. *Mënyra e identifikimit*, nënkupton që një përdorues paraqet vetëm biometrikën e tij, dhe sistemi duhet të gjejë në bazë të saj identitetin e subjektit (p.sh. emër, mbiemër). Në këtë rast bëhet një kontroll *1-me-N* në bazën e të dhënave. Në *mënyrën e verifikimit,* një subjekt paraqet biometrikën e tij, si dhe të dhëna të tjera (p.sh. ID, emër, kod unik, etj). Në këtë rast bëhet një kontroll *1-me-1* në bazën e të dhënave dhe nëse dy të dhënat përputhen mjaftueshëm, atëherë themi se subjekti u verifikua.

Karakteristikat biometrike janë të shumta: fytyrë, gjurmë gishtash, nënshkrim, iris, zë, etj. Sistemi duhet të nxjerrë një sërë veçorish nga kjo përmbajtje, të cilat mbrohen dhe ruhen formën e një *modeli* (template). Sipas përkufizimit, një *model biometrik* është një grup karakteristikash të ruajtura, të krahasueshme drejtpërdrejt me

karakteristika të tjera biometriketë ruajtura në sistem dhe të verifikuara [1]. Ai përmban informacion sensitiv dhe mbi të aplikohen mekanizma mbrojtës (njësoj si fjalëkalimet), por të tillë që të mos e humbin aftësinë për të identifikuar ose verifikuar një person [2].

Kjo është e rëndësishme, pasi modelet, nëse nuk janë të mbrojtura siç duhet, mund të zbulojnë pjesën më të madhe të informacionit të subjektit. Një mashtrues mund ta përdorë këtë informacion dhe të pretendojë të jetë, ai që nuk është. Modelet, mund gjithashtu të zëvendësohen, nëse sistemi i ruajtjes nuk është i sigurt, ose ato mund të modifikohen, kur kalojnë përmes kanaleve të komunikimit. Në këtë kuptim, trajtimi i *mbrojtjes së modeleve*, do të thotë që duhet të merren parasysh sulme të tjera të mundshme në sistem. Për këtë arsye, ne sugjerojmë që duhet të aplikohet *siguria me shumë nivele,* në bazat e të dhënave biometrike.

Siç është propozuar në [3] dhe zbatuar në [4], në skemën e mbrojtjes së modeleve biometrike, mund të shtohet një mekanizëm tjetër shtesë i tipit "karrem" për t'i çuar sulmuesit në rrugë të gabuar. Në të dy punimet, në mesin e një sërë modelesh sintetike, të rreme, u fshehën modele të vërteta biometrike, duke u përzier me njëra-tjetrën dhe ruajtur në të njëjtin rekord. Në këtë rast, nëse një keqdashës zotëron përmbajtjen e bazës së të dhënave, duhet të jetë shumë e vështirë dhe çorientuese për të, të gjejë mes një morie modelesh të padallueshme nga njëra-tjetra, se cili është i vërteti. Pra, vetia kryesore që këto elemente kërkohet të kenë, është *padallueshmëria*, d.m.th., duhet të jetë e pamundur që një sulmues të dallojë një model të vërtetë, nga një model sintetik, edhe nëse ai përdor klasifikues të trajnuar ose subjekte njerëzore të trajnuara. Në rastin ideal, *'e pamundur'* do të thotë se, probabiliteti për të dalluar një model të vërtetë nga një sintetik, është $p = 0.5$.

Në këtë punim ne paraqesim disa kontribute. Së pari, një skemë të re të mbrojtjes së modeleve, ku blloqe modelesh janë krijuar në bazë të metodës së *projeksionit të rastësishëm*, që më pas lidhen për të krijuar modelin e plotë. Së dyti, për të provuar vetinë e tyre të padallueshmërisë, janë ndërtuar disa profile sulmuesish dhe për eksperimentet është konsideruar një sulmues që ka njohuri të plota mbi sistemin. Nga ana tjetër, një grupi testuesish vullnetarë iu kërkua që t'i klasifikojnë ato, në bazë të perceptimit të tyre dhe rezultatet u krahasuan me ato të një klasifikuesi automatik.

Në seksionin 2 japim një pasqyrë të dobësive të sistemit biometrik dhe kërcënimeve të tij kryesore; në seksionin 3, shpjegojmë arkitekturën e sistemit dhe skenarët e sulmit, dhe në seksionin 4, jepet gjenerimi i vektorëve tipik sintetik bazuar në fytyra dhe, mekanizmi mbrojtës i propozuar. Në seksionin 5 paraqiten eksperimentet dhe rezultatet e tyre.

2. Kërcënimet ndaj sistemeve biometrike dhe mekanizmat mbrojtës

2.1 Kërcënimet dhe dobësitë

Përdorimi i biometrikës si një mjet për të verifikuar ose identifikuar një subjekt ka ngritur shpesh shqetësime, kryesisht sepse një sulm mund të imponojë kërcënime reale për gjithë sistemin. Jain et al. në [5] konsiderojnë tre sulme globale ndaj sistemit biometrik:

1. sulm administrativ: këto sulme janë të pranishme si rezultat i administrimit jo të mirënga brenda;

2. infrastrukturë jo e sigurt: këto sulme mund të gjenden në pajisje, programe ose kanale komunikimi të sistemit;

3. tejkalimi biometrik: një sulmues mund të anashkalojë sistemin duke paraqitur një karakteristike të rreme biometrike.

Kërcënimet, sulmet dhe dobësitë e sistemeve të tjera biometrike janë përshkruar në [6-8], duke u klasifikuar në 9 tipa të ndryshëm. Kështu, përmenden falsifikimet biometrike dhe sulmi me komponentë sintetikë [9]; sulmet *Replay* dhe *Hill climbing* [10, 11] që ridërgojnë sinjalet biometrike;*kuajt trojanë* [12] që janë sulme në modulin e ekstraktimit të vetive, krahasuesit dhe vendimmarrësit; sulmet ndaj kanaleve të komunikimit mes komponentëve të sistemit [13, 14], apo dhe sulmet më të shpeshta, që janë ato ndaj sistemeve të ruajtjes së të dhënave [15].

2.2 Mekanizmat mbrojtës së modeleve biometrike

Për të kapërcyer sulmet e lartpërmendura, ka pasur shumë përpjekje nga komuniteti shkencor në hartimin, zbatimin dhe testimin e skemave të ndryshme mbrojtjeje të modeleve biometrike. Ata mund të kategorizohen në dy grupe kryesore:

1. Kriptosistemet biometrike: gjithashtu të referuara si sisteme të bazuara në të dhëna ndihmëse, pasi disa informacione ruhen në modulin e ruajtjes [5]. Përmbajnë dy kategori: me *çelës të gjeneruar* (nga vetë të dhënat biometrike) [16], apo me *çelës të huazuar* (të pavarur nga karakteristikat biometrike). Mekanizmat përfaqësues përfshijnë: *fuzzy commitment* [17], *fuzzy vault* [18], *funksionet reflektues* [19]; dhe *skemat e kuantizimit* [5].

2. *Transformata e vetive* (ose biometrikë e anulueshme): në model aplikohet një funksion transformimi dhe rezultati ruhet në kujtesë. Kjo kategori e skemave të mbrojtjes së modeleve biometrike përfshin: kriptimin (ku modeli transformohet sipas një funksioni i cili ka të anasjelltë [7]) dhe transformimi i pandryshueshëm (në këtë rast funksioni i transformimit të funksionit është një funksion njëdrejtimësh [20]).

Ekzistojnë dhe mekanizmat hibridë, të cilët përfshijnë dy ose më shumë nga teknikat e përmendura, ose dhe skemat që ofrojnë siguri në disa nivele. Një skemë e tillë është sugjeruar në [3]. Kjo teknikë bazohet në PCA (*Principal Component Analysis*–funksion transformimi i diskutuar më tej në seksionin 4.1). Ai shton sigurinë e modeleve biometrike dhe aftësitë e zbulimit të rrjedhjes së informacionit, gjë që nuk gjendet në skemat ekzistuese mbrojtëse.

3. Sistemet biometrike të pasuruara me modele sintetike

Mekanizmat "*karrem*" të sigurisë së informacionit (njohur në literaturë si *honey objects*) përdoren për të tërhequr dhe çorientuar sulmuesit nga të dhënat sensitive. Një shembull i mirë përfaqësues janë *honeypots* [33], të cilat janë makina të rrjetit të përdorura për të larguar kundërshtarët nga makinat më të rëndësishme; ose *honeyfiles* [34] të cilat fshehin përmbajtjen e vërtetë midis dosjeve sintetike. Në fakt, zbatimi i objekteve të rreme në kontekstin biometrik u përdor për herë të pare si një adoptim i *honeywords* [21]. Sipas kësaj ideje, nëse një kundërshtar vjedh skedarin e fjalëkalimit të një përdoruesi, ai mund të hyjë lehtë në llogarinë e tij të sistemit, por nëse në dosjen e fjalëkalimit ka *k-fjalëkalime* ai nuk mund të zbulojë fjalëkalimin e vërtetë nga *'honeywords'*, sintetike. Një nga sfidat kryesore të kësaj metode ishte fakti se ishte e vështirë të gjeneroheshin rastësisht fjalëkalime të rreme, që do të dukeshin si fjalëkalime të vërtetë të përdoruesit, pra vetia e padallueshmërisë ishte e vështirë të sigurohej.

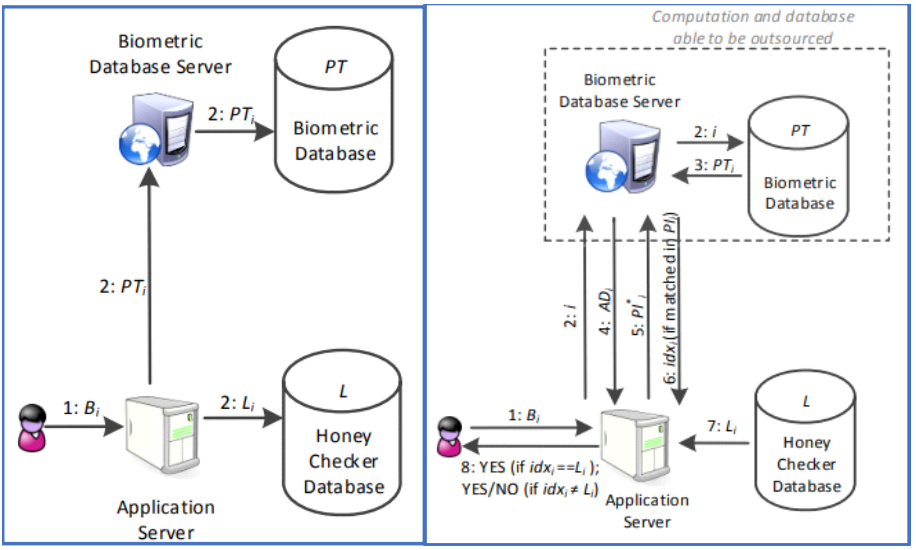
3.1 Arkitektura e sistemit

Në përshtatjen e konceptit të *honeywords*, ne kemi përdorur dhe përcaktuar termat e mëposhtëm:

Modele mjaltë: modele sintetike (*honey templates*) të vendosura në rekordet e një baze të dhënash për të mashtruar sulmuesit.

Bashkësi modelesh: grupi i modeleve biometrike që përmbajnë modelin e vërtetë biometrik të një subjekti, si dhe modelet e krijuara (mjaltë).

Kontrollori i modeleve: një sistem që kontrollon nëse modeli i paraqitur nga një subjekt është një model real apo model mjaltë. Nëse një kundërshtar posedon skedarin e modeleve dhe thyen mekanizmin mbrojtës, duhet të jetë e vështirë për të që të konstatojë modelin e vërtetë. Me gjasë, ai do të përdorë një model mjaltë. Nëse kjo ndodh, sistemi mund të gjenerojë një alarm, pasi u konstatua që sistemi ka zbuluar një rrjedhje informacioni. Një pamje e përgjithshme e arkitekturës së sistemit është paraqitur në Figurën 1 për regjistrimin dhe verifikimin.



(a) Regjistrimi (b) Verifikimi

Fig. 1. Arkitektura e një sistemi biometrik, i bazuar dhe pasuruar me modele mjaltë.

Gjatë regjistrimit: një subjekt S_i paraqet karakteristikën e tij biometrike dhe pas aplikimit të skemës së ekstraktimit dhe skemës së mbrojtjes, gjenerohen modelet sintetike HT_{ij} si dhe modeli real ST_i, të cilët ruhen së bashku. Si rezultat kemi bashkësinë PT_i, të përbërë nga $k+1$ modele:

$$PT_i = \{ST_i, HT_{i1}, HT_{i2}, ..., HT_{ik}\} \quad (1)$$

Modeli real ka pozicion rastësor në hapësirën e kujtesës të alokuar për përdoruesin i dhe indeksi i tij L_i ruhet në bazën e të dhënave kontrolluese (HoneyChecker).

Gjatë verifikimit: për përdoruesin i do të gjenerohet një model i ri (në biometrikë, modeli i prezantuar nuk është saktësisht i njëjtë me modelin e ruajtur gjatë regjistrimit). Ai do të krahasohet me tërë grupin e modeleve dhe rezultati më i mirë prej krahasimeve do të përcaktojë indeksin e modelit. Ky indeks do të krahasohet me L_i, që e merr nga

baza e të dhënave të *Honey Checker*. Nëse ato janë të njëjta, përdoruesi vërtetohet, dhe nëse jo, atëherë sistemi do të konsiderojë që është duke u përdorur një model i rremë, sintetik, pra ka ndodhur një rrjedhje e mundshme e informacionit.

Dy bazat e të dhënave në Figurën 1 (a) dhe 1 (b) propozohen të jenë të pavarura. Kjo pavarësi përmirëson të gjithë sigurinë e arkitekturës së sistemit, pasi një ndërhyrës i mundshëm duhet të kompromentojë të dyja për të marrë informacionin e identitetit të një subjekti. Pra, modelet mjaltë trashëgojnë avantazhet e kriptografisë së shpërndarë, ideja e së cilës është të mbrojë informacionin duke e shpërndarë atë në mesin e një grupi kompjuterësh bashkëpunues [22].

4. Skenarët e sulmit në sistemet biometrike me modele sintetike

Pavarësisht mekanizmave të sigurisë së një sistemi, sulmuesit tentojnë gjithmonë thyerjen e tyre, për të pasur qasje në të dhënat e sistemit. Mund të ekzistojnë lloje të ndryshme sulmuesish, bazuar në nivelin e tyre të njohurive për sistemin dhe sofistikimin e mjeteve që ata posedojnë:

Skenari i parë: Sulmuesi nuk është në dijeni të arkitekturës të sistemit, strukturës së bazës së të dhënave dhe si pasojë e ekzistencës së modeleve mjaltë. Ky sulmues mund të klasifikohet si *sulmues i nivelit të ulët*. Pas marrjes së modeleve të subjektit S_i, sulmuesi i konsideron ato si të vërtetë dheme gjasëvendos të përdorë modelin PT_{ij}. Nëse $j \text{ “‘} L_i$, do të detektohet që sistemi është kompromentuar.

Skenari i dytë: Sulmuesi është i vetëdijshëm për arkitekturën e sistemit biometrik, strukturën e bazës së të dhënave dhe për faktin se po përdor modele mjaltë. Ai nuk ka mjete në dispozicion dhe në këtë rast ai mund të konsiderohet si një *sulmues i nivelit të mesëm*. Pas marrjes së modeleve të subjektit S_i, sulmuesi do të përpiqet të gjejë modelin e vërtetë. Ai vendos të përdorë rastësisht modelin PT_{ij} ose mund t'i ruajë, p.sh. për klasifikim të mëtejshëm.

Nëse gjetja e tij është i saktë, d.m.th. $j = L_i$, sulmuesi do të jetë në gjendje të hyjë në sistem. Pra, probabiliteti i supozimit të modelit të vërtetë varet nga numri i modeleve të shtuar (si rezultat, kompleksiteti i sigurisë i skemës nuk varet vetëm nga kompleksiteti i algoritmit të mbrojtjes). Në varësi të numrit të modeleve, ky probabilitet duhet të jetë i barabartë me:

$$\text{Prob}\ (\text{j} = \text{L}_i) = \frac{1}{k+1} \qquad (2)$$

Skenari i tretë: Sulmuesi është i vetëdijshëm për: (1) arkitekturën e sistemit biometrik; (2) strukturën e bazës së të dhënave dhe faktit se përdor modelet sintetike; (3) algoritmin e përdorur për të gjeneruar bashkësinë e modeleve.

Ai ka mbledhur më parë bashkësi modelesh, por nuk mund t'i dallojë ato (pasi që modelet reale janë të ruajtura në mënyrë të rastësishme midis modeleve mjaltë), si dhe zotëron mjete të sofistikuara. Pas marrjes së modeleve të subjektit S_i, sulmuesi do të përpiqet të kryejë një test klasifikimi dhe pastaj të marrë një vendim. Ai konsiderohet si një *sulmues i nivelit të lartë* dhe perspektiva e tij do të përpunohet më tej, pasi është ky skenari që ne do të konsiderojmë.

5. Metodologjia eksperimentale

5.1 Dizajnimi i detajuar, i sistemit dhe i sulmuesit

Në këtë seksion do të supozojmë dy sisteme: nga njëra anë kemi dizajnuesit e sistemit, e në anën tjetër sulmuesit. Do të paraqesim kornizën eksperimentale të sistemit biometrik *S* dhe sistemit sulmues *A*. Do të përshkruajmë paralelisht perspektivat e tyre duke filluar nga: dizajnim i bazave së të dhënave, nxjerrja e funksioneve, algoritmi i mbrojtjes së modeleve dhe klasifikimi i tyre. Meqenëse në këtë qasje supozuam që sulmuesi është i nivelit të lartë, do të ndërtohen dy sisteme të njëjta nga ana arkitekturore.

Dizenjimi i bazave së të dhënave

Përmbajtja e dy bazave së të dhënave DB_S (sistemi) dhe DB_A (sulmuesi) janë marrë nga *faces94* [35]. Kjo bazë përmban 153 subjekte me 20 kampionë secili (133 meshkuj dhe 20 femra). I gjithë dataseti është përpunuar dhe ndarë më tej për dy sistemet, duke pasur:

$$DB_S = DB_{1..70} \tag{3}$$

$$DB_A = DB_{71..153} \tag{4}$$

Algoritmi nevojit dhe dy databaza ndihmëse, AD_S (sistemi) dhe AD_A (sulmuesi) që janë krijuar nga imazhe publike nga interneti. Ato kanë secili nga 40 imazhe në total (një kampion për çdo subjekt). Një fragment i AD_S është treguar në figurën 2 (a), ndërsa në 2 (b) janë paraqitur subjektet e DB_S.

Gjenerimi i vektorëve

Imazhet e para të DB_S dhe DB_A dekompozohen në vektorë të thjeshtë duke përdorur teknikën PCA. Sipas përkufizimit, PCA është një procedurë matematikore që përdor transformimin ortogonal për të kthyer një bashkësi variabëlish me korrelacion në një bashkësi variabëlish që nuk shfaqin korrelacion [23].

Përdoret gjerësisht në grupet e të dhënave multivariate për të gjetur një grup të reduktuar vektorësh, të cilat mund të shërbejnë si bazë nga e cila gjenerohen të gjithë vektorët e tjerë si kombinim i tyre linear. Të konvertuar në vektorë, imazhet shihen njësoj nga PCA, pra duke pasur qëllim gjetjen e vektorëve bazë [24], të quajtur *eigenfaces*. Teknika gjithashtu redukton dimensionin e imazheve, që është në favor të përpunimit të mëtejshëm. Sistemi i vërtetë biometrik S, do të përdorë AD_S për të gjeneruar *eigenfaces*. Të dy sistemet, S dhe A, veprojnë në mënyrë identike në gjenerimin e vektorëve.

Për thjeshtësi ne do të përshkruajmë vetëm sistemin e vërtetë. Çdo imazh I_i konvertohet nga matrica në vektor dhe pastaj matrica *G*, përmban të gjitha imazhet *I* në formën e tyre vektoriale. Dimensioni i *G* është $dim(G)=dim(I_i)$. Kjo rezulton në $dim(I_i)=92*112=10304$ dhe $dim(G)=10304*40$. Sigurisht që ky dimension është shumë i madh për të përpunuar më tej. Për të gjetur veçoritë më të veçanta mes imazheve, ato të zakonshmet do të hiqen, duke lënë $n = 40$ *eigenfaces*.

(a)

(b)

Fig. 2. (a) Subjekte nga baza e të dhënave ndihmëse të sistemit AD_s. (b) Subjekte nga baza e të dhënave të vetë sistemit DB_s [4].

Algoritmi i mbrojtjes së "templates" biometrike

Në sistemin ekzistues në [4] aplikohet një skemë mbrojtje, e paraqitur në Figurën 3. Ky mekanizëm përdor një vektor maskë m_j, i gjeneruar sipas vlerave të shenjave të vektorëve (+/-). Pastaj, aplikohet një raund i dyfishtë i modulit. Së pari, llogaritet mbetja e vektorit maskë dhe devijimi standard ($ó_x$ dhe $ó_y$ janë dy devijime standarde të parametrizuara, për të rregulluar më mirë performancën e sistemit). Rezultati i tij shtohet tek vektori i thjeshtë dhe pastaj aplikohet një raund i dytë i modulit. Vektori që rezulton, është modeli i mbrojtur STS_i që ka *i"{1,2,...,n}* me *n=70subjekte×20kampionë*. Sulmuesi i ndërton ata në të njëjtën mënyrë, duke gjeneruar nga vektorët e tij, modelet e mbrojtur STA_j me *j"{1,2,...,m}* ku *m=83subjekte×20kampionë*.

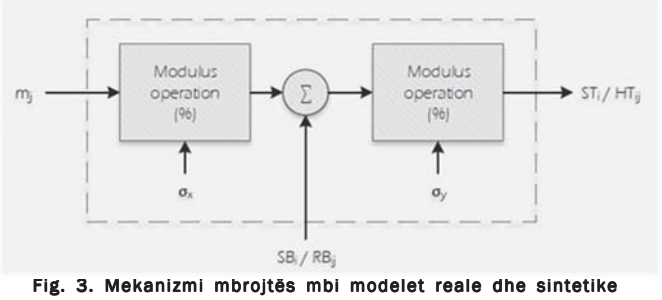


Fig. 3. Mekanizmi mbrojtës mbi modelet reale dhe sintetike

Për çdo kampion të bazave së të dhënave për të dy sistemet (*S* dhe *A*), krijohen 15 modele sintetike. Si karakteristika sintetike përdoren vektorë realë: RB_{St} dhe RB_{At}, me $t"\{1,2,...,k=15\}$, të gjeneruar për secilin kampion. Ato janë të mbrojtura duke ndjekur të njëjtën teknikë të figurës 3, që ka si rezultat HT_{St} dhe HT_{At}. Në sistemin e vërtetë, modelet e vërteta dhe sintetike janë ruajtur të randomizuara duke formuar PT_{Si}. Në figurën 4 mund të shohim një shembull të një përdoruesi nga baza e të dhënave të sistemit. Për një shpjegim të hollësishëm të skemës lexuesi mund t'i referohet [4].

Fig. 4. Shembull i një përdoruesi: (a) imazhi i papërpunuar siç merret gjatë regjistrimit; (b) imazhi i rindërtuar nga modeli real; (c) një pjesë e imazheve të modeleve sintetike të rindërtuara.

Klasifikimi i modeleve

Për të dizajnuar dy klasifikuesit C_S (të sistemit) dhe C_A (të sulmuesit) nevojiten grupe trajnimi dhe testimi për secilin. Qëllimi i C_S është të provojë dallueshmërinë e modeleve të vërtetë STS_i dhe modeleve sintetike HTS_{it}, ndërsa i C_A është të dallojë këto modele në bashkësinë e sistemit PTS_i. Pavarësisht qëllimit të tyre, klasifikuesit kanë dizajnimi të njëjtë. Kemi zgjedhur teknikën SVM (Support Vector Machines) të klasifikimit, pasi është e saktë për të ndarë vektorët në dy klasa dhe më efektive në të dhënat me dimension të lartë.

5.2 Klasifikimi i imazheve të rindërtuara

Përveç klasifikimit të drejtpërdrejtë, një sulmues mund të rindërtojë imazhe të modeleve të mbrojtura (të quajtura pre-imazhe). Thamë që imazhet mund të shprehen si një kombinim linear i peshave (vektorëve të thjeshtë) dhe eigenfaces. Pre-imazhet mund të ndërtohen nga sulmuesi duke përdorur *eigenfaces* e A dhe modelet e sistemit PT_S. Rezultati është një bazë të dhënash të pre-imazheve reale të përzier $SP_{I/A}$ dhe para imazheve të mjaltit $HP_{I/A}$ (të ngjashëm me figurën 4.c). Në këtë bazë të dhënash mund të kryhen dy teste: (I) klasifikim vizual i pre-imazheve; dhe (II) klasifikimi i vektorëve të rindërtuara. Për klasifikimin e vektorëve të rindërtuar u ndoq e njëjta teknikë e përshkruar në seksionin 4.1.

Përshkrim i klasifikimit vizual të pre-imazheve

Një qasje e re që ndërmorëm, është shtimi i një mjeti vizual të klasifikimit, për të

matur perceptimin njerëzor të fytyrave të ngjashme. Sidomos sulmuesit mund të trajnohen në klasifikimin vizual të imazheve paraprake për t'i dalluar ato. Për këtë qëllim, një grup prej 30 testuesish u pyetën për perceptimin e pre-imazheve. Secili prej tyre kërkohej të klasifikonte një grup prej 30 pre-imazhesh të zgjedhura rastësisht midis modeleve sintetike dhe reale. Nuk kishte kufizim kohor në procesin e klasifikimit, gjithsesi koha u mat për të kuptuar nëse klasifikuesit njerëzorë ishin me të vërtetë duke u fokusuar dhe menduar në veçoritë e imazhit për të bërë dallimin mes pre-imazheve. Para se të fillonin, ata u stërvitën duke shikuar dy grupe të fytyrave (një nga pre-imazhet reale dhe një nga pre-imazhet sintetike, të zgjedhur përsëri rastësisht), në mënyrë që të fitonin një perceptim mbi imazhet për të cilat do të testohej. Edhe gjatë testit ata kishin këto bashkësi në dispozicion të tyre. Platforma e testimit është ndërtuar në dy versione: *desktop-based* për vullnetarët në kampus; dhe w*eb-based* për vullnetarët në distancë. Ndërfaqja e platformës është në figurën 5.

Të dhëna dhe rezultate të eksperimentit

Ndër klasifikuesit njerëzorë: 57% ishin femra; 50% në kategorinë e moshës 26-35 vjeç; dhe në37% të rasteve është përdorur platforma e bazuar në internet. Shkalla mesatare e gabimit të subjekteve është 0,419. Shkalla maksimale e gabimit është 0,6 dhe vlera minimale, që do të thotë testuesi më i saktë ka një shkallë gabimi të barabartë me 0,23. Në Tabelën 1 janë paraqitur shkallët e gabimeve të kategorive të ndryshme, bazuar në gjini, platformë dhe moshë.

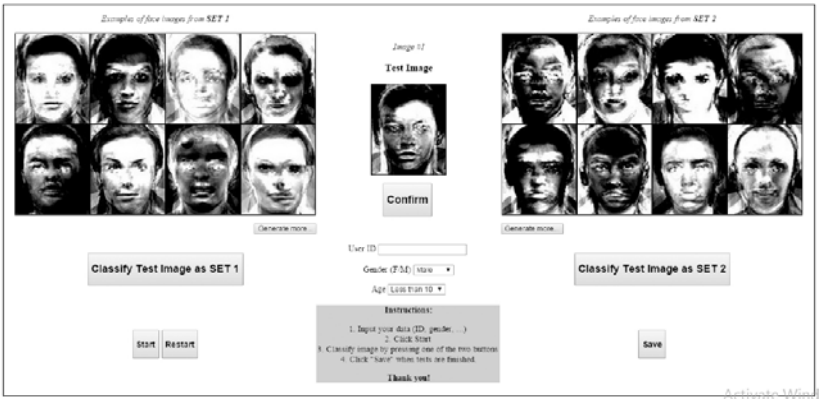


Fig. 5. Ndërfaqja grafike e programit për klasifikimin e pre-imazheve.

Kategori		Gabimi mesatar	Koha mesatare (sek.)
Gjinia	F	0,413	11,5
	M	0,427	17,7
Platforma	Kampus	0,436	14,8
	Online	0,407	13,9
Mosha	< 18	0,427	13,0
	18 – 25	0,407	16,1
	26 – 35	0,420	12,9
	36 – 40	0,450	17,9

Tabela 1. Statistikat mbi shkallën e gabimit dhe kohën mesatare të klasifikimit të pre-imazheve.

Në nënkategoritë e ndryshme, mund të shohim se femrat ishin pak më të sakta se meshkujt dhe gjithashtu, më të shpejta në marrjen e vendimit të tyre. Vullnetarët që mblodhëm në kampus ishin më të saktë se sa testuesit *online*, edhe pse koha e tyre ishte gati e njëjtë. Përsa i përket moshave, kategoria më e saktë ishte 18-25 vjeçe, të cilët gjithashtu morën më shumë kohë se sa kategoritë e tjera në klasifikimin e tyre. Sa i përket mesatares kohore të klasifikimit të pre-imazheve, duke qenë një proces kognitiv, mund të vërehet se vendimmarrja e imazheve të para është më e gjatë se ajo e imazheve të fundit. Pas testit kemi intervistuar subjektet në kampus. Ata u pyetën për perceptimin që kishin për imazhet, nivelin e vështirësisë dhe tipat e karakteristikave që ata shqyrtonin për të marrë një vendim. Karakteristikat që shihnin ishin: zona periokulare, forma e fytyrës dhe sfondi. Dallueshmërinë mes dy tipave (reale dhe sintetike) e vlerësuan si të vështirë.

Sa më afër vlerës ideale, 0.5, aq më të padallueshme janë modelet ose aq më pak të afta janë metodat e përdorura për klasifikimin. Kjo ishte arsyeja themelore pse ne ndoqëm këtë metodologji krahasuese. Nga pikëpamja e një sulmuesi, mund të përmbledhim se një klasifikues njerëzor sillet më mirë në aspektin e saktësisë së klasifikimit me normën mesatare prej 0.419, krahasuar me klasifikuesin SVM, shkalla e të cilit është 0.44.

6. Përfundime

Në këtë punim ofruam përfitimet që mund të sjellin përfshirja e modeleve sintetike si një mekanizëm sigurie në sistemet biometrike. Analizuam kërcënimet e ndryshme dhe dobësitë e sistemit dhe se si këto mund të lehtësohen duke përdorur modelet sintetike. Paraqitëm dy këndvështrime të mundshme, atë të dizajnuesit të sistemit, dhe atë të sulmuesit të një sistemi, ku supozuam që sulmuesi në këtë rast është i një niveli të lartë. Kjo do të thotë, që në supozimin tonë, ai zotëron mjete dhe të dhëna me të cilat teston dy tipat e ndryshëm të modeleve: të vërtetët nga të rremët.

Për të siguruar rezultat të shëndoshë, kemi përdorur dy teknika klasifikimi: një në bazë të klasifikimit njerëzor dhe një mbi klasifikimin automatik. Për llojin e parë është ndërtuar një platformë, ku testuesit njerëzorë klasifikuan një sërë imazhesh të rindërtuara, që mund të jenë nga modelet reale apo të rremet, të ndërtuara me anë të PCA. U mblodhën rezultatet dhe u krahasuan me një klasifikues SVM. Kemi vërejtur se, krahasuar me klasifikuesin SVM, testuesit njerëzorë kanë treguar rezultate më të mira në lidhje me dallimin e modeleve, pra janë më të saktë në dallimin e modeleve të rindërtuara. Nga pikëpamja e sulmuesit, ky është një lajm i mirë. Kjo do të thotë se me një subjekt të trajnuar, ai mund të përmirësojë shanset e tij për të gjetur pre-imazhin e modelit të vërtetë në mesin e një sërë modelesh sintetike. Testuesi më i saktë që kishim, rezultoi me shkallën minimale të gabimit të barabartë me 0,23 dhe testues të tjerë që arritën një rezultat të ngjashëm pas disa tentativash. Ky rezultat interesant, na shtyn që kjo metodë t'i nënshtrohet studimeve të mëtejshme, lidhur me perceptimin vizual dhe proceset e klasifikimit të kujtesës njerëzore, për pamje në dukje jo të rregullta, siç rezultojnë të jenë pre-imazhet.

Mirënjohje

Ky punim hulumtues u financua pjesërisht nga projektet PIDaaS dhe FIDELITY të FP7 dhe Komisionit Europian. Të gjitha informacionet sigurohen siç janë dhe nuk janë përdorur për ndonjë qëllim të veçantë deri tani. Komisioni Evropian nuk ka përgjegjësi në lidhje me këtë dokument, i cili thjesht përfaqëson pikëpamjen e autorëve. Falënderoj prof. asoc. Dr. Bian Yang nga departamenti i sigurisë së informacionit, seksioni i biometrisë, NTNU, si dhe vullnetarët në kampuset e UT (Shqipëri) dhe NTNU (Norvegji).

Bibliografi

1. ISO/IEC 24745, Information Technology - Security techniques - Biometric information protection, 2010.
2. Simoens, K., Yang, B., Zhou, X., Beato, F., Busch, C.,Newton, E.M., Preneel, B.: Criteria towards metrics for benchmarking template protection algorithms. In Proc. of5th IAPR International Conference on Biometrics (ICB),498-505, 2012.
3. Yang, B., Martiri, E.: Using Honey Templates to Augment Hash Based Biometric Template Protection. In Proc. of the 39th IEEE International Computers, Software and Applications Conference, 2015.
4. Martiri, E., Yang, B., Busch, C.: Protected honey face templates. In Proc. of 9th IEEE International conference Biometrics Special Interest Group, BIOSIG, 2015.
5. Jain, A. K., Nandakumar, K., Nagar, A.: Biometric tem-plate security, EURASIP Journal on Advances in Signal Processing, 2008, 113.
6. Breebaart, J., Busch, C., Grave, J., Kindt, E.: A ReferenceArchitecture for Biometric Template Protection based on Pseudo Identities. In Proc. of BIOSIG, 2008, 25-37.
7. Nandakumar, K.: Multibiometric Systems: Fusion Strategies and Template Security. ProQuest, 2008.
8. Buhan, I. R., Hartel, P. H.: The State of the Art in Abuse of Biometrics, Technical report, Centre for Telematics and Information Technology, University of Twente, 2005.
9. Bolle, R., Connell, J., Pankanti, S., Ratha, N, Senior, A.: Guide to Biometrics, Springer-Verlag, 2003.10. Uludag, U., Jain, A. K.: Attacks on biometric systems: a case study in fingerprints. In Proc. of Security, Seganogra-phy and Watermarking of Multimedia Contents VI, SPIE-EI 2004, pp. 622-633.
10. Martinez-Diaz, M., Fierrez-Aguillar, J., Alonso-Fernandez, F., Ortega-Garcia, J, Siguenza, J.A.: Hill-climbing and brute-force attacks on biometric systems: Acase study in Match-on-card fingerprint verification. In Proc. of Carnahan Conferences Security Technology, 40th Annual IEEE International, 2006, pp. 151-159.
11. Understanding Biometrics: http://www.griaulebiometrics.com/en-us/book/understanding-biometrics/types/attacks, accessed 21.05.2015.
12. Sarika, K., Gupta, P.C., Mantri. K.: Survey of Threats to the Biometric Authentication Systems and Solutions. International Journal of Computer Applications 61.17 (2013):39-43.
13. Maltoni, D., Maio, D., Jain, A. K., Prabhakar, S.: Hand-book of Fingerprint Recognition, Springer Professional Computing, 2006.
14. Kaur, M., Sofat, S.: Template and Database Security in Biometrics Systems: A Challenging Task, International Journal of Computer Applications, Volume 4, No.5, 2010.
15. Sutcu, Y., Li, Q., Memon. Protecting biometric templateswith sketch: Theory and practice. IEEE Transactions on Information Forensics and Security, 2(3), pp. 503-512, 2007.
16. Juels, A., Wattenberg, M.: A fuzzy commitment scheme. In Proc. of ACM Conference on Computer and Communications Security, pp. 28-36, 1999.
17. Juels, A.,Wattenberg, M.: A fuzzy vault scheme. In Proc.of IEEE International Symposium on Information Theory,2002.
18. Rathgeb, C., Uhl, A.: A survey on biometric cryptosystems and cancelable biometrics. EURASIP Journal on In-formation Security, no.1. pp. 1-25, 2011.
19. Ratha, N. K., Chikkerur, S., Connell, J. H., Bolle, R.: Generating Cancelable Fingerprint Templates. IEEE Trans-actions on Pattern Analysis and Machine Intelligence,29(4), pp. 561-572, 2007.
20. Juels, A., Rivest, R. L.: Honeywords: Making Password-Cracking Detectable. RSA Labs Cambridge, http://people.csail.mit.edu/rivest/honeywords/, accessed06.04.2015.
21. Cryptography and Information Security Group Research Project: Threshold Cryptology, http://groups.csail.mit.edu/cis/cis-threshold.html, ac-cessed 12.04.2015.
22. Jeong, D. H., Ziemkiewicz, C., Ribarsky, W., Chang, R.,Center, C. V.: Understanding Principal Component Analysis Using a Visual Analytics Tool. Charlotte Visualization Center, UNC Charlotte, 2009
23. Draper, B. A., Baek, K., Bartlett, M. S., Beveridgea, J.R.: Recognizing faces with PCA and ICA, Computer Visionand Image Understanding, 91(1), pp. 115-137, 2003.
24. The Database of Faces: http://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html,accessed 21.01.2014.
25. Calder, A. J. Burton, A. M., Miller, P., Young, A. W.,Akamatsu, S.: A principal component analysis of facial expressions, Vision Research (41), pp. 1179-1208, 2001.
26. Ghaoui, L. el: Optimization models and applications. https://inst.eecs.berkeley.edu/ee127a/book/login/l sym sed.html,accessed 03.09.2015.
27. Strandjev, B., Agre, A.: On Applicability of Principal Component Analysis to Concept Learning from Images. Innovations in Intelligent Systems and Applications (IN-ISTA), IEEE International Symposium, 2013.
28. Turk, M. A., Pentland, A. P.: Face recognition using eigenfaces. In Proc. of Computer Vision and Pattern Recognition (CVPR), IEEE Computer Society Conference, 1991.
29. Thakur, S., Sing, J. K., Basu, D. K., Nasipuri, M.,Kundu, M.: Face Recognition using Principal Component Analysis and RBF Neural Networks. In Proc. of IEEE First International Conference on Emerging Trends in Engineering and Technology (ICETET), pp. 695-700, 2008.
30. Blanchard, G., Bousquet, O., Massart, P.: Statistical performance of support vector machines. The Annals of Statistics 2008, Vol. 36, No. 2, 489-531 DOI:10.1214/009053607000000839, Institute of Mathematical Statistics, 2008.
31. Yang, B.; Hartung, D.; Simoens, K.; Busch, C.: Dy-namic random projection for biometric template protection. In Proceedings of the 4th IEEE International Conferenceon Biometrics: Theory Applications and Systems (BTAS),2010.
32. Honeypots. http://www.honeypots.org/, accessed: May2015.34.
33. J. Yuill, M. Zappe, D. Denning, and F. Feer, Honeyfiles:deceptive files for intrusion detection? in Proc. SMC Information Assurance Workshop (IAW), 2004, pp. 116?122.
35. Collection of Facial Images: Faces 94, http://cswww.essex.ac.uk/mv/allfaces/faces94.html,accessed: October 2015.

Dr. (proc.) Arqilea KOÇA, MSC. ARIAN MUÇAJ

Hapësira kompjuterike: situata e sulmeve kompjuterike në Shqipëri

Dr. (proc.) Arqilea KOÇA
Prokuroria e Rrethit Gjyqësor, Gjirokastër

MSc. Arian MUÇAJ
Prokuroria e Rrethit Gjyqësor, Gjirokastër
amucaj@yahoo.com

Abstrakt

Abstrakt

Globalizimi vazhdon të përhapet në të gjithë botën. Përfitimet nga teknologjia dhe interneti kanë bërë që kriminelët të përdorin hapësirën kompjuterike për të kryer sulme kompjuterike me pasoja të mëdha. Përparimi në teknologjia ka çuar në zbulime të paimagjinueshme 30 vite më parë, por kjo ka bërë më të lehtë krimin kompjuterik. Ekonomia botërore është bërë e varur nga teknologjia duke u përdorur në më shumë fusha. Përdoruesit e teknologjisë janë më të ekspozuar ndaj sulmeve kompjuterike. Sulmet kompjuterike kanë ndryshuar edhe koncepte tradicionale në lidhje me territorin në fushën juridike dhe të sigurisë kombëtare. Në fushën juridike për kimet kompjuterike ka ndryshuar koncepti i ndjekjes penale mbi bazën e vendit të ngjarjes. Hapësira kibernetike me zhvillimin e teknologjisë ka sjell heqjen e kufijve shtetëror për ndjekjen penale. Sulmet kompjuterike kane ndikim në ekonomi në psikologjinë e njerëzve madje dhe në mbrojtjen e vendit. Siguria kombëtare tradicionalisht ka qenë e lidhur me fuqinë ushtarake dhe ekonomike por në periudhën e teknologjisë, mbrojtja nga sulmet kompjuterike ka zëvendësuar ushtarin tradicional me pajisje dhe programe kompjuterike.

Presidenti Obama në vitin 2015 ka deklaruar se " . . . kërcënimi kibernetik është një nga sfidat më serioze të sigurisë ekonomike dhe kombëtare me të cilat përballemi si një komb . . . " Në këtë punim do të bëhet një vështrim i kërcënimit të sigurisë kombëtare nga sulmet kompjuterike dhe një trajtim kriminologjik dhe juridik i krimeve kompjuterike në botë dhe në Shqipëri.

Fjalëkyçe:

Sulme kompjuterike, krime kompjuterike, hapësira kibernetike, legjislacioni kibernetik, e drejta ndërkombëtare kibernetike.

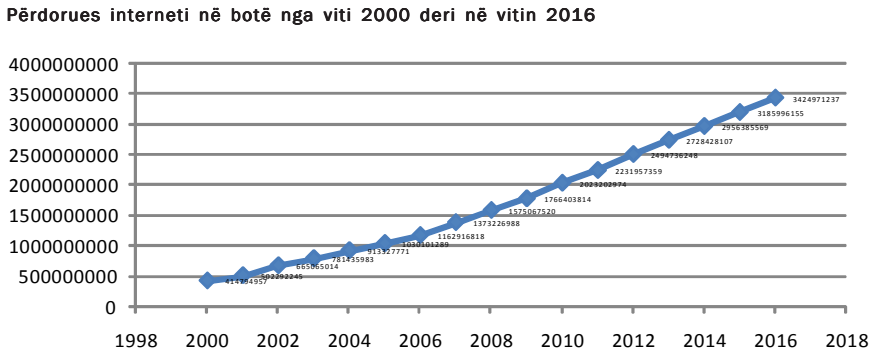
1. Hyrje

Globalizimi vazhdon të përhapet në të gjithë botën. Përfitimet nga teknologjia dhe interneti, kanë bërë që kriminelët të përdorin hapësirën kompjuterike për të kryer sulme kompjuterike me pasoja të mëdha. Përparimi në teknologji ka çuar në zbulime që ishin të paimagjinueshme 30 vite më parë, por kjo e ka bërë më të lehtë krimin kompjuterik. Ekonomia botërore është bërë e varur nga teknologjia, duke u përdorur në më shumë fusha. Përdoruesit e teknologjisë janë më të ekspozuar ndaj sulmeve kompjuterike. Sulmet kompjuterike kanë ndryshuar edhe koncepte tradicionale në lidhje me territorin në fushën juridike dhe të sigurisë kombëtare. Në fushën juridike, për krimet kompjuterike, ka ndryshuar koncepti i ndjekjes penale mbi bazën e vendit të ngjarjes. Hapësira kibernetike, me zhvillimin e teknologjisë ka sjellë heqjen e kufijve shtetërorë për ndjekjen penale. Sulmet kompjuterike kanë ndikim në ekonomi, në psikologjinë e njerëzve madje edhe në mbrojtjen e vendit. Siguria kombëtare, tradicionalisht ka qenë e lidhur me fuqinë ushtarake dhe ekonomike, por në periudhën e teknologjisë, mbrojtja nga sulmet kompjuterike ka zëvendësuar ushtarin tradicional me pajisje dhe programe kompjuterike. Presidenti Obama, në vitin 2015 ka deklaruar se: " ... kërcënimi kibernetik është një nga sfidat më serioze të sigurisë ekonomike dhe kombëtare, me të cilat, përballemi si komb..." Në këtë punim, do të bëhet një vështrim i kërcënimit të sigurisë kombëtare nga sulmet kompjuterike, dhe një trajtim kriminologjik, dhe juridik, i krimeve kompjuterike në botë, dhe në Shqipëri.

2. Hapësira kibernetike

Në shekullin e 20, zhvillimi i teknologjisë, në veçanti interneti, ka transformuar

mënyrën e jetesës dhe në veçanti, konceptet e krimit dhe të luftës ndaj krimit, të lidhur me teknologjinë.



Ndryshimi i kriminalitetit kompjuterik, ka nxjerrë mangësi në të drejtën penale materiale dhe në atë procedurale, duke krijuar sfida të reja. Një nga sfidat kryesore, është përcaktimi ligjor, për të rregulluar konfliktin ndërmjet sovranitetit dhe juridiksionit, në hapësirën kibernetike pa kufij. Hapësira kibernetike mund të ketë shumë përkufizime teknike. Për efekt të studimit të hapësirës kibernetike në aspektin juridik, do ta trajtonim në tri aspekte:

-aspekti fizik i cili përbëhet nga objekte materiale të tilla si tela, telefona celularë, satelitë, kompjuter etj.;

-aspekti logjik që përbëhet nga programe dhe protokolle që rregullojnë shkëmbimin e të dhënave në të gjithë rrjetin;

-aspekti i përmbajtjes që përbëhet nga vetë të dhënat kompjuterike që shpërndahen, shkëmbehen, ruhen, fshihen, ndryshohen etj.

Hapësira kibernetike nuk ka kufij të bazuar në territor, pasi shpejtësia e transmetimit të mesazhit në rrjet është e pavarur nga vendndodhja fizike e shpërndarësit dhe e marrësit. Ligji dhe jurisprudenca penale tradicionale, në shekullin e 21 nuk mjaftojnë për t'u zbatuar në hapësirën kompjuterike. Komunikimet elektronike globale krijuan hapësira të reja, në të cilat, duhet të zhvillohen rregulla të ndryshme nga bota reale. Hapësira kibernetike ka cenuar marrëdhënien ndërmjet veprimeve ligjore (*online*) dhe vendndodhjes fizike të përdoruesve të kësaj hapësire. Rrjeti global i kompjuterëve, po prish lidhjen, ndërmjet vendndodhjes fizike gjeografike dhe fuqisë së shteteve individuale: për të ushtruar kontroll mbi veprimet *online*; pasojave së veprimeve *online* të personave; përpjekjet individuale të shteteve për të rregulluar ketë veprimtari globale; dhe dilemës së vendndodhjes fizike të sistemeve kompjuterike për të përcaktuar ligjet që do të zbatohen.

Jurisprudenca e një vendi pasqyron përvojën dhe kulturën historike të këtij vendi. Ligjet e hapësirës kibernetike duhet të dallojnë nga çdo gjë që gjendet në botën fizike. Për ta thjeshtuar: nëse në botën fizike, çdo individ është i identifikuar nga një kartë identiteti, - fotografi, gjurmë gishtash ose profili i ADN-së, - në hapësirën kibernetike mjafton një adresë *e-mail* për të identifikuar një individ ose një grup individësh.

Koncepte tradicionale të botës si, "barazia", "të drejtat dhe detyrimet", etj., mund të mos funksionojnë siç i kuptojmë normalisht, në hapësirën kibernetike. Nëse në një legjislacion kombëtar mbizotëron liria e shprehjes, në një legjislacion tjetër kombëtar,

mbizotëron e drejta e individit për të mos u fyer. Përmbajtja e një njoftimi për një individ i cili e konsideron veten të fyer nga ky njoftim mundet të jetë bërë në një server mijëra kilometra larg vendndodhjes së këtij individi, në një juridiksion i cili nuk e dënon këtë, si vepër penale. Një faqe interneti ".al", që identifikon një *domain* i cili është licencuar sipas legjislacionit shqiptar, jo domosdoshmërish e ka serverin e saj në Shqipëri.

Gjykatat, deri tani e kanë trajtuar hapësirën kibernetike si "vend fizik" për të justifikuar zbatimin e ligjeve tradicionale që rregullojnë aspekte civile dhe penale. Edhe brenda një juridiksioni, sot ka vështirësi për përcaktimin e "vendit" të krimit. Kompetenca tokësore e gjykatave është e përcaktuar mbi bazën e krimit tradicional[1]. Mosmarrëveshjet në lidhje me kompetencën e gjykatave në Shqipëri, i zgjidh Gjykata e Lartë.

Pothuajse të njëjtën të drejtë e ka edhe Gjykata e Kasacionit, në Itali. Kjo gjykatë ka qenë në vështirësi për të përcaktuar kompetencën e gjykatave në lidhje me gjykimin e veprave penale të ndërhyrjes së paautorizuar në sistemet kompjuterike. Gjykata e Kasacionit Italiane, duke e trajtuar hapësirën kompjuterike si një vend, ka konsideruar se autoritet kompetent për gjykimin e një ndërhyrje të paautorizuar në një sistem kompjuterik është gjykata e vendit në të cilin kanë ardhur pasojat e krimit[2].

Dy vjet më vonë, po Gjykata e Kasacionit e Italisë, ka unifikuar praktikën gjyqësore duke përmbledhur se vendi i kryerjes së krimit të ndërhyrjes së paautorizuar në një sistem kompjuterik, është vendi në të cilin gjendet autori që po kryen këtë ndërhyrje kompjuterike[3]. Kjo vështirësi në përcaktimin e kompetencës brenda një shteti, shtohet shumëfish në marrëdhëniet ndërkombëtare, ku mungon një gjykatë e posaçme e cila do të vendoste kompetencën për gjykimin e rasteve që lidhen me sistemet kompjuterike.

Në të drejtën civile, një kontrate nuk mund t'i mohohet zbatimi vetëm se është elektronike ose nënshkruar në mënyrë elektronike. Sipas legjislacionit shqiptar kontratat elektronike janë të vlefshme sipas kufizimeve përkatëse. Në zgjidhjen e mosmarrëveshjeve ndërmjet palëve kontraktuese me kontratë elektronike legjislatori ka qenë në vështirësi për të bërë një rregullim të plotë të zgjidhje se tyre[4]. Në nenin 24 ka parashikuar se mosmarrëveshjet zgjidhen *"... nga gjykata e arbitrazhit, sipas klauzolave të arbitrazhit, në përputhje me legjislacionin në fuqi"*.

Me gjithë vështirësitë e mësipërme, në përfundim të gjykimit të një krimi kompjuterik, ka qenë një person fizik, i cili ka qëndruar pas një pajisje elektronike dhe ky person, është gjykuar. Nuk mund të parashikohen vështirësitë në ndjekjen penale që do të krijohet në një të ardhme të afërt, me zhvillimin shumë të madh të inteligjencës artificiale, e cila po krijon sisteme të pavarura nga njeriu që perceptojnë mjedisin dhe ndërmarrin veprime vet për zgjidhje. Ajo që ndodh në hapësirën kibernetike është e lidhur me atë që ndodh në hapësirën reale. Njerëzit përdorin hapësirën kibernetike duke qarkulluar informacione ose kryejnë transaksione elektronike, por këta njerëz ju përkasin juridiksioneve të ndryshme. Kur një person vendos të dhëna në hapësirën kibernetike, ai mund të komunikojë me persona në pothuajse të çdo juridiksioni.

Vlen të përmendet se njerëzit që vendosin informacion në hapësirën kibernetike duhet të jenë subjekt i juridiksionit në shtetin e tyre, por jo vetëm. Për këtë arsye kërkohet harmonizim i ligjeve në hapësirën kibernetike. Hapësira kibernetike u iniciua

[1] Nenet 76 dhe 77 të Kodit të Procedurës Shqiptare përcaktojnë rregullat e kompetencës tokësore.
[2] Vendimi nr. 40303, datë 27.9.2013 i Seksionit penal të Gjykatës së Kasacionit Itali.
[3] Vendimi Unifikues nr. 17325, datë 24.4.2015 i Gjykatës së Kasacionit Itali.
[4] Ligji nr. 10128, datë 11.5.2009 "Për tregtinë elektronike" i ndryshuar me Ligjin nr. 135/2013 "Për disa shtesa dhe ndryshime në ligjin nr. 10128, datë 11.5.2009 "Për tregtinë elektronike".

nga shteti dhe shumë shpejt u privatizua, duke bërë që shteti të minimizonte lidhjen e tij të drejtpërdrejtë me këtë hapësirë. Por shpejt shtetet kuptuan se duhet të ndërhynin për të rregulluar ligjërisht këtë veprimtari. Tashmë, shtetet kanë filluar të vendosin juridiksionin e tyre jashtë territorit të tyre fizik në lidhje me veprimet në hapësirën kibernetike. Këtë veprim ndërmori edhe legjislatori shqiptar në vitin 2008. Me ligjin nr. 10023, datë 27.11.2008, në nenin 7 të Kodit Penal Shqiptar, shtoi pikën "j":

" Ligji penal i Republikës së Shqipërisë është i zbatueshëm edhe për shtetasin e huaj që jashtë territorit të Republikës së Shqipërisë kryen në dëm të interesave të shtetit ose të shtetasit shqiptar një nga krimet e mëposhtme: .... j) vepra penale në fushën e teknologjisë së informacionit".

Formë e re, e kërcënimit të sigurisë sot, është edhe terrorizmi kompjuterik, i cili do të kishte pasoja të mëdha në një ose më shumë vende njëherësh. Vendndodhja fizike e personave të përfshirë në këto sulme terroriste, mundet të jetë shumë larg dhe në juridiksione të ndryshme nga vendi ose juridiksioni në të cilin kanë ardhur pasojat. Marrëdhëniet e sotme juridiksionale me jashtë, janë rregulluar me konventa dhe marrëveshje ndërkombëtare, por, që në thelb të tyre ndiqet rruga e letër porosive për marrje provash, ose transferim procedimesh dhe njohje vendimesh gjyqësore. Në një situatë të një sulmi terrorist kompjuterik, procedura burokratike e marrëdhënieve juridiksionale me jashtë do të pengonte një hetim dhe gjykim të shpejtë dhe efikas.

Hapësira kibernetike sfidon varësinë tradicionale të ligjit në kufijtë territorialë. Ajo është një hapësirë e pafund elektronike dhe vend i kufizuar, nga ekranet dhe fjalëkalimet, në vend të piramidave tradicionale fizike. Hapësira kibernetike nuk sfidon nocionin territorial të shtetit, si një grupim kolektiv, që banon brenda kufijve të caktuar gjeografikë, me një grup ligjesh që veprojnë në këtë territor, por thjesht shton një dimension të ri, në dobi të territorit dhe sovranitetit të shtetit. Nocioni tradicional i të qenit fizikisht në një vend të caktuar, i lidhur me veprimin ose pasojën e këtij veprimi, është i rrënjosur thellë në doktrinën juridike. Hapësira kibernetike e zgjeron këtë koncept reciprokisht për çdo shtet.

Komunikimi global me bazë kompjuteri, prek të gjithë kufijtë territorialë, duke krijuar një fushë të re të aktivitetit njerëzor dhe duke zvogëluar mundësinë e zbatimit të ligjeve, të bazuara në kufijtë gjeografikë. Ndërsa këto komunikime elektronike kalojnë kufijtë gjeografikë, sot është krijuar një kufi i ri, i përbërë nga ekranet dhe fjalëkalimet që e ndajnë botën virtuale të elektroneve nga "bota reale". Ky kufi i ri përcakton hapësirën kibernetike që ka nevojë dhe duhet të krijojë ligjin e vet dhe institucionet ligjore. Për këtë, është e nevojshme që të ketë disa rregullime ndërkombëtare në fushën e hapësirës kibernetike, ashtu siç ekzistojnë rregulla të veçanta ndërkombëtare, për hapësirën ajrore ndërkombëtare dhe zonat e detare. Një nga rregullimet më të vjetra në këtë fushë, është "Outer Space Treaty"[5], në të cilin u përcaktua se Hëna, hapësira, është e të gjithëve. Po kështu, me traktatin e Romës[6] është përcaktuar krijimi i Gjykatës Ndërkombëtare Penale, me seli në Hagë, e cila *"mund të ushtrojë funksionet dhe kompetencat e saj në territorin e çdo Shteti Palë"*[7].

[5] Traktati mbi parimet që drejtojnë veprimtaritë e shteteve në eksplorimin dhe përdorimin e hapësirës së jashtme, duke përfshirë hënën dhe trupa të tjerë qiellore, 27 janar 1967.

[6] Statuti i Romës për Gjykatën Penale Ndërkombëtare i miratuar nga Konferenca Diplomatike e të Plotfuqishmëve në Kombet e Bashkuara për themelimin e Gjykatës Ndërkombëtare Penale më 17 korrik 1998, hyrë në fuqi më datë 1 korrik 2002. Ratifikuar nga Shqipëria me ligjin Nr. 8984, datë 23.12.2002 "Për ratifikimin e statutit të Romës për Gjykatën Ndërkombëtare Penale".

[7] Neni 4 "Statusi ligjor dhe kompetenca e Gjykatës" i Statusit të Romës për Gjykatën Penale Ndërkombëtare.

Juridiksioni ndërkombëtar kibernetik është metoda më efikase dhe më e shpejtë për të parandaluar krimet kompjuterike ndërkombëtare, duke rritur mundësinë për ndjekje penale dhe ndëshkim të autorëve të tyre. Krijimi i jurisprudencës kibernetike ndërkombëtare, do t'i jepte kompetencën të gjitha gjykatave anembanë globit, të drejtën, të merren me transaksionet në hapësirën kibernetike, mosmarrëveshjet ose krimet kibernetike, siç është edhe terrorizmi kibernetik. Njohja reciproke e vendimeve të këtyre gjykatave, do të sillte siguri në hapësirën kibernetike dhe siguri në ekonominë e bazuar në tregtinë elektronike, pasi transaksionet ekonomike në hapësirën kibernetike, ndikojnë në të njëjtën kohë në të gjitha juridiksionet. Juridiksioni kibernetik ndërkombëtar, do të thotë se, çdo shtet, njerëzit e të cilit janë prekur në ndonjë mënyrë nga një veprim elektronik, do të ketë juridiksion për të vendosur dhe vendimi, do të jetë i zbatueshëm në çdo vend, duke u bazuar në një të drejtë ndërkombëtare, e cila do të zgjidhej me marrëveshje dhe konventa ndërkombëtare.

Në nivelin ndërkombëtar janë marrë masa për lehtësimin dhe bashkëpunimin ndërmjet juridiksioneve të ndryshme deri në nivel policor. Në Interpol dhe Europol janë krijuar struktura të posaçme vetëm për hetimin e krimeve kompjuterike duke lehtësuar procedurat e shkëmbimit të informacioneve.

Në këtë aspekt, nga Këshilli i Evropës është ndërmarrë një hap shumë i rëndësishëm, për zvogëlimin e juridiksionit territorial në hetimin e krimeve kompjuterike. Komiteti i Ministrave të Këshillit të Evropës, në sesionin e 109-të, më 8 nëntor 2001, miratoi "Konventën për krimin kibernetik", e cila u hap për nënshkrim në Budapest, më 23 nëntor 2001, në konferencën ndërkombëtare për krimin kibernetik. Hartuesit e kësaj konvente iu përgjigjën situatës së ndryshimeve të mëdha të globalizimit të hapësirës kompjuterike.

Qëllimet e "Konventës për krimin në fushën e kibernetikës" gjenden që në preambulën e saj, por përmbledhtas, kjo konventë ka rritur në një masë të madhe bashkëpunimin ndërkombëtar në luftën kundër krimeve kompjuterike[8]. Megjithëse kjo konventë është e Këshillit të Evropës, aktualisht po përdoret si një konventë ndërkombëtare, pasi është nënshkruar nga 25 shtete të cilat nuk janë pjesë e Këshillit të Evropës.

Diskutim i rëndësishëm, do të ishte ideja e krijimit të organeve ndërkombëtare të akuzës, por edhe i gjykatave kibernetike shtetërore, që të kenë juridiksion ndërkombëtar. Në rastet e krimeve kompjuterike me pasoja në disa shtete, krijimi i një organi akuze i cili do të drejtonte e koordinonte hetimet ndërmjet disa juridiksionesh,

[8] i. nevoja për ndjekjen në mënyrë prioritare të një politike të përbashkët penale për të mbrojtur shoqërinë nga krimi kibernetik, nëpërmjet edhe krijimit të legjislacionit të përshtatshëm dhe nxitjen e bashkëpunimit gjyqësor ndërkombëtar;
ii. nevoja për bashkëpunim midis shteteve dhe industrisë private në luftën kundër krimit kibernetik dhe nevoja për të mbrojtur interesat e ligjshme në përdorimin dhe zhvillimin e teknologjive të informacionit;
iii. lufta efektive kundër krimit kibernetik nëpërmjet një bashkëpunimi të gjerë, të shpejtë dhe efektiv në çështjet penale;
iv. nevoja për frenimin e veprimeve të drejtuara kundër konfidencialitetit, integritetit dhe disponueshmërisë së sistemeve kompjuterike, rrjeteve dhe të dhënave kompjuterike, sikurse edhe të keqpërdorimit të këtyre sistemeve, rrjeteve dhe të dhënave, nëpërmjet sigurimit që një veprimtari e tillë të kriminalizohet dhe nëpërmjet krijimit të forcave të mjaftueshme për luftimin efektiv të këtyre veprave penale, duke lehtësuar zbulimin, hetimin dhe ndjekjen penale të këtyre veprave penale në të dyja nivelet kombëtare;
v. nevoja për të siguruar një balancim të përshtatshëm ndërmjet interesave të zbatimit të ligjit nga njëra anë dhe respektimit të të drejtave themelore të njeriut nga ana tjetër. Tek këto të fundit veçohen liria e shprehjes (që përfshin të drejtën për të kërkuar, për të marrë dhe për të dhënë informacion dhe ide të të gjitha llojeve, pa marrë parasysh kufijtë), si dhe të drejtat që përfshijnë respektimin e privatësisë dhe mbrojtjen e të dhënave personale.

pa pasur nevojë për letër-porosi me këto juridiksione, do të ishte shumë efikas.

Vazhdimi i kësaj ideje me rëndësi, do të ishte:

Krijimi në çdo shtet, i gjykatave kibernetike, vendimet e të cilave do të kishin efekt në juridiksione të tjera. Nocionet, doktrinat dhe ligjet që lidhen me sovranitetin shtetëror duhet të jenë të zbatueshme drejtpërdrejt edhe në sovranitetin e "shtetit elektronik ndërkombëtar". Juridiksioni ndërkombëtar është metoda më operative, për të dekurajuar dhe parandaluar krimet ndërkombëtare, duke rritur mundësitë për ndjekjen dhe ndëshkimin e autorëve të saj.

Themelimi i jurisprudencës kibernetike ndërkombëtare, për hapësirën kibernetike, si hapësirë dhe vend elektronik, duke lejuar që të gjitha gjykatat anembanë globit të merren me transaksionet në hapësirën kibernetike, dhe mosmarrëveshjet ose krimet kibernetike, siç është terrorizmi kibernetikë.

3. Situata e sulmeve kompjuterike në Shqipëri dhe masat e marra

Me ligjin nr. 8733, datë 24.1.2001, në Kodin Penal Shqiptar, për herë të parë, është parashikuar një vepër penale në fushën kompjuterike[9]. Me këtë ligj është shtuar neni 192/b i cili parashikonte si kundërvajtje penale ndërhyrjen në transmetimet kompjuterike dhe në programe kompjuterike. Me ligjin nr. 9686, datë 26.2.2007, kjo kundërvajtje është ndryshuar duke u bërë krim por duke parashikuar të njëjtën masë dënimi si ka qenë më parë. Neni 192/b ishte një vepër penale e përgjithshme dhe ishte e vështirë për tu aplikuar nga organi i akuzës dhe nga gjykatat shqiptare.

Prej vitit 2003 deri në vitin 2008, për këtë vepër penale, sipas treguesve statistikorë të Prokurorisë së Përgjithshme, janë regjistruar vetëm tre procedime penale nga të cilët, një është regjistruar në Prokurorinë pranë Gjykatës së Shkallës së Parë Pogradec, dhe 2, në Prokurorinë Tiranë. Të tre këto procedime penale janë pezulluar.

Me ligjin nr. 10 023, datë 27.11.2008 në Kodin Penal, janë shtuar shumë vepra penale në fushën e teknologjisë. Në konventën për krimin në fushën e kibernetikës" ratifikuar nga Shqipëria me ligjin nr. 8888, datë 25.4.2002 për ratifikimin e "Konventës për krimin në fushën e kibernetikës", jepen shpjegime të rëndësishme ligjore, për termat e përdorur në veprat penale kompjuterike. Kështu, në këtë konventë jepen shpjegime për terma të përdorur në Kodin Penal dhe Kodin e Procedurës Penale, si: "sistem kompjuterik"; "të dhëna kompjuterike"; "dhënës shërbimesh" dhe "të dhëna trafiku"[10].

[9] Neni 192/b *"Ndërhyrja në transmetimet kompjuterike Ndërhyrja në çdo formë, në transmetimet dhe programet kompjuterike, përbën kundërvajtje penale dhe dënohet me gjobë ose me burgim gjer në tre vjet. Po kjo vepër, kur ka sjellë pasoja të rënda, dënohet me burgim gjer në shtatë vjet."*

[10] Neni 1. Përkufizimet/ Për qëllimet e kësaj Konvente:

a) *"Sistem kompjuterik" do të thotë çdolloj pajisje apo grup i ndërlidhur ose pajisje të lidhura, një ose më shumë prej të cilave, vazhduese të një programi kryejnë procesime automatike të të dhënave.*

b) "Të dhëna kompjuterike" do të thotë çfarëdolloj përfaqësimi të fakteve, informacioni apo konceptesh në një formë të përshtatshme për procesim në një sistem kompjuterik, që përfshijnë një program të përshtatshëm për punën e një sistemi kompjuterik për të kryer një funksion;

c) "Dhënës shërbimesh" do të thotë: (i) çfarëdo entiteti publik apo privat, që i siguron shërbimin e tij përdoruesve, me mundësinë për të komunikuar nëpërmjet një sistemi kompjuterik; dhe (ii) çfarëdo entiteti tjetër, që proceson apo memorizon të dhëna kompjuterike në të mirë të një shërbimi të këtillë komunikimi apo të përdoruesve për këtë shërbim.

d) "Të dhëna trafiku" do të thotë çdolloj të dhënash kompjuterike, të lidhura me komunikimin nëpërmjet një sistemi kompjuterik të prodhuara nga një sistem kompjuterik që përfaqëson një pjesë në zinxhirin e komunikimit, duke treguar origjinën e komunikimit(eve) destinacionin, rrugën, kohën, datën, përmasat, kohëzgjatjen apo tipin e shërbimit të poshtëshënuar.

Krimet kompjuterike që rregullohen nga kjo konventë dhe protokolli shtesë i saj, ndahen në katër grupe: "veprat penale kundër konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave dhe sistemeve kompjuterike"; "krimet e lidhura me kompjuterët"; "veprat penale të lidhura me përmbajtjen" dhe "veprat penale të lidhura me dhunimin e të drejtës së autorit dhe të drejtave të tjera të lidhura me të".

Në grupin e parë të veprave penale kompjuterike, futen të gjitha veprat penale, të cilat kryhen vetëm në sistemet kompjuterike. Në Kodin Penal Shqiptar, parashikohen në nenet: 192/b; 293/a; 293/b; 293/c dhe nenin 293/ç[11].

Në grupin e dytë futen veprat penale të parashikuara nga nenet 143/b "Mashtrimi kompjuterik"dhe neni 186/a "Falsifikimi kompjuterik". Në veprat penale të grupit të tretë, futen veprat penale të parashikuara nga nenet 74/a: "Shpërndarja kompjuterike e materialeve pro gjenocidit ose krimeve kundër njerëzimit" ; 84/a "Kanosja me motive racizimi dhe ksenofobie nëpërmjet sistemit kompjuterik"; 119/a "Shpërndarja e materialeve raciste ose ksenofobike nëpërmjet sistemit kompjuterik"dhe neni 119/b i Kodit Penal "Fyerja me motive racizmi ose ksenofobie nëpërmjet sistemit kompjuterik. Në këtë grup veprash penale, futen edhe ato të parashikuarat nga nenet: paragrafi i katërt i nenit 108, "Vepra të turpshme", dhe neni 117, "Pornografia", kur kryhen "në", ose, "nëpërmjet" sistemeve kompjuterike.

Në grupin e katërt, futen veprat penale të parashikuara nga: neni 147, "Mashtrimi me veprat e artit e të kulturës"; neni 148, "Botimi i veprës së tjetrit me emrin e vet"; neni 149, "Riprodhimi pa të drejtë i veprës së tjetrit"; neni 149/a, "Shkelja e të drejtave të pronësisë industriale", kur kryhen në sisteme kompjuterike, dhe, neni 149/b, "Shkelja e

---

[1] Neni 192/b *Hyrja e paautorizuar kompjuterike (Shtuar me ligjin nr. 8733, datë 24.1.2001; ndryshuar me ligjin nr. 8686, datë 26.2.2007; ndryshuar me ligjin nr. 10 023, datë 27.11.2008) Hyrja e paautorizuar apo në tejkalim të autorizimit për të hyrë në një sistem kompjuterik a në një pjesë të tij, nëpërmjet cenimit të masave të sigurimit, dënohet me gjobë ose me burgim deri në tre vjet. Kur kjo vepër kryhet në sistemet kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile, të shëndetësisë apo në çdo sistem tjetër kompjuterik, me rëndësi publike, dënohet me burgim nga tre deri në dhjetë vjet*

Neni 293/a Përgjimi i paligjshëm i të dhënave kompjuterike (Shtuar me ligjin nr. 10 023, datë 27.11.2008) Përgjimi i paligjshëm me mjete teknike i transmetimeve jopublike, i të dhënave kompjuterike nga/ose brenda një sistemi kompjuterik, përfshirë emetimet elektromagnetike nga një sistem kompjuterik, që mbart të dhëna të tilla kompjuterike, dënohet me burgim nga tre deri në shtatë vjet. Kur kjo vepër kryhet nga/ose brenda sistemeve kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile apo në çdo sistem tjetër kompjuterik, me rëndësi publike, dënohet me burgim nga shtatë deri në pesëmbëdhjetë vjet.

Neni 293/b Ndërhyrja në të dhënat kompjuterike (Shtuar me ligjin nr. 10 023, datë 27.11.2008; shtuar paragrafi i tretë me ligjin nr. 36/2017, datë 30.3.2017) 1. Dëmtimi, shtrembërimi, ndryshimi, fshirja apo suprimimi i paautorizuar i të dhënave kompjuterike dënohen me burgim nga gjashtë muaj deri në tre vjet. 2. Kur kjo vepër kryhet në të dhënat kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile, të shëndetësisë apo në çdo të dhënë tjetër kompjuterike, me rëndësi publike, dënohet me burgim nga tre deri në dhjetë vjet. 3. Në rastet kur veprimet e parashikuara në paragrafin e parë janë kryer nga një i mitur, ndaj tij do të zbatohen dispozitat e Kodit të Drejtësisë për të Mitur.

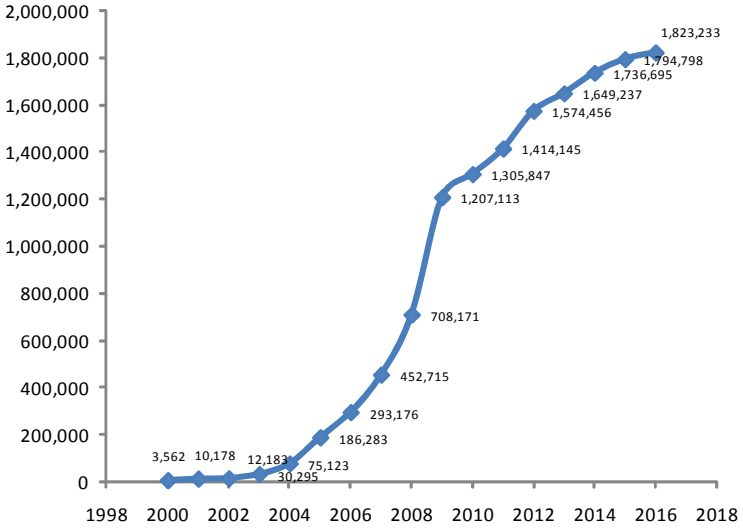
Neni 293/c Ndërhyrja në sistemet kompjuterike (Shtuar me ligjin nr. 10 023, datë 27.11.2008; ndryshuar me ligjin nr. 36/2017, datë 30.3.2017) Krijimi i pengesave serioze dhe të paautorizuara për të cenuar funksionimin e një sistemi kompjuterik, nëpërmjet futjes, dëmtimit, shtrembërimit, ndryshimit, fshirjes apo suprimimit të të dhënave, dënohet me burgim nga tre deri në shtatë vjet. Kur kjo vepër kryhet në sistemet kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile, të shëndetësisë apo në çdo sistem tjetër kompjuterik, me rëndësi publike, dënohet me burgim nga pesë deri në pesëmbëdhjetë vjet. Në rastet kur veprimet e parashikuara në paragrafin e parë janë kryer nga një i mitur, ndaj tij do të zbatohen dispozitat e Kodit të Drejtësisë për të Mitur.

Neni 293/ç Keqpërdorimi i pajisjeve (Shtuar me ligjin nr. 10 023, datë 27.11.2008) Prodhimi, mbajtja, shitja, dhënia në përdorim, shpërndarja apo çdo veprim tjetër, për vënien në dispozicion të një pajisjeje, ku përfshihen edhe një program kompjuterik, një fjalëkalim kompjuterik, një kod hyrjeje apo një e dhënë e tillë e ngjashme, të cilat janë krijuar ose përshtatur për hyrjen në një sistem kompjuterik ose në një pjesë të tij, me qëllim kryerjen e veprave penale, të parashikuara në nenet 192/b, 293/a, 293/b e 293/c të këtij Kodi, dënohen me burgim nga gjashtë muaj deri në pesë vjet.

të drejtave të topografisë së qarkut të gjysmëpërçuesit".

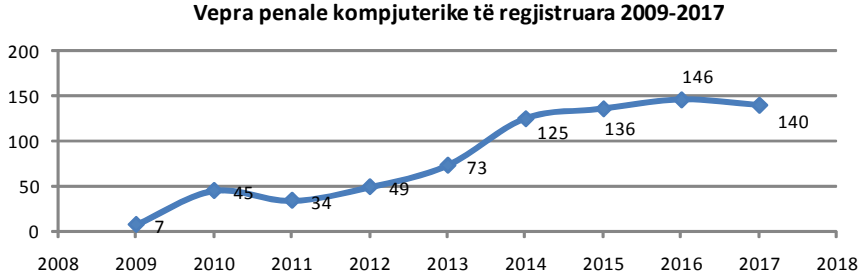
Përdoruesit e internetit në Shqipëri, nga viti 2000 deri në vitin 2016, janë rritur pothuajse 511 herë duke shkuar në vitin 2016 në 1 823 233 përdorues[12].

Tabela. Përdorues interneti në Shqipëri nga viti 2000 deri në vitin 2016



Rritja e madhe e përdoruesve të internetit në Shqipëri, është pothuajse e njëjtë me trendin botëror. Faktor i veçantë, që ka çuar në këtë rritje në Shqipëri, është edhe kalimi i shumë shërbimeve që më parë bëheshin pranë sporteleve në institucionet shtetërore, në shërbime *on-line* siç janë prokurimet publike, certifikatë personale dhe familjare, etj. Veprat penale kompjuterike nga viti 2003 deri në vitin 2017 janë rritur me 755 herë, pra pothuajse i njëjti numër i rritjes së përdoruesve të internetit në Shqipëri.

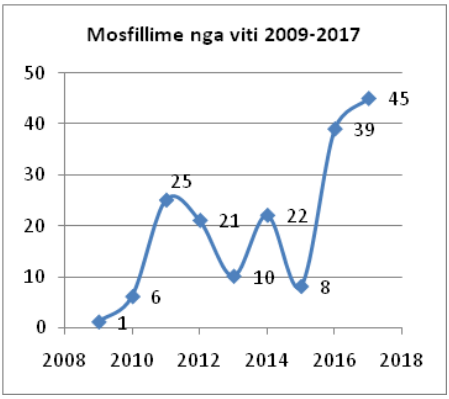
Vepra penale kompjuterike të regjistruara 2009-2017 [13]

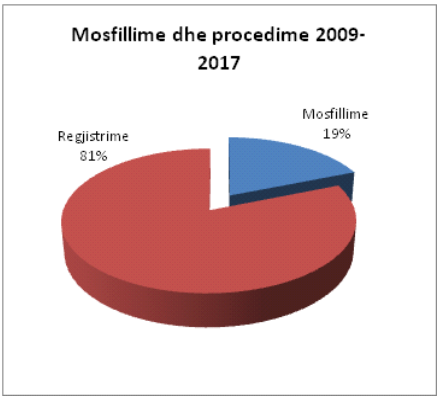


[12] http://www.internetlivestats.com/internet-users/albania/ aksesuar për herë të fundit datë 30.09.2018

[13] Në këtë shkrim janë studiuar treguesit statistikorë të Prokurorisë së Përgjithshme për veprat penale të parashikuar nga nenet 74/a; 84/a; 119/a; 119/b; 143/b; 186/a; 192/b; 293/a; 293/b; 293/c dhe 293/ç, pasi për veprat e tjera penale të përmendura në grupet e tjera ka vështirësi në identifikimin dhe ndarjen e tyre vetëm në sistemet kompjuterike.

Nga viti 2009 deri në vitin 2017 janë *mosfilluar* 177 procedime penale nga prokuroritë e rretheve gjyqësore në Shqipëri, që përbëjnë 19 % të totalit prej 822 referime dhe kallëzimeve në prokurori.





Në analizë të treguesve statistikor rezulton se numri më i madh i veprave penale kompjuterike e zënë vepra penale e "Mashtrimit kompjuterik " parashikuar nga neni 143/b të Kodit Penal. Pesha specifike që zë kjo vepër penale është 46 % e të gjithë veprave penale kompjuterike. Numri i lartë i kësaj vepre penale, lidhet me përdorimin, në Shqipëri, të kartave të kreditit të vjedhura nëpër botë. Këto karta krediti, pasi vidhen, shiten në shtete të ndryshme duke përfshirë edhe vendin tonë. Pasi klonohen, përdoren për të bërë pagesa në pika të ndryshme tregtare, duke sjell edhe përfitime të mëdha për autorët e këtyre veprave penale.

Prej disa kohësh në Shqipëri, është përhapur shumë ndërhyrja në komunikimet ndërmjet bizneseve vendase dhe atyre të huaja. Autorët e këtyre veprave penale, pasi kanë ndërhyrë në komunikimin elektronik, dërgojnë e-mail në biznesin shqiptar, duke ju dhënë udhëzime për transaksionin e radhës në një numër llogarie që ju përket këtyre autorëve. Hetimi i kësaj veprimtarie ka qenë shumë i vështirë dhe në shumë raste i pamundur për tu zbuluar autori. Për periudhën nga viti 2009 deri në vitin 2017 janë regjistruar gjithsej 347 vepra penale të "Mashtrimit kompjuterik " dhe janë pezulluar 303 procedime që zënë 87 % të gjithë regjistrimeve. Kjo tregon edhe një herë vështirësinë shumë të madhe të hetimit të kësaj vepre penale.

Në tabelën e mëposhtme, jepen të dhënat e për veprën penale të mashtrimit, në Itali[14], dhe të veprës penale të mashtrimit kompjuterik, në Shqipëri[15].

Viti	2010		2011		2012		2013		2014	
	Shqipëri	Itali	Shqipëri	Itali	Shqipëri	Itali	Shqipëri	Itali	Shqipëri	Itali
Vepra penale e mashtrimit (Truffe e frodi informatiche)	25	96442	24	105692	28	116767	31	140614	51	133261
Për 100 000 banorë	0,8	159,5	0,8	174,1	0,9	196,1	1,07	233,4	1,7	219,2

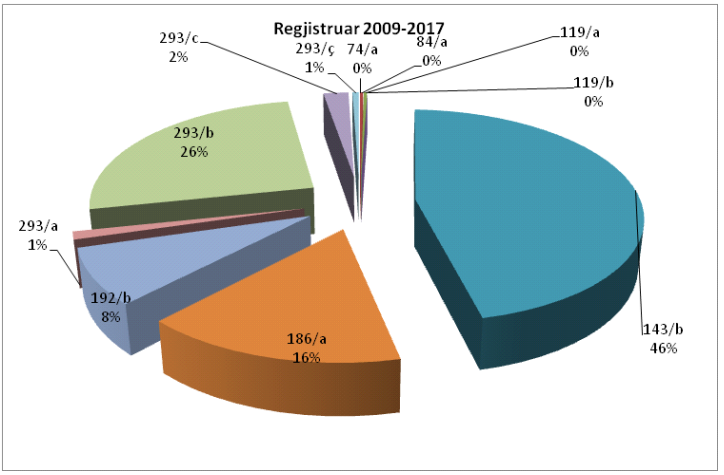
[14] https://www.istat.it/it/files/2017/10/Delitti-imputati-e-vittime-dei-reati.pdf
[15] http://www.instat.gov.al/al/temat/treguesit-demografik%C3%AB-dhe-social%C3%AB/popullsia/#tab2

Diferenca e madhe për 100 000 banor për këtë tregues ka shpjegim pasi interneti në Shqipëri në vitet në studim përdorej mesatarisht nga 45 % deri në 50 % të popullsisë ndërsa në Itali rreth 55 % deri në 60 % e popullsisë. Faktor tjetër që ndikon është edhe përdorimi disa herë më pak i hapësirës kibernetike për kryerjen e transaksioneve ekonomike në Shqipëri, krahasuar me Italinë.

Vepra e dytë penale që zë 26 % të totalit të veprave penale kompjuterike është ajo e parashikuar nga neni 292/b "Ndërhyrja në të dhënat kompjuterike". Kjo vepër penale është në këtë shkallë të lartë pasi lidhet me përdorimin e madh të rrjeteve sociale. Përdoruesit e këtyre rrjeteve në përgjithësi kanë qenë pre e sulmeve të autorëve të ndryshëm.

Kjo vepër, është e përhapur në këtë masë, pasi shumë përdoruesve të rrjeteve sociale u ndërhyhet në adresat e tyre, duke ua ndryshuar fjalëkalimet[16]. Këto vepra penale, në përgjithësi kryhen pa përfitim nga autorët e tyre dhe zakonisht, janë të rinj, me aftësi shumë të mira në fushën e teknologjisë së informacionit. Kjo vepër është shoqëruar në disa raste, edhe me kërkesën për pagesa, në shkëmbim të mos publikimit së të dhënave intime të përdoruesve të faqeve sociale[17].

Vepër penale, që zë 16 % të totalit të veprave penale kompjuterike, është edhe vepra penale e parashikuar nga neni 186/a, "Falsifikimi kompjuterik". Numri i lartë i kësaj vepre penale lidhet me paraqitjen e rrethanave të rreme ose false, në regjistra shtetërorë që janë të formës *online*. Kështu, kjo vepër penale, ka ndodhur nga shtetas të ndryshëm, duke falsifikuar të dhënat kompjuterike për pajisje me dokumente identiteti, hedhen në sistemin e OSHE-së nga punonjësit e kësaj ndërmarrje të të dhënave të rreme, të konsumit të klientëve të kësaj kompanie etj.



Veprat penale të parashikuar nga nenet 74/a dhe 119/a janë 0 nga viti 2009 deri në vitin 2017.

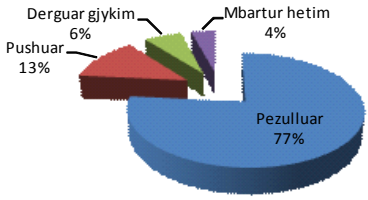
Numri i përgjithshëm i veprave penale të regjistruara si procedime penale, është 755. Nga këto procedime, në total, janë pezulluar 578 procedime, 98 janë pushuar dhe

[16] Vendimi numër 640 datë 02.03.2016, Gjykata e Shkallës së Parë Tiranë, me anë të cilit është shpallur fajtor i pandehuri I. SH. për veprën penale "Ndërhyrjen në të dhënat kompjuterike''parashikuara nga neni 293/b te K. Penal.

[17] Vendimi numër 2556 datë 14.10.2015 i Gjykatës së Lartë.

48 procedime janë dërguar për gjykim.

Tregues statistikorë të veprave penale kompjuterike



Pezullimet dhe pushimet e këtyre procedimeve zënë një numër shumë të lartë pasi hetimi i veprave penale kompjuterike është i lidhur me letër porosi në shtete të ndryshme. Përdorimi i sistemeve kompjuterike anonime[18] nga autorët e veprave penale kompjuterike, i ka bërë të pamundur edhe zbulimin e autorëve të tyre duke sjell një numër shumë të madh të pezullimeve të këtyre veprave penale.

Nga ana e organit të akuzës, janë dërguar për gjykim për periudhën 2009-2017, gjithsej, 99 të pandehur. Nga këta të pandehur, janë dërguar 48 të pandehur me masë sigurimi "arrest në burg". Nga këta të pandehur, 89 kanë qenë meshkuj dhe 10 të pandehur, femra. Tërheqja për të kryer krime në fushën kompjuterike ka bërë që në totalin e të pandehurve kanë qenë edhe 10 të mitur, nga mosha 14 deri në 18 vjeç.

Nga studimi i rasteve të ndodhura në Shqipëri, vlen të përmendet bashkëpunimi në goditjen e grupeve të cilat përfitonin nga përdorimi i kartave të kreditit të vjedhura, dhe më pas, të klonuara, duke proceduar dhe dënuar edhe shtetas të huaj[19], ose i grupeve, të cilët në mënyrë të padrejtë përfitonin shërbime të televizioneve me pagesë[20].

Në harkun kohor 2009-2017, konstatohet se për veprat penale të parashikuara nga nenet 192/b paragrafi 2, 293/a paragrafi 2 dhe 293/b paragrafi 2 dhe 293/c paragrafi 2, janë vetëm 2 vepra penale të regjistruara. Paragrafët e neneve që përmendëm, parashikojnë ndërhyrje në sistemet kompjuterike të infrastrukturës kritike, siç janë: "sistemet kompjuterike ushtarake, të sigurisë kombëtare, të rendit publik, të mbrojtjes civile, të shëndetësisë apo në çdo sistem tjetër kompjuterik, me rëndësi publike".

Nga puna e përditshme kemi konstatuar, se, shumë nga ndërhyrjet në sisteme kompjuterike, nuk kallëzohen në organet ligj zbatuese. Mos përdorimi i madh i sistemeve kompjuterike për kryerjen e transaksioneve ekonomike, është një faktor që ka mbajtur tregues kriminaliteti të ulët. Por, përveç këtyre faktorëve, nga ana e shtetit shqiptar janë ndërmarrë masa të rëndësishme legjislative dhe organizative, në drejtim të parandalimit dhe të goditjes së krimeve që lidhen me sistemet kompjuterike.

Institucionet shqiptare kanë konsideruar si rrezik për sigurinë kombëtare sulmet kibernetike. Në "Strategjinë e sigurisë kombëtare" të vitit 2014, është parashikuar se,

[18] Përdorimi i Proxy server, Tor etj.

[19] Vendimi numër 82 datë 17.01.2014, Gjykata e Shkallës së Parë Tiranë, me anë të cilit janë shpallur fajtor të pandehurit me shtetësi Malajzinë M.P dhe L.K për veprën penale të "Mashtrimit kompjuterike" parashikuar nga neni 143/b/2 i Kodit Penal ;
Vendimi numër 1213 datë 16.04.2015, Gjykata e shkallës së Parë Tiranë, me anë të cilit është shpallur fajtor i pandehuri kosovar Z.B për veprën penale "Mashtrimit kompjuteri " parashikuar nga neni 143/b/2 i Kodit Penal;
Vendimi numër 4639 datë 23.12.2015, Gjykata e shkallës së Parë Tiranë, me anë të cilit është shpallur fajtor i pandehuri me shtetësi turke S.B për veprën penale "Mashtrimit kompjuteri " parashikuar nga neni 143/b/2 i Kodit Penal.

[20] Vendimi numër 1112 datë 21.07.2010 Gjykata e Shkallës së Parë Tiranë.

Shqipëria është e ekspozuar *"...ndaj rreziqeve të natyrës kibernetike me aktorë shtetërorë dhe joshtetërorë. Sulmet kibernetike kanë potencial për të dëmtuar rëndë shkëmbimin e informacionit në institucionet publike, të telekomunikacionit dhe sistemin financiar e bankar, duke shkaktuar edhe ndërprerje të shërbimeve jetike...."*[21].

Me vendimin e Këshillit të Ministrave, numër 973, datë 2.12.2015, është miratuar "Dokumenti i politikave për sigurinë kibernetike 2015-2017", dokument mjaft i rëndësishëm për mbrojtjen nga sulmet kompjuterike me pasoja të rënda.

Republika e Shqipërisë, me ligjin nr. 8888, datë 25.4.2002, ka ratifikuar konventën për krimin në fushën e kibernetikës, ndërsa në vitin 2004 është ratifikuar edhe protokolli shtesë i kësaj konvente.

Për të reflektuar angazhimet e Shqipërisë në kuadër të konventës së krimit kibernetik, Ministria e Drejtësisë ndërmori nismën për parashikimin e shtesave, në Kodin Penal të Republikës së Shqipërisë dhe në Kodin e Procedurës Penale. Këto nisma u finalizuan respektivisht, me miratimin e ligjit nr. 10023, datë 27.11.2008 dhe ligjit nr. 10054, datë 29.12.2008.

Nenet e shtuara në Kodin Penal dhe në atë të Procedurës Penale, janë pothuajse parashikimet që ka bërë konventa për krimet kompjuterike.

Shteti shqiptar, në kuadër të luftës kundër krimeve kompjuterike, ka ndërmarrë masa shumë të rëndësishme organizative.

Kështu, në laboratorin e Policisë Shkencore është ngritur dhe funksionon me shumë sukses, sektori i ekspertimeve kompjuterike. Ky sektor e filloi punën e tij ne vitin 2009, me mbështetjen e strukturave homologe të policisë britanike dhe të asaj të Shteteve të Bashkuara të Amerikës; laboratori, është i pajisur me programe dhe pajisje bashkëkohore kompjuterike dhe aktet e ekspertimit që kryen, janë shumë cilësore.

Gjithashtu, edhe në Drejtorinë e Përgjithshme të Policisë, është krijuar një strukturë e specializuar për zbulimin, ndjekjen dhe hetimin e krimeve kompjuterike.

Drejtoria e Përgjithshme e Policisë, në bashkëpunim me struktura të specializuara homologe të vendeve të Evropës dhe SHBA-së, ka realizuar shumë kurse trajnimi në këtë fushë.

Gjithashtu, edhe në Prokurorinë e Përgjithshme, është krijuar një strukturë e specializuar vetëm për krimet kompjuterike. Në sistemin e trajnimeve vazhduese të prokurorëve dhe gjyqtarëve, prej vitit 2009, Shkolla e Magjistraturës ka bërë pjesë të programit të trajnimit vazhdues kurset për krimet kompjuterike, të cilët kanë rezultuar të domosdoshme.

Me anë të ligjit nr. 8457, datë 11.2.1999, "Për informacionin e klasifikuar *sekret shtetëror*", i ndryshuar me ligjin nr. 9541, datë 22.5.2006 "Për disa shtesa e ndryshime në ligjin nr. 8457, datë 11.2.1999 "Për informacionin e klasifikuar *sekret shtetëror*" ", është krijuar në Shqipëri "Drejtoria e Sigurimit të Informacionit të Klasifikuar" (DSIK). Një ndër detyrat kryesore të kësaj drejtorie, është edhe certifikimi i sistemeve kompjuterike që lidhen me sigurinë kombëtare[22].

[21] Strategjia e sigurisë Kombëtare 2014-2014 faqe 23.

[22] Neni 6

... b) aftësi apo dobësi, kapacitete të sistemeve, instalimeve, projekteve dhe planeve që kanë të bëjnë me sigurinë kombëtare;

c) veprimtari të shërbimeve informative, me forma dhe metoda të punës, me kriptologji në objektet e mjetet teknike, në vendet ku përpunohet dhe në arkivat ku ruhet informacioni;

Neni 25

2. Mbikëqyr rregullat e sigurimit fizik, ushtarak dhe elektronik të informacionit të klasifikuar, si dhe të anës teknike të marrjes, përpunimit, administrimit dhe arkivimit të tyre.

4. Konkluzione

Duke e konsideruar hapësirën kibernetike, si një formë të re të jurisprudencës ndërkombëtare, por kritike për pothuajse çdo vend në botë, është i nevojshëm edhe ndryshimi i koncepteve mbi territorin dhe juridiksionin e lidhur me këtë hapësirë. Organizatat ndërkombëtare, në veçanti Kombet e Bashkuara, duhet të përgatisin për miratim konventa ndërkombëtare për unifikimin e ligjeve të aplikuara në hapësirën kibernetike. Po në këtë kuadër, krijimi i institucioneve të drejtësisë, prokurori dhe gjykata, me juridiksion ndërkombëtar do të parandalonte dhe do të lehtësonte hetimin e krimeve në fushën kompjuterike. Shteti shqiptar ka ndërmarrë masa organizative dhe legjislative të rëndësishme, në parandalimin dhe goditjen e krimeve kompjuterike. Teknologjia ecën me ritme shumë të shpejta dhe kjo gjë kërkon që legjislacioni dhe strukturat përkatëse shqiptare, të jenë të përditësuara me situata e reja për një përgjigje efikase ndaj kërcënimeve kibernetike. Kjo kërkon specializime të strukturave përkatëse ligjzbatuese, por edhe fuqizimin e këtyre strukturave me teknologjinë e përditësuar në fushën e krimeve kompjuterike. Në këtë kuadër, duhet të bëhet edhe një ndërgjegjësim më i madh i përdoruesve të teknologjisë, që ndërhyrjet në sistemet kompjuterike, janë parashikuar si krime në kodin penal dhe për këtë arsye, ato duhet të denoncohen dhe të ndiqen ligjërisht, siç bëhet për çdo vepër tjetër penale të parashikuar nga legjislacioni penal.

Bibliografi

1. Nenet 76 dhe 77 të Kodit të Procedurës Shqiptare përcaktojnë rregullat e kompetencës tokësore.
2. Vendimi nr 40303 datë 27.09.2013 i Seksionit penal të Gjykatës së Kasacionit Itali.
3. Vendimi Unifikues Nr. 17325 datë 24.04.2015 i Gjykatës së Kasacionit Itali.
4. Ligji nr. 10128, datë 11.5.2009 "Për tregtinë elektronike" i ndryshuar me Ligjin Nr. 135/2013 "Për disa shtesa dhe ndryshime në ligjin nr. 10128, datë 11.5.2009 "Për tregtinë elektronike".
5. Traktati mbi parimet që drejtojnë veprimtaritë e shteteve në eksplorimin dhe përdorimin e hapësirës së jashtme, duke përfshirë hënën dhe trupa të tjerë qiellore, 27 janar 1967.
6. Statuti i Romës për Gjykatën Penale Ndërkombëtare i miratuar nga Konferenca Diplomatike e të Plotfuqishmëve në Kombet e Bashkuara për themelimin e Gjykatës Ndërkombëtare Penale më 17 korrik 1998, hyrë në fuqi më datë 1 korrik 2002. Ratifikuar nga Shqipëria me ligjin Nr. 8984, datë 23.12.2002 "Për ratifikimin e statutit të Romës për Gjykatën Ndërkombëtare Penale".
7. Neni 4 "Statusi ligjor dhe kompetenca e Gjykatës" i Statusit të Romës për Gjykatën Penale Ndërkombëtare.
8. Neni 192/b "Ndërhyrja në transmetimet kompjuterike Ndërhyrja në çdo formë, në transmetimet dhe programet kompjuterike, përbën kundërvajtje penale dhe dënohet me gjobë ose me burgim gjer në tre vjet. Po kjo vepër, kur ka sjellë pasoja të rënda, dënohet me burgim gjer në shtatë vjet."
9. Neni 192/b Hyrja e paautorizuar kompjuterike (Shtuar me ligjin nr. 8733, datë 24.1.2001; ndryshuar me ligjin nr. 8686, datë 26.2.2007; ndryshuar me ligjin nr. 10 023, datë 27.11.2008).
10. Neni 293/a Përgjimi i paligjshëm i të dhënave kompjuterike (Shtuar me ligjin nr. 10 023, datë 27.11.2008).
11. Neni 293/b Ndërhyrja në të dhënat kompjuterike (Shtuar me ligjin nr. 10 023, datë 27.11.2008; shtuar paragrafi i tretë me ligjin nr. 36/2017, datë 30.3.2017).
12. Neni 293/c Ndërhyrja në sistemet kompjuterike (Shtuar me ligjin nr. 10 023, datë 27.11.2008; ndryshuar me ligjin nr. 36/2017, datë 30.3.2017).
13. http://www.internetlivestats.com/internet-users/albania/ aksesuar për herë të fundit datë 30.09.2018
14. Treguesit statistikorë të Prokurorisë së Përgjithshme për veprat penale të parashikuar nga nenet 74/a; 84/a; 119/a; 119/b; 143/b; 186/a; 192/b; 293/a; 293/b; 293/c dhe 293/ç, pasi për veprat e tjera penale të përmendura në grupet e tjera ka vështirësi në identifikimin dhe ndarjen e tyre vetëm në sistemet kompjuterike.
15. https://www.istat.it/it/files/2017/10/Delitti-imputati-e-vittime-dei-reati.pdf

16. http://www.instat.gov.al/al/temat/treguesit-demografik%C3%AB-dhe-social%C3%AB/popullsia/#tab2
17. Vendimi numër 640 datë 02.03.2016, Gjykata e Shkallës së Parë Tiranë, me anë të cilit është shpallur fajtor i pandehuri I.SH. për veprën penale "Ndërhyrjen në të dhënat kompjuterike''parashikuara nga neni 293/b te K. Penal.
18. Vendimi numër 2556 datë 14.10.2015 i Gjykatës së Lartë.
19. Vendimi numër 82 datë 17.01.2014, Gjykata e Shkallës së Parë Tiranë, me anë të cilit janë shpallur fajtor të pandehurit me shtetësi Malajzinë M.P dhe L.K për veprën penale të "Mashtrimit kompjuterike" parashikuar nga neni 143/b/2 i Kodit Penal.
20. Vendimi numër 1213 datë 16.04.2015, Gjykata e shkallës së Parë Tiranë, me anë të cilit është shpallur fajtor i pandehuri kosovar Z.B për veprën penale "Mashtrimit kompjuteri " parashikuar nga neni 143/b/2 i Kodit Penal; Vendimi numër 4639 datë 23.12.2015, Gjykata e shkallës së Parë Tiranë, me anë të cilit është shpallur fajtor i pandehuri me shtetësi turke S.B për veprën penale "Mashtrimit kompjuteri " parashikuar nga neni 143/b/2 i Kodit Penal.
21. Vendimi numër 1112 datë 21.07.2010 Gjykata e Shkallës së Parë Tiranë.
22. Strategjia e sigurisë Kombëtare 2014-2014.

Hetimi kibernetik i burimeve të hapura - impakti në sigurinë kombëtare

■**Dr. Hergis JICA***
Drejtoria e Përgjithshme e Policisë së Shtetit
hergis.jica@asp.gov.al

Abstrakt

Institucionet e zbatimit të ligjit kanë si rol kryesor ruajtjen e rendit, zbatimin e ligjit, mbrojtjen e qytetarëve si dhe parandalimin, zbulimin dhe hetimin e krimit. Hetimi i burimeve të hapura mund të ofrojë aftësi të rëndësishme për institucionet e zbatimit të ligjit dhe shërbimet e sigurisë për të plotësuar dhe përmirësuar aftësitë e tyre të hetimit, pasi aftësia për të mbledhur me shpejtësi dhe për të përpunuar, dokumentuar dhe analizuar saktë të dhënat e burimeve të hapura mund të jetë një ndihmë e rëndësishme gjatë hetimeve dhe të përdoret për planifikimin strategjik në nivel kombëtar për të luftuar krimin. Monitorimi i rrjetit në mënyrë të qëllimshme dhe ligjore e më pas analizimi dhe paraqitja e të dhënave të përfituara nga burimet e hapura duhet të konsiderohet si kërkesë e detyrueshme për çdo strategji të sigurisë kombëtare. Institucionet e zbatimit të ligjit në të njëjtën kohë duhet të marrin në konsideratë bashkëpunimet me partnerët publikë dhe privatë duke përfshirë dhe duke përdorur implementimin e strukturave, pajisjeve dhe metodave të reja për kërkime të të dhënave në rrjet me qëllim sigurinë dhe mbrojtjen e qytetarëve. Hetimi i burimeve të hapura ka fituar një rëndësi të konsiderueshme në vitet e fundit. Tradicionalisht, informacioni dhe marrja e tij, ka qenë metoda e zbulimit të sekreteve duke përdorur një sistem të mbyllur të grumbullimit dhe analizimit. Edhe pse burimet e hapura janë përdorur shpesh në procesin e mbledhjes së informacionit, vlera e tyre është parë gjithmonë si e "mesme". Informacioni i klasifikuar është vlerësuar gjithnjë si më i vlefshëm dhe si më i besueshëm. Përvetësimi sistematik dhe përdorimi i informacionit jo të klasifikuar, rrallë shihej si një prioritet i inteligjencës, por, sot, rëndësia e hetimit të burimeve të hapura, është pranuar gjerësisht. Sot, vlerësohet se hetimi i burimeve të hapura, ofron mbi 90% të informacionit të përdorur nga institucionet ligjzbatuese, por dhe me një vlerë të padiskutueshme në aspektet e sigurisë kombëtare.

Fjalëkyçe:
burime, siguri, kibernetike, informacion, hetim, kombëtare

* *Sektori për hetimin e krimeve kompjuterike.*

1. Burimet e hapura

Rëndësia e hetimit të burimeve të hapura është rritur gjatë viteve të fundit. Për komunitetin e hetimeve tradicionale, hetimi i burimeve të hapura ka të ngjarë të mbetet një përbërës i tërësisë së të gjithë burimeve që përfshijnë burimet e klasifikuara. Megjithatë, për shumicën e agjencive qeveritare, hetimi i burimeve të hapura është e vetmja pjesë e informacionit që ata mund të kenë një qasje të lehtë dhe në shumë raste të pakufizuar, gjë që e bën atë një mundësi konkrete dhe strategjike për vendimmarrjen dhe krijimin e politikave. Konsiderimi i saj në formën e duhur për formulimin e një strategjie kombëtare për hetimin e burimeve të hapura dhe krijimin e një strukture brenda krimit kibernetik për hetimin e këtyre burimeve do të lejonin shfrytëzimin efektiv të informacionit të përfituar nga këto burime.

Informacioni i përfituar nga burimet e hapura ka fituar një rëndësi të konsiderueshme në vitet e fundit. Tradicionalisht, përdorimi i informacionit të kualifikuar ka qenë dhe është duke përdorur një sistem të mbyllur të mbledhjes dhe analizës. Burimet kyçe përfshinin inteligjencën njerëzore, inteligjencën e sinjaleve por dhe inteligjencën e imazheve. Edhe pse burimet e hapura janë përdorur shpesh në procesin e inteligjencës, vlera e tyre shihej si e mesme dhe për këtë mund të themi që në shumë procese dhe sot, akoma shihet si e tillë. Informacioni i klasifikuar në formën tradicionale vlerësohet më i vlefshëm dhe shpesh më i besueshëm për fillimin dhe vazhdimin e hetimeve. Përvetësimi sistematik i informacionit jo të klasifikuar rrallë shihej si një prioritet i inteligjencës por dhe sot ndryshimi është shumë i vogël për sa i përket ndryshimit të këtij koncepti. Gjithashtu informacioni i pa klasifikuar shpeshherë nuk konsiderohet vendimtar për fillimin e hetimeve, gjë e cila në shumë raste nuk është e vërtetë.

Sot, kudo në botë, rëndësia e marrjes së informacionit nga burimet e hapura po

pranohet gjerësisht. Vlerësohet se informacioni i marrë nga burimet e hapura përbën pjesën më të madhe të informacionit të përdorur nga komuniteti i inteligjencës. Kjo ndodh për shkak se ne rrethohemi nga informacioni mjafton që të tregohemi të vëmendshëm në atë që kërkojmë si dhe të përdorim mënyrat e duhura për mbledhjen dhe analizimin e tij.

Ekziston një debat në rritje, brenda dhe ndërmjet degëve të ndryshme të qeverisë, por edhe strukturave të sigurisë kombëtare, për mënyrën e përdorimit të informacionit nga burimet e hapura. Sidoqoftë, roli dhe potenciali i informacionit të burimeve të hapura mbetet një çështje e cila u jep rrugë disa mosmarrëveshjeve. Mbrojtësit e informacionit të marrë nga burimet e hapura, besojnë se kjo është përgjigja e shumë prej sfidave të sotme të inteligjencës. Ata bëjnë thirrje për një paradigmë të re të inteligjencës, e cila do të mbizotërohet nga informacioni i burimeve të hapura, por dhe nga një bashkëpunim ndërsektorial i inteligjencës, që përfshin një rrjet të gjerë të aktorëve publik dhe privatë. Por, ka të tjerë që paralajmërojnë se kjo do të sillte një dëm të madh, tek të gjitha burimet e tjera për mbledhjen e informacionit, si dhe në analizën e mëtejshme të tyre.

2. Stërvitja "Burundi", "Komisioni Aspin-Brown"[1]

Por, që të kuptojmë se sa i rëndësishëm mund të bëhet hetimi i informacioneve të marra nga burimet e hapura, le të shohim ushtrimin "Burundi"[2], në mënyrë të përmbledhur. Incidenti që fillimisht çoi në themelimin e *Komisionit Aspin-Brown*, në vitin 1994, ishte përplasja ushtarake në Mogadishu të Somalisë, në muajin tetor të vitit 1993, në të cilin ushtarët e një komandanti luftëtarësh somalez, vranë 18 ushtarë të Forcave Speciale të SHBA-së. Trupat amerikane u befasuan nga fuqia e zjarrit dhe vendosmëria e forcave somaleze dhe në të njëjtën kohë, amerikanët u tronditën nga shfaqja televizive poshtëruese, me ushtarët e vrarë në qytet, por kjo tragjedi vazhdoi me një dështim tjetër të inteligjencës: me shpërthimin e eksplozivëve në bazë të Qendrës Botërore të Tregtisë, në shkurt të atij viti, i cili ishte një sulm terrorist.

Robert Steele, një ish-oficer i CIA-s dhe mbështetës i inteligjencës nga burimet e hapura, dëshmoi para Komisionit Aspin-Brown, rreth vlerës së jashtëzakonshme të informacionit të paklasifikuar. Komisioni vendosi ta testonte dhe udhëzoi që Steele, dhe rrjeti i tij i kontakteve të inteligjencës tregtare, të përballeshin me komunitetin e fshehtë të inteligjencës (CIA), në një betejë informacioni ku subjekti do të ishte pikërisht "Burundi".

Testimi filloi në ora 17:00, ditë e enjte, dhe afati i përfundimit ishte ora 10:00 i të hënës së ardhshme.

Të hënën në mëngjes, Steele paraqiti:

- emrat e 10 gazetarëve kryesorë që mbulonin Burundin;
- emrat e 10 akademikëve kryesorë që mbulonin Burundin;
- 22 përmbledhje politiko-ushtarake në nivel ekzekutiv për Burundin;
- informacionin për urdhrat e betejës, në nivelin fisnor Burundi;
- lista lufte ushtarake ruse, harta të vendit të shkallës 1:50, si dhe imazhet e paarkivuara të vendit që ishin më pak se 3 vjeçare.

[1] https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no3/article01.html#author1

[2] Burundi bën pjesë në vendet e Afrikës dhe ndodhet në pjesën qendrore të saj. Burundi është një ndër vendet më të varfra të botës.

CIA[3] u paraqit me :

- një tabelë *PowerPoint* me vlera nominale;
- një studim ekonomik rajonal, jo për vendin.

Imazhi që u krijua ishte që me informacionin e Steele mund të kryej një operacion joluftarak në Burundi, por nga ana tjetër, në bazë të asaj që ofroi CIA askush nuk mund të shkonte në Burundi.

3. Koncepti i burimeve të hapura

Për të kuptuar debatin për mbledhjen e informacionit nga burimet e hapura, është e rëndësishme që së pari të përcaktohet koncepti. Për këtë është e nevojshme që ne të ngremë pyetjen:

- Çfarë është informacioni i marrë nga burimet e hapura?

Nuk është asgjë tjetër, përveçse është një e dhënë e mbledhur nga burimet e disponueshme, me qëllim përmbushjen e kërkesave specifike të inteligjencës. Këto burime mund të jenë të lira ose të bazuara në regjistrime përkatëse, brenda ose jashtë një drejtimi të caktuar. Ky informacion nuk është i kufizuar vetëm në internet, megjithëse në internet gjendet një vëllim në rritje i informacionit të vlefshëm, kjo për shkak të qasjes dhe shpërndarjes së lehtë. Mediet, agjencitë publike, universitetet, organizatat e ndryshme jofitimprurëse si dhe sektori privat përbëjnë burime të hapura informacioni. Evolucioni i debatit mbi informacionin e marrë nga burimet e hapura mund t'i atribuohet disa faktorëve kryesorë.

Faktor kryesor, është zgjerimi problematikave të sigurisë gjatë dy dekadave të fundit. Pas Luftës së Dytë Botërore, shërbimet e inteligjencës filluan të kishin shqetësime për një numër të kufizuar sfidash, kryesisht qendrore, si p.sh., ndarja e shteteve në dy blloqe (perëndim-lindje) do të çonte që zbulimi i qëllimeve dhe aftësive të një blloku, do të ishte detyra kryesore e komunitetit të inteligjencës të bllokut tjetër. Pas kalimit të këtij rreziku (vitet 1990), këto kërcënime janë shumëfishuar dhe janë bërë më të larmishme sa i përket natyrës së tyre. Kjo sjell shumëllojshmëri çështjesh duke u zgjeruar në mënyrë dramatike, dhe agjencitë e inteligjencës duhet të krijojnë strategji dhe forma të reja, për tu marrë me to. Sot çështjet e reja, përfshijnë, ndër të tjera, terrorizmin, përhapjen e armëve të shkatërrimit në masë, krimin e organizuar, konfliktet brenda shtetit apo shteteve, emigracionin e paligjshëm, sigurinë e energjisë etj. Shumë agjenci qeveritare kanë pasur shqetësim kryesor zgjerimin e fushës së veprimit të tyre, për sa i përket sigurisë, dhe kanë shfaqur si problem kryesor kërkesën për më shumë informacion; dhe kjo kërkesë, nga ana e tjetër, ka nxitur një vlerësim në rritje të vlerës dhe dobisë së informacionit të marrë nga burimet e hapura.

Një faktor tjetër është teknologjia. Evolucioni i internetit dhe shfaqja e rrjetit të ndërlidhur, ka shqetësuar këdo që merret me sigurinë dhe hetimin e krimit nëpërmjet kompjuterit të cilët potencialin e mjeteve të reja e shohin si "armë" ndaj çështjeve të sigurisë kombëtare, të cilat janë dhe çështjet me nivelin më të lartë të rrezikshmërisë dhe teknologjinë për mbledhjen, analizimin dhe shpërndarjen e njohurive si një mjet i cili është shumë vështirë për tu kontrolluar. Përhapja e faqeve të internetit, portaleve të ndryshme etj., ka hapur derën e një bote të re, e cila përmban informacion deri tani të paarritshëm për shumicën e profesionistëve të inteligjencës; P.sh, *Google Earth* ofron

[3] CIA (Central Intelligence Agency), Agjencia Qendrore e Inteligjencës së Shteteve të Bashkuara të Amerikës.

më shumë informacion sesa ishte në dispozicion më pak se një dekadë më parë. Edhe shërbimet si: *Wikipedia*, gjithnjë e më shumë po citohen si burime të inteligjencës, kjo për faktin se informacioni i hedhur po bëhet gjithnjë e më i plotë dhe personat që e përdorin janë gjithnjë e më të shumtë. Por, gjithashtu, në internet mund të gjesh dhe faqe të cilat ofrojnë inteligjencë tregtare, gjë e cila më parë nuk mund të mendohej se mund të merrej në këtë lloj forme. Falë, revolucionit të informacionit, komuniteti tradicional i inteligjencës nuk ka më monopol mbi mënyrën apo aftësitë për të marrë informacionin e nevojshëm, me qëllim analizimin ose adresimin mbi kërcënimet e sotme të sigurisë.

Dështimet e inteligjencës në vende të ndryshme të botës kanë shtyrë aktorët e çështjeve të sigurisë të vlerësojnë çdo lloj informacioni, duke mos e konsideruar të rëndësishme mënyrën se si përfitohet ai. Gjithashtu, këto dështime kanë nxitur në shumë vende, një rivlerësim të plotë të mënyrës se si merret dhe si përdoret inteligjenca, për të formuar procesin e hartimit të politikave. Pra, nevoja që komuniteti i inteligjencës të përdorë më shumë informacionin e burimeve të hapura, është tashmë evidente, por kjo, nuk do të thotë që ky informacion nuk duhet verifikuar apo nuk duhet krahasuar, me informacione të marra nga burimet e kualifikuara me qëllim nxjerrjen e konkluzioneve përfundimtare.

4. Përfitimet nga burimet e hapura

Mbrojtësit e burimeve të hapura janë të prirë për të nxjerrë në pah përfitimet e tyre dhe një nga përfitimet kryesore, është çështja e kostos. Përdorimi i burimeve të hapura është shumë më pak i shtrenjtë se mbledhja e informacionit nëpërmjet burimeve të klasifikuara. Për shembull, një burim i vlefshëm i inteligjencës njerëzore janë hulumtuesit dhe gazetarët të cilët punojnë në fushën e informacionit. Inteligjenca e komunikimit, e cila është shumë e dobishme mund të gjendet në shumë bloge, forume të dedikuara për çështjet kombëtare apo ndërkombëtare, por dhe në faqet e çdo gazete cilësore. Inteligjenca e imazheve të cilësisë së lartë është në dispozicion të lirë nga "Google Earth", por dhe shërbime të ngjashme. Fakti që informacioni i mbledhur nga burimet e hapura, nuk kërkon kosto sa mund të kërkonte përdorimi i një burimi të klasifikuar, është veçanërisht i rëndësishëm për vendet që veprojnë me buxhete të pamjaftueshme. Por, Inteligjenca e burimeve të hapura, gjithashtu, ka dhe përparësi të tjera, të mëdha të cilat janë të preferueshme nga çdo agjenci inteligjence.

E para dhe më kryesorja, ajo është e ndashme duke mos krijuar probleme në lidhje me çështjen e sekretit të informacionit të marrë nga burimet e kualifikuara. Informacioni i mbledhur nga një organizatë mund t'i jepet një tjetri me pak ose pa kosto.

Së dyti, informacioni i mbledhur duke përdorur mjete teknike, mund të përdoret në procedurat ligjore pa rrezikuar ekspozimin e aseteve të ndjeshme të inteligjencës siç janë burimet e kualifikuara të informacionit. Në të vërtetë, informacioni i marrë nga burimet e hapura, pothuajse nuk ka rrezik, krahasuar me operacionet e inteligjencës tek të cilat duhen përdorur informatorë apo asete të tjera për përfitimin e inteligjencës.

Së treti, informacioni i burimeve e hapura mund të merret, shfrytëzohet dhe më pas të transmetohet për përdorim të gjerë, duke përcjellë në mënyrë të menjëhershme një informacion i cili nuk ka nevojë të klasifikohet.

Së katërti, informacioni i mbledhur nga burime publike të rëndësishme dhe serioze në fushën e tyre, mund të përdoret për të informuar publikun për kërcënimet serioze

ndaj sigurisë kombëtare.

Së pesti, dhe ndoshta më e rëndësishmja, është se nëpërmjet informacionit të burimeve të hapura dhe hetimit të tyre, sigurohet një kontekst dhe ndërgjegjësim që është kritik për të kuptuar axhendën globale të sigurisë. Kompleksiteti në rritje dhe ndërlidhja e botës sonë, kanë bërë që niveli i sigurisë dhe parashikueshmërisë të jetë në rënie, dhe në këtë mënyrë, rëndësia e skanimit të gjithçkaje dhe vlerësimit afatgjatë të inteligjencës strategjike që merret me njohjen e burimeve dhe disiplinave të shumëfishta, bëhet gjithmonë e më i rëndësishëm.

5. Kufizimet dhe dobësitë

Inteligjenca e burimeve të hapura nuk është pa kufizimet e saj. Për agjencitë tradicionale të inteligjencës, burimet e hapura, nuk kanë gjasa të ofrojnë zgjidhje të plotë për nevojat e informacionit pasi jo gjithçka ekziston në mënyrë të hapur. Gjithashtu ka të ngjarë që të përbëjë në disa raste dhe një problem me të cilin duhet të përballen, siç është mbingarkesa e informacionit, por dhe informacioni i panevojshëm. Ndarja e "informacioneve" nga "jo-informacionet" bëhet gjithnjë e më e vështirë dhe konsumon kohë e cila është shumë e rëndësishme.

Megjithëse shumë programues nxjerrin programe të cilat në vetvete tregojnë se mund të përdoren për të kryer këtë filtrim kaq të nevojshëm, ato, nuk mund të zëvendësojnë analizimin e këtij informacioni nga qeniet njerëzore, pra nga punonjësit e inteligjencës. Për më tepër, fakti që agjencitë e shumta të lajmeve raportojnë një ngjarje, mund të mos e bëjnë atë të saktë apo të vërtetë në vetvete, gjithashtu dhe vetë aktorë shtetërorë, qeveritarë apo dhe aktorët joshtetërorë mund të përdorin burime të hapura informacioni për të transmetuar të dhëna të pasakta ose mashtruese. Pra, në raste të caktuara informacioni i marrë nga burime të hapura duhet të verifikohet edhe nga burime të klasifikuara.

Dobia e burimeve të hapura nuk shtrihet gjithmonë në sigurimin e inteligjencës së zbatueshme, në nivelin taktik ose operativ. Për shembull, ndërkohë që një burim i hapur mund të sigurojë një sasi të bollshme informacioni mbi kërkesat dhe motivimet e një grupi terrorist, nga krahu tjetër, nuk do të zbulojë domosdoshmërish vendndodhjen e saktë të kreut të këtij grupi terrorist ose të japë informacion taktik të nevojshëm për ta kapur atë. Ndërsa grupet terroriste, por dhe organizatat kriminale të krimit të organizuar bëhen gjithmonë e më të vetëdijshëm, se sa e rëndësishme është gjurma e tyre dixhitale, dhe për këtë, ata gjithmonë e më shumë kërkojnë mënyra të reja për të qëndruar jashtë kësaj linje, si dhe të qëndrojnë poshtë "radarit".

6. Përshtatja e burimeve të hapura sipas nevojave

Dy vlerësime mund të nxirren nga sa më sipër, të cilat do të na ndihmojnë të kuptojmë përshtatjen e burimeve të hapura sipas nevojave.

Së pari, përdorimi strategjik i burimeve të hapura është i domosdoshëm, i realizueshëm dhe premtues.

Së dyti, burime të hapura do të thotë gjëra të ndryshme për njerëz të ndryshëm.

Për komunitetin tradicional të inteligjencës, burimet e hapura ka të ngjarë të mbeten një komponent i një kapaciteti mbledhës të informacionit, që përfshin burime klandestine dhe kjo bën të qartë se proceset tradicionale të inteligjencës, do të duhet të përmirësohen

më tej, për të përdorur më mirë burimet e hapura. Megjithatë, për shumicën e agjencive qeveritare, burimi i hapur është e vetmja inteligjencë që ata mund të kenë qasje. Ai është vendi i vetëm, ku ata mund të kenë mundësinë të marrin informacion, i cili do të ishte dhe një mundësues strategjik i politikës dhe vendimmarrjes së mëtejshme. Por, brenda komunitetit të inteligjencës tradicionale, ajo që kërkohet më së shumti është një ndryshim i mentalitetit të mëparshëm, dhe kjo, kërkon njerëz të cilët të jenë të hapur për forma të reja të inteligjencës, por edhe të jenë të aftë të përdorin dhe të kuptojnë rëndësinë dhe përdorimin e informacionit. Shumë analistë, veçanërisht ata të cilët kanë punuar një kohë të gjatë me formën tradicionale të informacionit, por dhe ata që nuk kanë pasur të bëjnë me informacionin, vazhdojnë të jenë të njëanshëm ndaj burimeve të hapura dhe refuzojnë të pranojnë vlerën e tyre.

Shumë herë, informacioni i mbledhur nga burimet e hapura arkivohet në mënyrë tradicionale, duke marrë nivel klasifikimi të njëjtë me atë të informacionit të marrë nga burime konfidenciale, dhe duke vepruar kështu në mënyrë të pavetëdijshme, kufizojnë dobinë e tij. Gjithashtu, një numër agjencish të inteligjencës kufizon qasjen e stafit të tyre në internet për shkaqe sigurie, gjë e cila absolutisht duhet parë në një këndvështrim tjetër, p.sh. duke krijuar procese të cilat nuk kufizojnë, por kontrollojnë veprimtarinë etj.

Për të qenë efektiv, komuniteti i inteligjencës do të duhet të investojë më shumë në zhvillimin e kapaciteteve të burimeve të hapura. Një hap i parë do të ishte përmirësimi i trajnimeve dhe afrimi i studiuesve dhe analistëve të ngarkuar me gjetjen dhe shfrytëzimin e burimeve të hapura të informacionit. Përmirësimi i aftësive gjuhësore, është gjithashtu me rëndësi vitale, pasi inteligjenca më e vlefshme është shpesh në një gjuhë tjetër nga ajo e folur në zyrë apo rreth ambientit ku ne jetojmë. Gjithashtu, është i nevojshëm investimi shtesë në pajisje dhe mjete, që edhe nëse nuk ka gjasa të ofrojë zgjidhjen e çdo problemi, do të jetë ndihmues; por, edhe për sfidën e mbingarkesës në informacion, do të mund të përdoreshin, duke lehtësuar procesin.

Duke kërkuar përtej nevojave të komunitetit të inteligjencës për informacionin e marrë nga burime të hapura, sfida është dhe më e madhe. Personat apo strukturat përgjegjëse për krijimin e strukturave të reja, duhet të shmangin zgjidhjet specifike apo propozimet e paanalizuara, që çojnë në eliminim të strukturave ekzistuese ose në një dyfishim të tyre, në mënyrë të panevojshme. Përpjekjet, në këtë lloj forme, do krijonin një sistem të pakoordinuar ku do të përfshiheshin edhe kontrata të jashtme, por dhe marrëveshje ndërmjet partnerëve të cilat jo vetëm nuk do ishin efektive, por do të krijonin një situatë edhe më të vështirë. Për të mos kryer veprime të cilat do të krijonin situata të turbullta dhe pa rendiment, do të duhej një strategji gjithëpërfshirëse që adreson disa sfida themelore, të cilat mund të ishin:

- Si duhet ndërtuar një organizatë e aftë për të shfrytëzuar inteligjencën kolektive të mijëra burimeve të ndryshme?

- Si mund të anashkalosh në mënyrë efektive informacionet e shumta, dhe të inkurajosh në të njëjtën kohë, më shumë njohuri dhe bashkëpunim?

- Ku mund të gjenden brenda organizatës, por edhe jashtë saj, në raste specifike, njerëz të aftë që të mendojnë dhe të punojnë në disiplina të ndryshme, duke mos krijuar hapësira boshe?

- Si mund të menaxhohet në mënyrë efektive evolucioni i shpejtë i teknologjisë, duke mos krijuar distanca thelbësore?

- Cilat politika dhe procese mund të krijohen, apo të shtyhen më para, për të rritur

efektivitetin operativ dhe teknologjik?

Gjithashtu, mund të ngremë edhe pyetje të tjera, por është e sigurt që për asnjë nga këto pyetje nuk do të kishte përgjigje të lehta. Që të kemi përgjigje për këto pyetje, është e nevojshme që ekspertë të hetimit, mbledhjes dhe analizimit të informacionit etj., si dhe aktorë politikë që kanë në dorë legjislativin, por edhe buxhetin, të bëhen bashkë dhe të kërkojnë me vullnet zgjidhje optimale.

7. Vlerat e një qendre për burimet e hapura

Një mënyrë për të ecur përpara do të ishte krijimi i një strukture që do të fokusohej tek burimet e hapura, dhe e cila do të ishte e detyruar të ofronte informacionin e marrë në të gjitha degët e qeverisë dhe në të njëjtën kohë të koordinojë me burimet e klasifikuara. Një strukturë e tillë mund të vendoset brenda një kuadri ekzistues të sigurisë kombëtare dhe ajo që është më e rëndësishmja, është që duhet të mbetet e pavarur nga ndikimi i ndonjë departamenti qeveritar.

Një strukturë e tillë mund të ngarkohet me mbështetjen e të gjitha shërbimeve, qofshin ato sekrete apo jo; të evidentojë zhvillimet e reja në teknologjinë e informacionit dhe tu sigurojë agjencive qeveritare mjetet dhe teknologjitë më të përshtatshme, për të shfrytëzuar informacionin, por dhe të informojë aktorët joqeveritarë, të cilët nëse cenohen indirekt, cenojnë sigurinë kombëtare etj. Gjithashtu, kjo strukturë mund të hulumtojë për të gjetur praktikat më të mira në mbledhjen, menaxhimin, analizimin dhe shpërndarjen e informacionit, ofrimin e trajnimeve, të kryejë paralajmërime në lidhje me çështje sensitive, por dhe aktivitete hetimore afatgjata, pa qenë i nevojshëm krijimi i materialeve procedurale.

Një strukturë e tillë, për burimet e hapura, duhet të kombinojë stafin e përhershëm (specialistët e hetimit, analistët e informacionit, etj.) bashkë me stafin nga agjencitë e ndryshme qeveritare, me qëllim koordinimin dhe veprimin e menjëhershëm dhe efikas në raste kur ai nevojitet.

Për të mbajtur kostot e strukturës në nivele të ulëta, njohuritë dhe ekspertiza nga akademia dhe sektori privat, duhet të merren në mënyrë sistematike. Ndërsa krijimi dhe mbajtja e një strukture të tillë, do të kërkojë një investim fillestar financiar, ai është i destinuar t'i shpëtojë qeveritë nga një kosto e konsiderueshme në bazë vjetore, duke konsoliduar aksesin në shërbimet e informacionit, por edhe duke koordinuar me strukturat e tjera që kanë nevojë për informacion në mënyrë të vazhdueshme.

8. Shqipëria dhe burimet e hapura

Kohët e fundit po bëhet gjithnjë e më serioze, që informacione të pakontrolluara, në rrjete sociale, faqe të ndryshme, media etj., dhe në shumë raste transmetimi i tyre, të kenë një historik të mëparshëm. Hetimi i burimeve të hapura kërkon një impenjim të thellë nga strukturat e agjencive ligjzbatuese, gjë e cila është e pamundur për shkaqe të ndryshme, të cilat kërkojnë një analizim të veçantë.

Krijimi i një grupi pune, ndërinstitucional, për burimet e hapura, është më se i nevojshëm për të shqyrtuar ndërveprimet e mundshme midis agjencive të ndryshme qeveritare. Institucionalizimi i një strukture për burimet e hapura duhet të jetë sa më i shpejtë, duke krijuar edhe kushtet përkatëse për funksionimin e saj.

Formulimi i një strategjie kombëtare në lidhje me burimet e hapura, që do të

koordinonte këtë veprimtari në nivel politik, do të përcaktonte rolet, përgjegjësitë dhe krijimin e strukturave ndërvepruese për të gjitha institucionet e interesuara. Krijimi i një strukture të tillë, do të bënte të mundur marrjen e informacioneve paraprake në lidhje me akte të ndryshme kriminale apo terroriste, nxitje për akte të dhunshme etj., dhe në këtë mënyrë, strukturat e tjera do të ishin në gjendje të analizonin dhe të vepronin gradualisht, për të respektuar kuadrin ligjor dhe atë të sigurisë.

Hetimi i burimeve të hapura ka një impakt të menjëhershëm në çështjet e sigurisë kombëtare, duke qenë se nëpërmjet këtij procesi, mund të gjendet dhe të analizohet informacioni që në fillesat e tij, duke e mbajtur në kontroll dhe duke parandaluar akte të rënda në një periudhë të mëvonshme, që padyshim, do të cenonin sigurinë kombëtare.

Bibliografia

1. D. Steele, *Intelligence exploitation of the internet*, October 2002.
2. D. Steele, *Nato open source intelligence reader*, February 2002.
3. C. Hobbs and M. Moran, *Open source intelligence in the twenty-first century : new approaches and opportunities*, Saarbrucken: Palgrave MacMillan, 2014.
4. W. F. Kernan, *NATO open source intelligence handbook*, [. D. Steele], Ed., Norfolk VA: SACLANT, 2002.
5. R. D. Steele, *The new craft of intelligence : personal, public, & political*, Oakton VA: OSS International Press, 2002.
6. S. Tekir, *Open source intelligence analysis : a methodological approach*, Saarbrucken: VDM Verlag, 2009.
7. M. Glassman and M. J. Kang, "Intelligence in the information age : the emergence and evolution of open source intelligence (osint)," *Computers in human behavior*, vol. 28, iss. 2, pp. 673-682, 2012.
8. S. C. Mercado, "Sailing the sea of osint in the information age : a venerable source in a new era," , vol. 48, iss. 3, 2007.
9. D. F. Noble, "Fusion of open source information," , 2005.
10. D. F. Noble, "Asessing the reliability of open source information," , 2004.
11. C. Pallaris, "Open source intelligence : a strategic enabler of national security," *Css analysis in security policy*, vol. 3, iss. 32, 2008.
12. R. D. Steele, "The importance of osint to the military," *International journal of intelligence and counterintelligence*, vol. 8, 1995.
13. R. J. Heuer, *Psychology of intelligence analysis*, Washington D.C.: Central Intelligence Agency, 1999
14. "A compendium of analytic tradecraft notes," Directorate of Intelligence, Notes 1-10, 1997.
15. R. Johnston, "Analytic culture in the us intelligence community : an ethnographic study," , Washington D.C. 2005.
16. L. H. Silberman and C. S. Robb, "The commission on the intelligence capabilities of the united states regarding weapons of mass destruction : report to the president of the united states," 2005.
    G. F. Treverton and B. C. Gabbard, "Assessing the tradecraft of intelligence analysis," National Security Research Division, Santa Monica cop. 2008.

Burime interneti

1. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no3/article01.html#author1
2. https://www.fbi.gov/about/leadership-and-structure/intelligence-branch.

Një qasje e integruar në ekzaminimin ligjor të sistemeve CCTV

MSc. Kastriot GJOKA
EnCE®[1], CCLO[2], CCPA[3]
Instituti i Policisë Shkencore
kastriot.gjoka@asp.gov.al

MSc. Bledar KURTI
Telecom Albania
IP Networking Systems specialist

Abstrakt

Pamjet filmike të regjistruara nga kamerat e sigurisë kanë një rëndësi shumë të madhe si për sa i përket ndihmës që ato japin në hetimin e ngjarjeve të ndryshme ashtu edhe për përdorimin e tyre si prova ligjore në gjykatë. Sipas një raporti nga policia e Londrës, më shumë se 70% e hetimeve të vrasjeve janë zgjidhur me ndihmën e kamerave të sigurisë dhe hetimet për krimet e rënda kanë gjithmonë një strategji hetimi me kamera sigurie (CCTV). Në Sektorin e Ekzaminimeve Kompjuterike dhe Audio Video gjatë viteve të fundit kërkesat për ekspertimin e pajisjeve të kamerave të sigurisë (DVR) janë katapultuar. Këtë vit numri i vendimeve të ekspertimit për pajisjet DVR zë rreth 15-20% të totalit të vendimeve, të dytat pas telefonave celularë, duke lënë prapa kërkesat për ekzaminim kompjuterësh (5-8%). Në përgjithësi këto pajisje dërgohen për ekspertim kur është e pamundur kopjimi i pamjeve filmike me interes direkt në vendin e ngjarjes, kur pamjet janë fshirë, kur kërkohet rikuperim i pamjeve më të hershme se sa ato që ka të ruajtura pajisja DVR, apo kur DVr-ja ka datën dhe orën gabim dhe për këtë arsye kërkohen interpretime e njohuri të posaçme për përcaktimin dhe kopjimin e pamjeve filmike për intervalin kohor me interes. Në mjaft raste këto pajisje janë të kyçura më fjalëkalim duke mos lejuar mundësinë e hyrjes në menytë përkatëse për kopjimin e të dhënave. Sigurimi i fjalëkalimit përgjithësisht nuk është i mundur për shkaqe nga më të ndryshmet; pronarët apo administratorët mund ta harrojnë atë për shkak se ndërveprimi me këtë pajisje ndodh rrallë, pretendojnë se nuk e mbajnë mend për t'ju shmangur kërcënimeve apo akuzave nga autorët e veprave penale të fiksuara në pamjet filmike që ruhen në këto pajisje apo për të shmangur përgjegjësinë e tyre në rastet kur ato vetë janë autorë te veprave penale. Në shumë raste të tjera, autorët i fshijnë apo dëmtojnë këto pajisje, para ose pas ngjarjes. Ky material analizon qasjen në ekzaminimin ligjor të sistemeve CCTV, duke ofruar në fund edhe rekomandimet përkatëse.

Fjalëkyçe: sisteme CCTV, ekzaminim ligjor, kamerat e sigurisë, hetim, pajisjet DVR.

[1] EnCase Certified Examiner (Titulli EnCase- Ekspert i certifikuar për ekzaminime kompjuterike dhe përdorimin e metodologjisë EnCase, nga kompania Guidance Software Inc. SHBA).
[2] Cellebrite Certified Logical Operator(Ekspert i çertifikuar për ekzaminim logjik të telefonave celularë nga kompania Cellebrite LTD, Israel).
[3] Cellebrite Certified Physical Analyst (Ekspert i certifikuar për ekzaminime të avancuara, rikuperim dhe analizim të dhënash të fshira nga telefonat celularë nga kompania Cellebrite LTD, Israel).

Fjalorth*

a. Metadata: është informacion i strukturuar që lokalizon, shpjegon dhe përshkruan të dhëna të tjera. Metadata-t njihen edhe si "të dhënat në lidhje me të dhënat" (data about data). Një informacion i tillë e bën më të lehtë identifikimin dhe lokalizimin e një dokumenti të veçantë.
b. Imazh: një kopje identike bitstream (sektor për sektor) e të dhënave që ruhen në një pajisje ruajtje informacioni (hard disk, USB, kartë memorie etj).
c. Raw: të dhëna të papërpunuara - të dhëna në nivel individual bajtësh, siç janë të shkruara në hard disk.
d. DVR (Digital Video Recorder): pajisje elektronike për ruajtjen në format digjital, në hard disk, ose pajisje të tjera ruajtje informacioni (lokale ose në rrjet), të pamjeve filmike të filmuara nga kamerat e sigurisë.
e. Pajisje bllokuese shkrimi (write blocker): pajisje që shërbejnë për lidhjen e hard diskut provë materiale me kompjuterin ekzaminues me qëllim imazhimin, analizimin apo kopjimin e të dhënave, duke ruajtur të paprekur përmbajtjen e tij.
f. Header: disa bajt në fillim të një skedari, të njohur ndryshe edhe si numra magjik, që shërbejnë për identifikimin dhe verifikimin e skedarit.
g. Frame: videot janë të përbëra nga seri fotografish të renditura në mënyrë të njëpasnjëshme, fotografi të cilat njihen me emrin frame. Kur themi se një video është 25 frame për sekondë nënkupton se një sekondë e videos është e përbërë nga 25 fotografi të njëpasnjëshme.
h. File-System: një metodë për organizimin dhe menaxhimin e skedarëve në një medium ruajtës, si p.sh. një hard disk. File System-i më i përdorur në Windows është NTFS. Një file system mund të mendohet si një indeks apo databazë që përmban vendndodhjen fizike të çdo pjesë të së dhënave në hard drive ose në një pajisje tjetër ruajtëse.
i. Offset: një mënyrë referimi për lokalizimin e një të dhëne, në cilin bajt ose sektor gjendet e dhëna konkrete (germa, karakteri, fjala) duke filluar numërimin nga fillimi i skedarit apo "hard diskut".

1. Hyrje

Dikur autorët ktheheshin në vendngjarje për të parë veprimet e policisë apo për të fshehur apo shkatërruar gjurmët e lëna në vendngjarje, sot një motiv më shumë i rikthimit në vendngjarje është fshirja apo shkatërrimi i pamjeve filmike në të cilat ata mund të jenë fiksuar në kryerje e sipër të veprës penale apo gjatë afrimit e largimit nga vendngjarja. Sidoqoftë edhe kur nuk jemi në situatat e mësipërme, për nxjerrjen (kopjimin) e pamjeve filmike nga këto pajisje hasen vështirësi të ndryshme. Ato shpesh kanë probleme me portat që shërbejnë për kopjimin e të dhënave ose ofrojnë mundësi të kufizuara të kopjimit. Shumica e tyre janë të programuara që t'i fshijnë pamjet filmike pas mbushjes së memories me parimin FIFO (*First in-First Out*, hyn e para, fshihet e para) apo pas një intervali kohor të caktuar. Në raste të tjera për shkak të keqfunksionimit ato bëjnë inicializimin e hard diskut apo memories duke fshirë çdo të dhënë të mëparshme. Në të tilla situata e vetmja zgjidhje për nxjerrjen apo rikuperimin e këtyre pamjeve filmike është ekspertimi kompjuterik. Kjo mund të realizohet duke

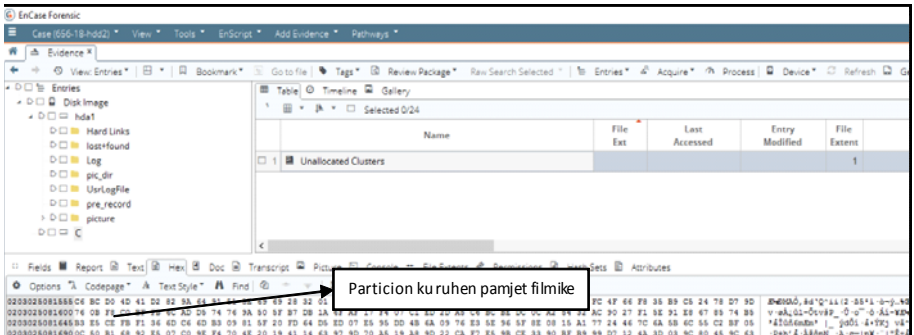
* *Shënim i redaktorit:* Materiali që lexoni, është disi i ngarkuar me terma shumë specifikë të fushës. Këta janë lënë nga autorët në gjuhën origjinale ose janë huazuar, pa pasur raste të ngjashme referimi në shqip. Ky detaj, shërben për të sjellë në vëmendje, nevojën e hartimit të fjalorëve të vegjël profesionalë me shqipërim termash. Për shkak të tematikës dhe fushës së trajtuar, kjo nevojë vihet re thuajse në të tëra punimet e kësaj konference, por ky material, përfaqësonte atë me mbigarkesën më të lartë të termave të huazuara. Autorët, janë përpjekur të ndihmojnë në këtë drejtim duke sjellë një fjalorth sqarues për termat e shkrimit.

dekoduar strukturën e këtyre videove të ruajtura në memoriet e këtyre pajisjeve dhe më pas aplikimin e teknikave të kopjimit të këtyre pamjeve në format të lexueshëm, manualisht ose në mënyrë të automatizuar. Metoda që ne propozojmë jep një konkluzion kategorik për ekzistencën ose jo qoftë edhe të një *frame*-i të vetëm video me interes në memorie dhe nëse po kopjimin nga hard disku i pajisjes dhe ruajtjen në një format të lexueshëm. Kjo metodë nuk bazohet në file *system*-in e memories, ajo bazohet në analizimin në nivel "raw", të hard diskut kështu që rikuperon çdo sekuencë të mundshme që ka mbetur në hard disk. Duke përdorur *skript-e Python* dhe programe ekzaminuese si EnCase, ne mund ta automatizojmë procesin, të krijojmë raporte që na japin informacion të plotë të metadatave për çdo *frame* video në hard disk dhe më pas për intervale kohore e kamera me interes, nxjerrjen e tyre jashtë në skedarë të veçantë të ndarë sipas kamerave (*demultiplexing*). Pas përftimit të pamjeve filmike me interes, njohuri dhe teknika të posaçme nevojiten me qëllim përmirësimin e cilësisë së këtyre pamjeve të përftuara, pasi kamerat e sigurisë përgjithësisht lënë për të dëshiruar për sa i përket rezolucionit, dukshmërisë apo detajeve të objekteve me interes. Edhe pse përdorimi i programeve automatike për këtë qëllim duket një veprim i lehtë, përdorimi i filtrave apo teknikave përmirësuese mbi regjistrime video apo imazhe duhet të jetë i kujdesshëm pasi në shumë raste mungesa e njohurive përkatëse në përdorimin e tyre jep efekt të kundërt.

2. Një vështrim i shkurtër për mënyrën e organizimit të të dhënave në pajisjet DVR

Shumica dërrmuese e pajisjeve CCTV përdorin *file system*-e si dhe mënyra të kodimit të pamjeve filmike të personalizuara. Për më tepër nuk ekziston asnjë lloj standardizimi si dhe ky informacion përgjithësisht nuk është publik.

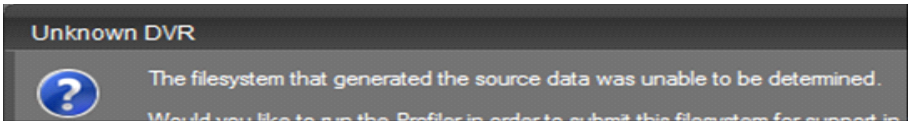
Ekzistojnë disa qindra lloje *file system*-esh që përdoren nga prodhuesit, të cilët janë të palexueshëm (dekodueshëm) nga sistemet dhe programet tradicionale.



Imazhi hard disku i një DVR-je të markës HAWOELL, i ngarkuar në programin ekzaminues kompjuterik EnCase v.8.07.00.93. Particioni "C" ku ruhen pamjet filmike nuk është i lexueshëm, pra nuk dallohen folder-a apo skedarë, me qëllim identifikimin apo kopjimin e tyre jashtë hard diskut.

Programet ekzaminuese kompjuterike si *EnCase, FTK, X-Ways, Forensic Explorer, Axiom*, etj., nuk janë në gjendje të rikuperojnë pamje filmike nga këto pajisje. Aktualisht ekzistojnë një numër tepër i kufizuar programesh ekzaminuese për sistemet CCTV.

Në përgjithësi, për shkak se nuk mund të lexojnë e dekodojnë *file system*-in e tyre, hard disqet ose imazhet e DVR-ve paraqiten në këto programe si "Unallocated Clusters" ose si "Unused Disk Area". Në disa raste këto programe mund të jenë në gjendje të lexojnë disa nga llojet e *file system*-ve që përdorin këto pajisje (si NTFS, FAT etj), megjithatë në rastet e dëmtimit apo korruptimit të file *system*-it, të fshirjes së pamjeve filmike, të formatimit të hard diskut ku ruhen këto pamje, këto programe nuk janë në gjendje të rikuperojnë të dhëna.



DVR që nuk mund të dekodohet nga program i dedikuar për ekzaminimin e tyre

Të dhënat kompjuterike në një pajisje ruajtje informacioni (hard disk, kartë memorie, USB, etj.) edhe pse mund të jenë fshirë vazhdojnë të ekzistojnë në memorien e tyre për sa kohë që zona ku ato ruhen nuk është rishkruar (*overwrite*) apo e gjithë memoria apo zona ku ato ruhen nuk është sterilizuar (*wipe*).

Në këto raste e vetmja mënyrë është inxhinierimi i kundërt i strukturës së videove direkt në hard disk, për identifikimin e pamjeve filmike për intervale kohore apo kamera me interes. Sfida e më pasme dhe më e vështira është në kopjimin e tyre jashtë hard diskut në format të lexueshëm.

Shumica e DVR-ve përdorin formatin H.264 për të regjistruar pamjet filmike nga kamerat e sigurisë (vëzhgimit). Nëse videot (pamjet filmike) janë të koduara në formatin H.264, çdo *chunk* video zakonisht përmban një *header* (disa bajt identifikuese) më pas të dhëna ne "H.264 bytestream" dhe mundet ose jo një *footer*. Të dhënat H.264 konsistojnë në varg bajtësh të paketuar në një njësi NAL (*Network Abstraction Layer*). Përmbajtja e kompresuar e *videostream* gjendet brenda këtyre njësive NAL. Çdo njësi NAL fillon me pesë bajt "0x00000001xy". Tre bajtët pas bajtit të parë(\x00), njihen me emrin "start code prefix". Bajti i fundit ruan informacion rreth NAL-it, ndër të tjera edhe për tipin e tij[4]. Ky bajt i fundit merr vlera të ndryshme në varësi të tipit të njësisë NAL. Kështu që bajtët që na shërbejnë për të identifikuar se ku fillon një *frame video* janë grupi i bajtëve "0x00000001".

Videot H.264 në këto pajisje zakonisht konsistojnë në I-frame (*intra-frame encoded frames*), P-frame (*predictive encoded frames*) dhe shumë rrallë edhe *frame* të tipit "B[4]".

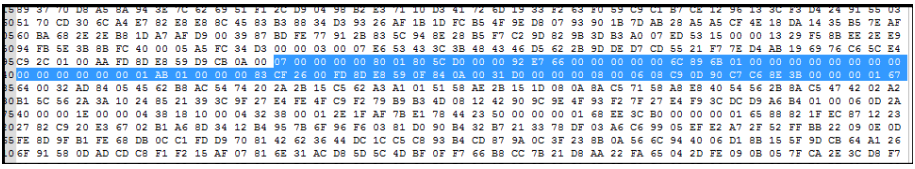
Nga studimi i një numri të konsiderueshëm tipash të ndryshme pajisjesh CCTV (DVR, NVR etj.) kemi konstatuar se shumica e tyre stampojnë (shkruajnë) disa *metadata* përpara çdo *I-frame* dhe në shumicën e rasteve edhe përpara çdo *P-frame*.

Këto *metadata* përmbajnë kryesisht datën dhe orën, numrin e kamerës dhe në shumë raste madhësinë (*frame size*) e *frame*-it.

[4] SWGDE Best Practices for the Recovery of Data from Security Digital Video Recorders Containing H.264 Data. Version: 1.2 (June 23, 2016).

3. Struktura dhe inxhinierimi i kundërt i *metadata*-ve të "video-frame"-ve

Pas lokalizimit të një *I-frame* apo *P-frame* në hard disk, zona prej disa bajtësh përpara njësisë NAL, siç u përmend më lart, zakonisht përmban disa *metadata* (datë, orë, numër kamere etj.). Këto janë *metadata* të stampuara nga pajisja koduese e videos.

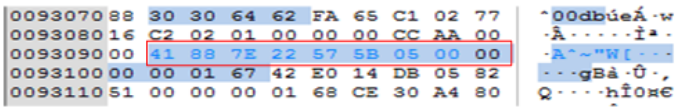


Pamje e zonës së metadata-ve përpara një I-frame në një NVR të markës HAOOWELL. Me katrorë të kuq janë rrethuar numri i kamerës dhe data dhe ora

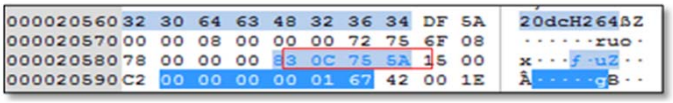
Formati i datës dhe orës:

Për stampimin e datës dhe orës në *metadata*, prodhues të ndryshëm përdorin formate (*enkodime*) të ndryshme. Ndër më të përhapurit janë:

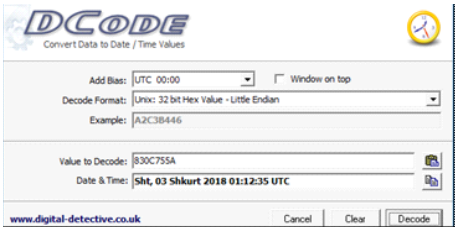
- 64-bit integer (UInt64), *Unix numeric value or Unix millisecond value*.
- *Unix/Epoch format* (32 bit, *little endian, hexadecimal*).
- Në *hexadecimal*, në formatin vit-muaj-datë-orë-min-sek. ose muaj-datë-vit-orë-min-sek.
- Në formatin binar, bit *masked* 4 ose 5 *byte*.
- Në formatin binar, bit *masked* katër ose 5 *byte*, *swap bytes*.[5]



Datë dhe orë e stampuar në metadata në formatin 64-bit integer



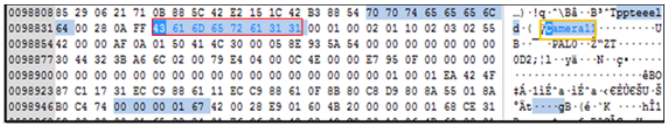
Datë dhe orë e stampuar në *metadata* në formatin *Unix/Epoch* format (32 bit, *little endian, hexadecimal*).

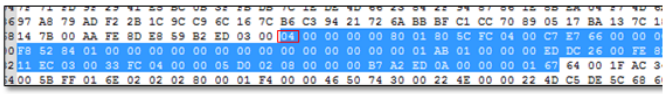


Dekodimi i këtij formati në programin DCODE

[5] - SWGDE Best Practices for the Recovery of Data from CCTV Digital Video Recorders- Version: 1.0 (February 05, 2015). - "A Million Words: Demystifying Video Carving from CCTV Systems ", Kastriot Gjoka, Bledar Kurti, Konferenca EnFuse 2018, Las Vegas SHBA.

Formati i numrit të kamerës:
Më të zakonshmet që ndeshen janë:
- në format ASCII,
- në format Unicode,
- në format decimal,
- të emërtuara nga përdoruesi ("Hyrja kryesore", "Dalja e pasme", etj.).





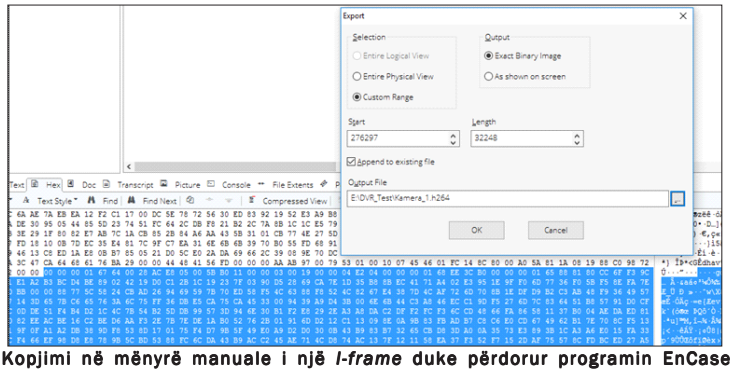
Forma të ndryshme të stampimit të numrit të kamerës në metadata

- Formati i madhësisë së frame-it (frame size)

Zakonisht është i stampuar në 4 *byte*. Këto 4 *byte* të dekoduara në formatin 32 bit *integer* japin madhësinë në *byte* të atij *frame*-*i*. Madhësia në *byte* është pa zonën e *metadatave header*-it apo *footer*-it që ato mund të përmbajnë.

4. Rikuperimi i automatizuar i pamjeve filmike nga pajisjet CCTV

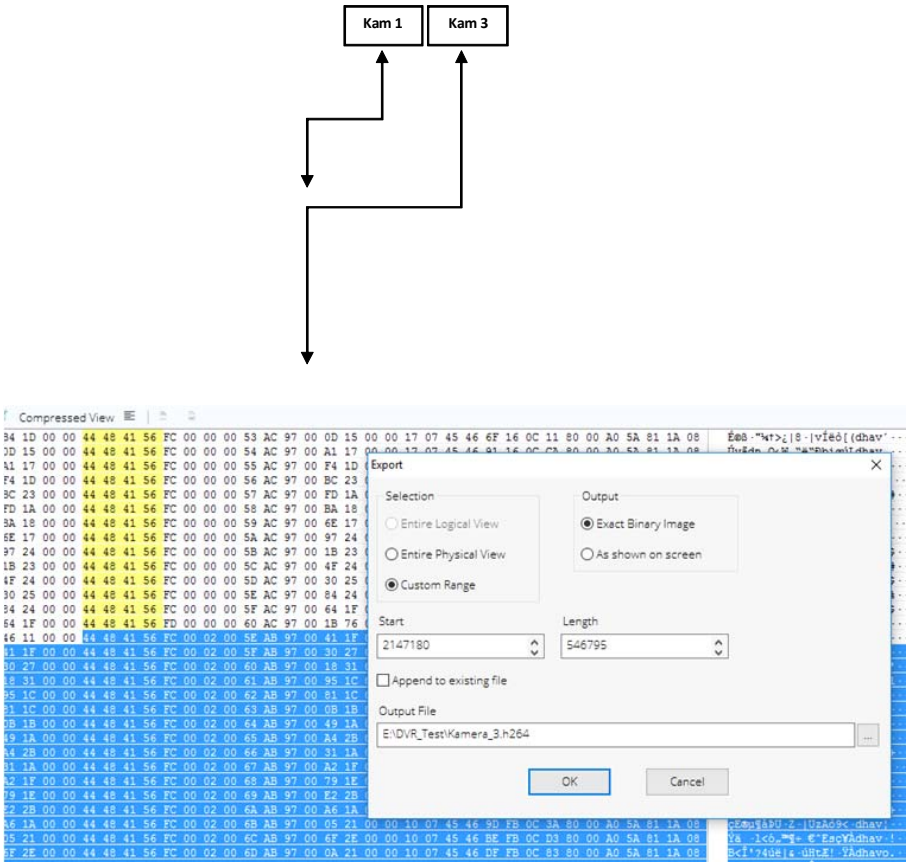
Rikuperimi i pamjeve filmike për intervale kohore tepër të shkurtra mund të bëhet edhe në mënyrë manuale. Kështu pasi të kemi identifikuar një *frame video*-je dhe dimë kujt kamere i përket, kujt date dhe ore dhe sa e ka madhësinë në bajt, duke u nisur nga *offset*-i ku fillon, ne kopjojmë jashtë hard diskut aq bajt sa është madhësia e tij. Më pas vazhdohet me *frame*-in e radhës të së njëjtës kamerë, por duke ruajtur renditjen e orës dhe datës, e kopjojmë atë jashtë dhe e vendosim në fund të skedarit që sapo krijuam me *frame*-in e pare (merge) e kështu me radhë. Megjithatë duke menduar se vetëm një sekondë e vetme përbëhet prej një *I-frame* dhe disa *P-frame*-sh, shumëzuar kjo me numrin e kamerave pamjet e të cilave nevojiten, ndarja e tyre sipas kamerave dhe radhitja sipas datës dhe orës për rikrijimin e sekuencave të gjata me pamje filmike në mënyrë manuale, është një punë në kufijtë e të pamundurës.



Kopjimi në mënyrë manuale i një *I-frame* duke përdorur programin EnCase

Në rastet kur DVR-ja i ka shkruar *frame*-t në grupe (disa *frame* të njëpasnjëshme nga e njëjta kamera), selektohet i gjithë grupi i *frame*-ve të saj kamere (fillimi dhe mbarimi i tyre dallohet nga numri i kamerës në *metadata*) dhe kopjohet jashtë në një skedar. Më pas shkohet më poshtë në hard disk deri sa të identifikojmë një grup tjetër *frame*-sh të së njëjtës kamera, kopjohen dhe vendosen në fund të skedarit që krijuam. Ky veprim përsëritet për aq interval kohor pamjesh na nevojitet.

Në programin ekzaminues EnCase, pasi ngarkojmë imazhin e hard diskut, ndërtojmë fjalë kërkimi me *header* dhe gjetjet (*search hits*) i shikojmë në opsionin "Compressed View" në dritaren "View Pane". Ndryshe nga rasti më sipër këtu nuk është e nevojshme madhësia e *frame*-it, pas fundi i tij zakonisht është ku fillon *frame*-i i më pasëm.



Kopjimi i një grupi *frame-sh* nga e njëjta kamera me programin EnCase v.8. Kamera është e stampuar në vlerë decimale(*hexadecimal* në decimal). Zakonisht DVR-të e fillojnë numërimin e kamerave nga zero, kështu që kamera zero në *metadata* i përket kamerës 1.

Nga analizimi që i kemi bërë një DVR-je të tipit Neutron me *hard disk 3TB* (që janë normal në ditët e sotme në këto pajisje) kemi konstatuar rreth 340 milionë *frame* "I" dhe "P". Siç mund të kuptohet nga sa u tha më lart zgjidhja është automatizimi i procesit.

3.1 Analizimi i automatizuar i hard disqeve të DVR-ve, krijimi i raporteve për çdo frame *me numrin e kamerës, datën dhe orën dhe madhësinë e tij*

Duke përdorur informacionin e dekoduar nga metadatat (përshkruar më lart) ne mund të shkruajmë *script*-e (Enscript në EnCase, C++, JAVA, Python, etj) për të automatizuar procesin e analizimit të hard diskut të DVR-së për çdo *frame* të mundshme të ruajtur apo të fshirë, por që akoma ekziston në hard disk (i pambishkruar) dhe të krijojmë një raport në formate si *txt, csv, html* etj. Ky raport do të përmbajë informacion për datën dhe orën e çdo *frame*, numrin e kamerës të cilës i përket, *offset*-in ku ndodhet në hard disk dhe madhësinë e tij (*frame size*).

Kjo do të ishte mjaft e dobishme ndër të tjera për:

- të dimë nëse gjendet në hard disk ndonjë sekuencë sado e vogël filmike për datën, orën dhe kamerën me interes;
- të rikuperojmë pamjet me interes bazuar në datë, orë dhe numër kamere;
- të sigurohemi që pamjet filmike, të eksportuara nga vetë DVR-ja apo duke përdorur ndonjë program tjetër, janë kopjuar saktësisht.

3.2. Përdorimi i gjuhës Python *në analizimin dhe rikuperimin e pamjeve filmike nga pajisjet CCTV*

Gjuha e zgjedhur Python. Pse?

- është një gjuhë *object-oriented*;
- mund të aplikohet në kategori të ndryshme problemesh;
- përdoret pothuajse në çdo platformë;
- ka librari të gjëra standarde që mbulojnë zona të tilla si procesim *string*-esh, *regular expressions*, *Unicode*, llogaritje diferencash ndërmjet dokumenteve (*files*) etj.;
- mund të zgjerohet funskionaliteti duke përdorur gjuhë të tjera si C or C++ [6].

3.2.1. Analizimi i përmbajtjes së hard diskut dhe shkrimi i një raporti për çdo frame *të mundshëm në hard disk (të fshirë ose jo)*

Hard diskut të DVR-së i merret një imazh (kopje ekzakte) gjithmonë duke përdorur pajisje bllokuese shkrimi (*write blocker*). Pajisja "*write blocker*" mbron hard diskun provë materiale nga kontaminimi gjatë procesit të marrjes së imazhit, duke e ruajtur gjendjen e informacionit në hard disk të pandryshuar.

Algoritmi dhe kthimi në script:

- Krijojmë një shprehje kërkimi të formatit "*regular expression*" për të cilën do të kërkojmë në hard disk (imazh). *Regular expression* krijohet duke marrë si shprehje një grup bajtësh të cilët përsëriten në mënyrë të qëndrueshme dhe në të njëjtin pozicion përpara çdo *frame* (header), si dhe duhet të përfshijë të gjithë zonën e *metadata-ve*.
- Nëpërmjet funksioneve të veçanta konvertojmë nga *metadata*-t në format human datën dhe orën, numrin e kamerës dhe madhësinë e çdo *frame*.
- Identifikojmë *offsetin* ku fillon çdo *frame*.
- Shkruajmë rezultatet në një skedar, në një format që dëshirojmë (txt, xls, html, etj).

Kthimi në script:

Në *script*-in e mëposhtëm, tek "*regular expression*", bajti i parë është kamera, bajtët 24-28 është data dhe ora në formatin "32 bit hexadecimal little endian".

Funksioni i parë në script "pt(byte)" bën konvertimin e datës dhe orës nga format *hexadecimal* në format human (datë/muaj/vit orë:minuta:sekonda).

Leximi i imazhit "raw" të hard diskut bëhet duke përdorur *buffer-size*. Në scriptin e mëposhtëm për *buffer-size* është përcaktuar vlerë fikse por kalkulimi i tij mund të bëhet edhe në mënyrë dinamike, në varësi të memories RAM që ka kompjuteri ku po kryhet ekzaminimi.

```
import re
from datetime import datetime


def pt(byte):
    ts = int.from_bytes(byte, byteorder='little')
    return str(datetime.fromtimestamp(ts).strftime('%d/%m/%Y %H:%M:%S'))


def scan():
    buffer_size = 1073741824
    file = 'image wth full path' # 'D:\cases\test\test_image.dd'
    input = open(file, 'rb')
    output = open('results_of_scan.txt', 'w')
    p = re.compile(b'[\s\S]{2})\x64\x63\x48\x32\x36\x34[\s\S]{24}\x00{3}\x01')
    i = 0
    for chunk in iter(lambda: input.read(buffer_size), b''):
        for m in p.finditer(chunk):
            output.write(pt(m.group()[24:28]) + ' Cam: ' +
                         str((m.group()[0] + 1)).zfill(2) +
                         " Offset: " + str(m.start() +
                         (i * buffer_size)).rjust(13) + '\n')
        i += 1

    input.close()
    output.close()
```

Regular Expression

Ky *script* pasi skanon imazhin e hard diskut të DVR-së do të gjenerojë një raport i cili përmban:

- datën dhe orën e çdo *frame;*
- numrin e kamerës;
- ku ndodhet ai *frame* në hard disk(*Start offset*).

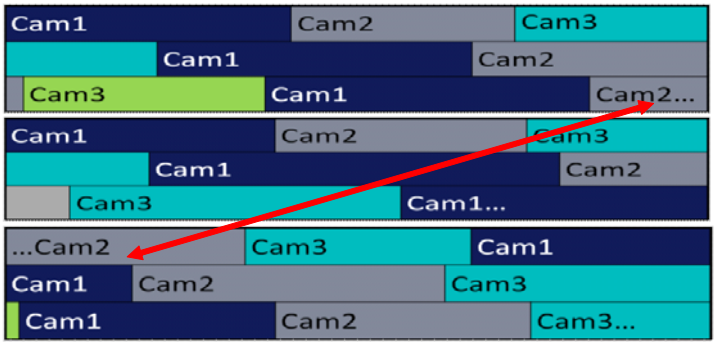
Raport i gjeneruar me scriptin e propozuar mësipër

3.2.2. Rikuperimi i pamjeve nga hard disku

Me informacionin e gjeneruar me *script*-in e mësipërm mund të shkruajmë një *script* tjetër i cili do të kopjojë të gjitha *frame*-t jashtë nga hard disku, duke i shkruar në skedarë të veçantë për secilën kamer.

I vetmi problem që haset më mënyrën e rikuperimit që do të trajtohet më poshtë është "multiplexing". Pamjet filmike që vijnë nga kamerat e lidhura me pajisjen shumë shpesh nuk shkruhen në skedarë të veçantë por *frame*-t nga kamera të ndryshme shkruhen në hard disk të përziera. *Multiplex* haset në dy forma; në nivel blloku dhe nivel *chunk*-u.

Shumë DVR e ndajnë hard diskun në blloqe me madhësi të caktuar, në të cilët shkruajnë regjistrimet video. Në rastin kur një bllok mbushet ndodh shumë shpesh që një pjesë e *frame*-it të fundit shkruhet në këtë bllok, ndërsa pjesa tjetër e tij vazhdon në një bllok tjetër, pasi nuk ka hapësirë për të shkruar *frame*-in e plotë. Bashkimi i këtyre dy copave për të rikrijuar këtë *frame* është shumë i vështirë.



Një paraqitje skematike e "multiplexing".

Megjithatë nëse rikuperojmë një video të fshirë për intervalin kohor me interes për hetimin le të themi prej disa minutash, humbja e një *frame* apo e një sekonde zakonisht nuk ka ndonjë impakt në identifikimin apo analizimin e veprimeve në skenën e krimit.

Nëse është e rëndësishme edhe këto frame mund të rikuperohen. Videot në format "H264" janë të kompresuara me mënyrën "temporal compression". Zakonisht frame-t "I" janë *frame* reference (bazë) ndërsa *frame*-et e tjera mbajnë vetëm ndryshimet që pëson videoja gjatë kohës së regjistrimit nga *frame*-i bazë. Nëse e rikrijojmë një *I-frame* nga dy fragmentet tij, të krijuara për shkak të procesit "multiplex" dhe e kopjojmë atë jashtë hard diskut, përmbajtja e tij mund të shikohet me programe të ndryshme si "*ffmpeg*", etj. Në rastet kur *frame*-i i fragmentuar është i tipit P-*frame*, ai rikrijohet dhe i bashkohet grupit të *P-frameve* të tjera, në pozicionin që i takon.

Nëse dihet madhësia ekzakte e bllokut ky proces i ribashkimit të copave të *frame*-it të fragmentuar është më i lehtë. Mënyra e rikuperimit *frame*-ve të fragmentuara është jashtë objektit të këtij punimi.

Ndërtimi i një algoritmi dhe kthimi në script:

- Analizo informacionin nga raporti i përftuar nga *script*-i i skanimit.
- Nëse *frame* është brenda datës dhe orës me interes, shkruaje rekordin në një listë.
- Ndaje listën fillimisht bazuar në start *offset*-in e çdo rekordi.
- Shkruaj si *end offset* të *frame*-it start *offset*-in e *frame*-it të radhës, nëse dihet madhësia e *frame*-it shkruaj madhësinë e tij.
- Pastaj bëj një ndarje tjetër bazuar në numrin e kamerës dhe datën dhe orën.
- Lista përmban tashmë grup *frame*-sh të së njëjtës kamera të ndarë sipas datës dhe orës.
- Duke përdorur këtë listë kopjo *frame*-t nga hard disku dhe shkruaji në skedarë veçmas, bazuar në numrin e kamerës.

```
def sort_and_carve(file, st_dt, et_dt):
    selection = []
    with open('scan_report.txt', 'r') as f:
        for line in f:
            found_time = line[0:19]
            cam = int(line[25:27])
            start = int(line[36:50])
            found_dt = datetime.strptime(found_time, '%d/%m/%Y %H:%M:%S')
            if st_dt <= found_dt <= et_dt:
                select = [found_dt, cam, start, None]
                selection.append(select)
```

```
selection.sort(key=operator.itemgetter(2))
```

```
for i in range(len(selection)):
    try:
        diff = selection[i + 1][2] - selection[i][2]
        if selection[i + 1][1] != selection[i][1] and diff < 600000: # diff value depends on approximate frame size
            selection[i][3] = selection[i + 1][2]
            selection[i + 1][2] = selection[i + 1][2]
        elif selection[i + 1][1] == selection[i][1] and diff < 600000:
            selection[i][3] = selection[i + 1][2]
        else:
            pass
    except IndexError:
        pass

for i in range(len(selection)):
    try:
        if selection[i][3] is None:
            del selection[i]
    except IndexError:
        pass
```

```
selection.sort(key=operator.itemgetter(1, 0))
```

```
cams = []
records = []
for key, group in groupby(selection, lambda zh: zh[1]):
    records.append(list(group))
    cams.append(key)

f = open(file, 'rb')
for a, c in enumerate(cams):
    time_frame = records[a][0][0].strftime('%d_%m_%Y_%H_%M_%S') + '-' + \
                 records[a][-1][0].strftime('%d_%m_%Y_%H_%M_%S')
    f_out = open('Cam-{0}-{1}.h264'.format(c, time_frame), 'ab')
    for b in range(len(records[a])):
        f.seek(int(records[a][b][2]))
        capture = f.read(int(records[a][b][3]) - int(records[a][b][2]))
        f_out.write(capture)
    f_out.close()
f.close()
```

Një model *script*-i sipas algoritmit të mësipërm.

5. Formati i videove të rikuperuara dhe leximi (shikimi i tyre)

Video e rikuperuar në mënyrën e rekomanduar në këtë punim janë në formatin siç janë shkruar nga pajisja në hard disk, pra nuk përdoret asnjë lloj konvertimi apo ndryshimi i strukturës së tyre. Ndonëse kopjimi në këtë mënyrë mund të ketë disa kufizime si p.sh në lidhje me disa elementë si shkalla e *bitrate*, proporcionin e dimensioneve (*aspect ratio*) etj., në përgjithësi pamjet e përftuara janë në maksimumin e cilësisë që ka regjistruar kjo pajisje.

Për luajtjen e këtyre pamjeve filmike mund të përdoren programe të ndryshme si "Elecard AVC HD Player", "Media Player Lite", "Media Player Classic", "ffmpeg",

programet e vetë pajisjeve, etj. Rekomandohet që të testohen sa më shumë programe që disponohen për të përzgjedhur atë që i luan më saktë.

Videot e rikuperuara mund të konvertohen edhe në formate të tjera të hapura si avi, mp4 etj. Një komandë e thjeshtë për konvertimin e tyre në formatin mp4 nëpërmjet programit pa pagesë "ffmpeg" jepet më poshtë:

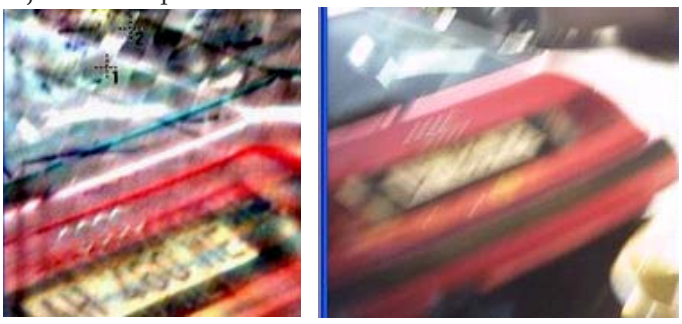
"Ffmpeg -framerate 24 -i input.264 -c copy output.mp4": një nga limitimet e kësaj metode është se me anë të saj mund të rikuperojmë vetëm pamjet filmike. Në rast se regjistrimet filmike janë edhe me audio, audio nuk mund të rikuperohet në këtë mënyrë.

6. Një vështrim i shkurtër mbi përmirësimin e cilësisë së pamjeve filmike të përftuara nga pajisjet CCTV

Një nga problemet që haset me pamjet filmike të kamerave të sigurisë është cilësia e këtyre pamjeve. Cilësia e dobët e tyre varet nga shumë faktorë si cilësia e kamerave regjistruese, fokusimi jo i saktë i saj, ndriçimi i ambientit të filmuar, distanca e zonës apo objektit të filmuar, objekti ka qenë në lëvizje apo në kënd të pjerrët në raport me objektivin e kamerës etj. Aplikimi i teknikave (filtrave) të ndryshme për përmirësimin e cilësisë së pamjeve filmike kërkon njohuri të posaçme dhe përvojë në këtë fushë. Programet apo filtrat janë thjesht mjete, përdorimi i saktë i tyre varet nga eksperti. Përdorimi i gabuar çon në shtim apo heqje elementësh nga videoja apo fotografia, apo degradim të pamjes. Prandaj është e nevojshme që nëse pamjet filmike nuk nevojiten thjesht për të analizuar veprimet në vendngjarje por kërkohet identifikim objektesh, personash, targash automjetesh, qartësim i pamjeve etj., ato duhet të procesohen nga ekspertë me njohuri dhe pajisje e programe të posaçme. Qëllimi i këtij punimi nuk është shtjellimi në detaje i këtij lloj ekspertimi por për t'i dhënë lexuesit disa njohuri bazë, në mënyrë që në rastet kur ndeshet në situatat e përmendura më lart të ketë një informacion të përgjigjshëm se çfarë ekzaminimesh të mëtejshme mund të kryhen mbi këto pamje filmike apo qoftë edhe mbi fotografi të ndryshme.

Pamjet e turbullta(blurr). Blurr haset në dy forma; në rastet kur kamera nuk është në focus dhe në rastet kur objekti ose kamera është në lëvizje.

Turbullira në lëvizje (motion blurr). Në rastet kur objekti në pamjet filmike lëviz më shpejt se koha e ekspozimit të aparatit apo kamerës, objekti do të paraqitet i turbullt (*motion blurr*). Korrigjimi mund të bëhet me filtra "motion deblurr" dhe në mjaft raste rezultatet janë të kënaqshme:



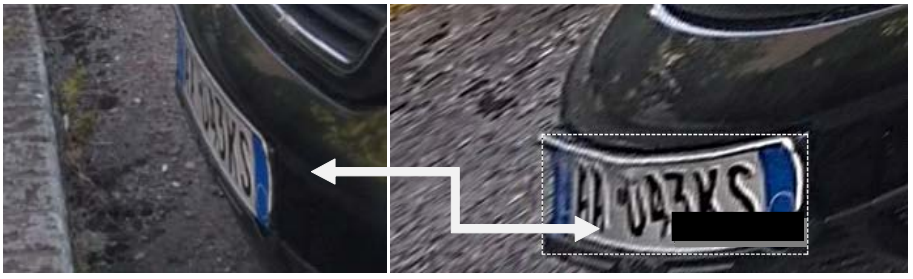
Korrigjimi me filtrin "motion deblurr" në programin *Amped Five* [7].

[7] https://www.moonsoft.fi/materials/amped_five_en.pdf

Turbullira optike (optical blurr). Ndodh kur objekti i filmuar nga kamera nuk është plotësisht në fokus. Në kamerat e sigurisë kjo haset shpesh.

Korrigjimi me filtrat "Optical Deblurring", "Curve" dhe "Resize", në programin Amped Five

Korrektimi i perspektivës. Në raste të ndryshme ndodh që objekti është në një kënd të tillë me objektivin e kamerës saqë elementë të rëndësishëm të tij si p.sh targa e automjetit është e palexueshme. Filtra korrektues japin në disa raste rezultat domethënës në identifikimin e plotë të këtyre elementeve. Por edhe kur të gjithë elementët nuk janë plotësisht të lexueshëm ky përmirësim i pamjes mund të shërbejë për të ngushtuar rrethin e kërkimeve.



Korrigjimi i perspektivës me filtrin "Correct Perspective", në programin Amped Five", për identifikimin e targës së një automjeti. Majtas fotografia objekt ekspertimi, djathtas fotografia pas përpunimit.

Një sërë filtrash apo teknikash të tjera mund të përdoren në varësi të gjendjes së filmimit origjinal, si dritë dhe kontrast, filtra për stabilizimin e videove kur kemi objekte në lëvizje, apo filtra të tjera si "sharpen", "Histogram Equalisation", "resize", "frame average", "super resolution", filtra për korrigjim ngjyre, për eliminimin e zhurmave (*noice*), të sfondit, etj.

Megjithatë filtrat dhe teknikat e mësipërme japin rezultat vetëm kur detaji është i fiksuar në video ose foto, por për shkaqet që u përmendën më lart (ndriçim i dobët, mungesë fokusimi, lëvizja e objektit apo kamerës, etj.), nevojiten disa filtra apo teknika për ta bërë të identifikueshëm apo më të qartë. P.sh. një targë automjeti që është e fiksuar vetëm në një *pixel* (dhe që ndodh shpesh) nuk mund të bëhet e identifikueshme.

Një nga gabimet që bëhet shpesh gjatë këqyrjes së pamjeve filmike është nxjerrja e fotografive nga videot duke i hapur videot në programe të ndryshme dhe duke përdorur komandën "print screen", për të marrë fotografi me interes nga këto pamje filmike apo filmimi i këtyre pamjeve (me celular apo mjet tjetër) mbi ekranin ku ato po shfaqen. Kjo është krejtësisht e gabuar sepse me komandën "print screen" apo fotografim nga ekrani ne po marrim atë rezolucion që pamja shfaqet në ekran dhe jo rezolucionin (cilësinë) e vërtetë të saj siç është i regjistruar në video.

Kjo teknikë duhet të përdoret vetëm kur nuk ekziston asnjë mundësi tjetër, ose vetëm për qëllime ilustruese apo si masë paraprake për sigurimin e pamjeve.

7. Përfundime

Sistemet e kamerave të sigurisë (CCTV) ose siç njihen ndryshe videoregjistruesit dixhital (DVR), kanë të instaluar programet e tyre përkatëse për eksportimin e pamjeve filmike nga hard disku apo memoria ku ato ruhen. Por, në rastet e dëmtimit të këtyre pajisjeve, kyçjes me fjalëkalim të panjohur, keqfunksionimit të tyre apo fshirjes së pamjeve filmike, rikuperimi i këtyre pamjeve është një proces mjaft kompleks dhe shpeshherë sfidues.

Ky prezantim njeh ekspertët e ekzaminimeve kompjuterike me teknika të avancuara për rikuperimin e pamjeve filmike direkt nga hard disku i këtyre pajisjeve në nivel "*raw*" pa u bazuar në file-system. Këto teknika janë e vetmja mënyrë për të rikuperuar pamje filmike sidomos në dy raste; së pari kur nuk është e mundur kopjimi (eksportimi) i pamjeve bazuar në *file-system* pavarësisht se pamjet filmike nuk janë fshirë dhe së dyti kur file *system*-i është funksional dhe ekzistojnë mjetet për ta lexuar (vetë DVR-ja apo ndonjë program i posaçëm), por pamjet filmike janë fshirë.

Gjithashtu ato janë një mjet mjaft i mirë për verifikimin e të dhënave të nxjerra me programe të tjera apo nga vetë pajisja për të pasur një siguri prej 100% se as edhe një fragment pamjesh filmike me interes "nuk është lënë prapa" (pa u nxjerrë).

Megjithëse kjo metodë ka disa limitime të vogla (*aspect ratio*, humbja e disa *frame*-ve për shkak të *multiplexing*, etj.), pamjet filmike të rikuperuara janë pothuajse në çdo rast në të njëjtin kualitet me të cilin kanë regjistruar kamerat. Metodat e mësipërme me pak modifikime mund të adaptohen mbi shumicën e këtyre lloj pajisjesh. Pamjet filmike të përftuara nga pajisjet DVR përgjithësisht nuk shquhen për cilësi të lartë e madje në shumë raste ato janë në cilësi të ulët e të degraduara nga faktorë të ndryshëm si ndriçimi, fokusimi jo i qartë, cilësia e kamerave, kompresimi, etj. Aktualisht ekzistojnë shumë programe e teknika që mund të ndihmojnë për rritjen e cilësisë së tyre, për të nxjerrë në pah detaje e karakteristika identifikuese, apo për të dhënë një tablo më të qartë të asaj se çfarë ka ndodhur.

8. Rekomandime

- Metodat dhe teknikat e rekomanduara në këtë punim, për rikuperimin e pamjeve filmike, aplikohen vetëm në rastet kur kopjimi (eksportimi) i pamjeve filmike nga këto pajisje është i pamundur apo kur kërkohet për pamje filmike të fshira (edhe pse pajisja është funksionale apo një program kompjuterik që lexon file *system*-in e hard diskut të tyre është i disponueshëm).

- Kjo metodë rikuperimi duhet përdorur me mjaft kujdes. Një gabim i vogël në dekodimin e saktë të *metadatave* apo në shkrimin e *script*-eve, mund të çojë në mosdetektimin, e për pasojë mosrikuperimin, e pamjeve filmike me interes, edhe pse ato akoma ekzistojnë në hard disk (të fshira ose jo) apo në nxjerrjen e pamjeve të gabuara, apo me *metadata* të gabuara.

- Përdorimi i programeve për përmirësimin e cilësisë së pamjeve filmike të përftuara nga këto pajisje, duhet të bëhet vetëm nga specialistë me njohuri të posaçme dhe përvojë në këtë fushë. Përdorimi i gabuar i këtyre filtrave apo teknikave, çon në shtim apo heqje elementësh nga videoja apo fotografia, apo degradim të pamjes në vend të

përmirësimit të saj.

Megjithatë, këto programe jo gjithmonë japin rezultat dhe duhet të jemi të vetëdijeshëm kur kërkojmë aplikimin apo rezultate prej tyre. Ato janë efektive vetëm kur detaji është i fiksuar, pra gjendet në video ose foto, por që nevojiten disa filtra apo teknika për ta bërë të identifikueshëm apo më të qartë.

Bibliografia

1. A Million Words: Demystifying Video Carving from CCTV Systems ", Konferenca Enfuse 2018, Las Vegas SHBA. *Kastriot Gjoka, Chief of Computer and Audio-Video Forensic Sector, Scientific Police Institute, Albanian State Police & Bledar Kurti, IP Networking Systems specialist | Telecom Albania.*
2. *P*ërtej kopjimit apo rikuperimit automatik nga sistemet e kamerave të sigurisë (DVR), Konferenca e II-t Shkencore Ndërkombëtare "Shkencat Ligjore dhe sfidat e sigurisë", Akademia e Sigurisë Tiranë.*Kastriot Gjoka, Shefi i Sektorit të Ekzaminimeve Kompjuterike dhe Audio-Video në Institutin e Policisë Shkencore.*
3. What Lurks Beneath: Beyond Automated Carving.
4. Konferenca "Enfuse", 2017, (www.guidancesoftware.com/enfuse-conference/sessions).
5. *Kim Thomson, (Instructor/Examiner, H-11 Digital Forensics), Kastriot Gjoka, (Chief of Computer and Audio-Video Forensic Sector, Scientific Police Institute, Albanian State Police)*
6. SWGDE Best Practices for the Recovery of Data from Security Digital Video Recorders Containing H.264 Data.*Version: 1.2 (June 23, 2016).*
7. Advanced file carving-How much evidence are you ignoring.*Bas Kloet, Hoffmann Investigations September 2010.*
8. Analysis of Hikvision Date/Time *February 25,2016 / Jimmy Schroering /Forensic DVR Recovery, / DVR Forensics*
9. SWGDE Best Practices for the Recovery of Data from CCTV Digital Video Recorders Version: 1.0 (February 05, 2015)

Academy of Security

Third International Scientific Conference

Computer crime, cybercrime and national security

21 November, 2018
Tirana, Albania

ENGLISH

ABSTRACTS

"POLICIMI DHE SIGURIA", NR. 12, NOVEMBER, 2018

CYBER CHALLENGE. IT: NURTURING THE NET ITALIAN GENERATION OF CYBER-EXPERTS

- Alberto Marchetti SPACCAMELA, Emilio COPPA, Daniele Cono D'ELIA, Camil DEMETRESCU and Paolo PRINETTO

ABSTRACT
Cyber security Ventures forecasts there will be about 3.5 million cyber security job openings by 2021. Filling the talent gap in the area is of the essence, requiring timely coordinated efforts by educators, companies, and governments. In this paper, we describe Cyber Challenge.IT, a talent scouting program in cyber security for students 16-22 prototyped at the Cyber Intelligence and Information Security Center of Sapienza University of Rome in 2017 and extended to 8 Italian universities in 2018. The program, organized by the CINI National Laboratory of Cyber security with the support of the Italian Intelligence System for the Security of the Republic, aims to attract bright students to the fast-growing cyber security domain, addressing its unique intellectual challenges and career opportunities. In 2018, the program received about 1900 registrations and selected 160 promising students from high schools and universities all over the country, who participated in a 3-months training program covering a broad spectrum of topics in
Cyber security. The program culminated in a final national capture-the-flag competition among the 8 Italian teams formed by the best students of each Cyber Challenge.IT site. Winners of the national competition were selected to form the Italian National Cyber security Team, which represented the country at the European Cyber security Challenge 2018.
Keywords: cyber security, training, CTF, education, skill shortage.

ALBANIAN SOCIETY PERCEPTIONS FOR COMPUTER CRIME AND CYBERNETIC SECURITY

- PhD. Xhavit SHALA

ABSTRACT
The purpose of this paper is to scan, analyze and evaluate perceptions of the Republic of Albania citizens on cybernetics and security in Albania. The data used in this paper is provided through a survey conducted with broad participation of citizens, who belong to different strata and professions. Such data informs us on the perception of citizens about the role and impact of information and communication technology, in relation to society and the individual; the level of knowledge on criminal offenses in the computer field and the threat of cybercrime, the level of cyber security and their perceptions about the legislation of the investigation of this crime, as well as the ways of its prevention. By analyzing these perceptions, it is aimed at identifying the issues, influencing factors, and providing recommendations for improving policies to prevent and reduce them, with the view of further improving the process of policing based on intelligence and our national security.
The increase of the level of social and commercial interaction through electronic communication and not only, as well as the tendency of the economic development to lean towards advanced technologies irreversibly increases dependence on technology, which now based on the grounds gained, requires a collaborative approach

to achieve avoiding the use of technology, contrary to the main purpose. But, since there is an endless list of usefulness that the Internet and cyber space offers, also there exists a presence of social and commercial interactions threatens.
Internet has also given criminals a platform to grow and spread themselves in cyberspace. Today we cannot talk separately about cybercrime or cyber security, but about cybercitizens - digital citizens, and families, societies, organizations, nations, criminals, threats and security, all together in a cyber space.
This rapid development of mass communication in the cyber space (virtual), especially after 2000, puts a new problem for the structures of the State Police, other law enforcement agencies and security structures, and a progressive increase in criminal offenses in the computer field, but also in cyber threats. In our country, in 2017, as compared to 2010, there were 3.3 times more criminal offenses in the field of cybercrime and a level of discoverability of only 27%. Meanwhile, cyber threats/ attacks have significantly increased, as a deliberate attempt to access, manipulate, interfere with or impair the integrity, confidentiality, security or availability of computer system data without the legal authority to do so.
Under these conditions, identification of cybercrime issues that are related with cyber security is indispensable, influential factors, ways of coping with the aim of providing recommendations for improving policies to prevent and reduce cybercrime and enhance cyber security.
In its function, a broad survey of different strata and occupations of Albanian society has been organized and analyzed their perceptions of the role of information and communication technology in relation to society and the individual; the level of their knowledge of criminal offenses in the computer domain, the cybercrime threat and the cyber security levels well as their perceptions about the legislation, the investigation and the ways of preventing these criminal offenses and not only.
During this paper, basic research methods and instruments have been applied. The findings of this paper fully corroborate our hypothesis that cybercrime and cyber threat continue to spread in Albania among other things and due to the lack of awareness and the education of social strata with the risk of uncontrolled and unsafe use of the Internet and of the information and communication technology.
At the end of the paper an approximate prognosis of further developments is made and relevant policy development recommendations are made to improve ongoing work on the treatment, management, prevention and reduction of crime and cyber threat in our country.
Key words: criminal offense in computer field, cybercrime, internet, survey, target group, cyber security, cyber attack, education, training.

THE IMPORTANCE OF PROTECTING CRITICAL INFORMATION INFRASTRUCTURES - THE CASE OF ALBANIA

- PhD. Vilma TOMÇO, MSc. Klorenta PASHAJ

ABSTRACT
Protection of information infrastructure is a priority area since the creation of the Internet to the present day when attacks on critical information systems affect every critical sector. The functioning of critical systems is closely related to the information infrastructure, while the interruption of the latter's functionality hampers the functioning of the system itself.

Developed countries have managed to implement measures to protect critical information infrastructures, but these solutions are not always suitable for developing countries, or for countries such as Albania.
With the adoption of a list of critical and important information infrastructures, there is a need to draft a document that includes measures to protect the systems and ensure continuity of work, following cyber attacks that can be identified.
Protecting Critical Information Infrastructures is a shared responsibility of the public and private sectors. Although there is no approved strategy published for the protection of critical information infrastructures, the drafting of regulations and the pursuit of best practices diminishes the threatening factors and reduces the risk of cyber attacks. National / state and sector CERT teams are coordinating bodies in the protection of critical information infrastructures by taking action to prevent attacks, and by acting reactive in dealing with incidents. Following the occurrence of a cyber attack, it is recommended to interact between sectoral CERTs and national CERTs for the most effective crisis management. In Albania, the National Authority for Electronic Certification and Cyber Security (AKCESK) acts as a national CERT. Also, co-operation with other international organizations and awareness-raising / training programs can greatly reduce threats to Critical Information Infrastructures.
This article highlights the need to protect critical information infrastructures and develop their protection practices, underlining the requirements in Albania's case by critical sectors, in line with the national and European regulatory framework for cyber security.
At the end of this paper are presented the conclusions drawn and some recommendations for a better approach of the strategies for the protection of critical information infrastructures, achieved as a result of the findings made during the preparation of the paper.
Key words: critical information infrastructure, critical systems, safeguards, critical sector, CE

CYBERCRIME AND CYBER THREATS AFFECT NATIONAL SECURITY

-PhD. Bajram IBRAJ

ABSTRACT
The world has come to a very rapid development of mass communication in the cyber space (virtual) as a result of the rapid development that technology has brought. Computer grafts have nowadays been identified as the newest and the most common forms of criminality. This new form of crime is difficult to document and be investigated, and as a consequence the scale of detection and punishment is low. Cyber security is one of the strategic goals and important part of the national security of Albania.
The study aims to address the legal aspect, the criminal procedure of investigation and trial of cybercrime, the identification of the main problems and challenges in combating cybercrime in Albania, the cybercrime forms, the cyber threats and national security violations.
The analytical model and methodology of this study is fully in line with the ultimate goal of research. The study spans theoretical, legal, professional and methodological dimensions used to answer the research question and to accomplish the purpose of the study is the analytical methodology based in Albania, combining qualitative and

quantitative methods. The research model on which the study is based is a theoretical and comparative analysis focused on the regional context, Albania.
This study through analyzing and confronting with literature, legal aspects of statistical data, national cyber security strategies and national security aims to raise awareness of state institutions on the importance of protecting the national security of the state and Albanian citizens from the dangers posed by cybercrime. This study is focused on some key aspects of cyber crime, as well it draws conclusions and recommendations on measures to be taken to combat cybercrime more effectively in Albania.
Key words: Cyber space, cybercrime, computer threats, national security, cybercrime strategy.

CYBERNETICS AS A HYBRID INSTRUMENT OF STATES INTELLIGENCE SERVICES TO ACHIEVE BOTH OLD AND NEW GOALS

-PhD. Mimoza XHARO

ABSTRACT
Cyber space in evolution, rapid growth and extension, is becoming a new target area of hydride threats such as, cybercrime, cyber terrorism and cyber espionage. State and non-state actors are preferring this space to administer, transmit communicate on their activity. Collection of sensitive data by using cyber space is converting to one real tool with high level of use from the state/intelligence services or other non-state actors/entities acting on their behalf. The use of cyber space for espionage purposes appears to be more sophisticated, designed to cover the identity, originating state or actors on their behalf. This form of collection, dissemination, and disinformation is implying to the economies, social cohesion, political relationships, security architecture. Cyber espionage is being identified as used not only in global level, but also in our region where global actors such as, Russia, China, Iran etc., are active on their strategic interests related to political developments, interstate unresolved problematics, orientation/steps toward Euro Atlantic integration, economy developments, democratic reforms etc. A part of continuous presence and activity through classic means of espionage, there are engagements on propaganda activity, disinformation and cyber espionage. Countering this new reality requires a clear understanding of the threats and an approach highlighted by renewed national commitment and increased investment. This paper provides a reference for all those desiring to know more about or charged with dealing with this significant national security problem.
Furthermore, helps the public in general understanding of cyber espionage, its motives, methodology, the raising concern of its impact to security and necessity to clearly address aspects of protective measurements and capabilities.
Key words: cyber space, cyber espionage, threats, national security.
PhD. Fejzi Lila – “Cyber crime and its management – Albanian Approach!”.
Abstract
Currently, cyber crime is one of the biggest challenges facing emerging societies, where Albanian society is currently. Developments in communication technology and expanding internet usage, especially in recent decades, have brought about an evolution and openness to positive and negative phenomens of users. Current statistics on internet users point out that globally around 4.5 billion people are online.
Cyber space poses a major social challenge, affecting the appearance of other forms

of crime from traditional approaches to currently unknown ones. The environment, web and communication innovations make it possible for cybernetics and its users to report to individuals, property, organizations and societies.
Referring to the challenges, global openness to these phenomena of Albanian society requires more general reconciliation and more frequent adaptation as part of the National Security Strategy. Albanian environment and reality is evolving, requires functional membership, law-enforcement structure and contemporary legal basis, human capacities and clear strategies. These measures, reflected in the National and Cybernetic Strategies, are less part of national traditional domestic approaches, even more alternating with external approaches, referred to academic approach and international partners, particularly to the EU, NATO and the US.
In recent decades, the Albanian reality is faced by deliberate and deliberate efforts to gain access, manipulation, interference, damage to integrity and confidentiality from individuals or subjects without the right legal authority to exercise.
Cybercrime management raises a lot of dilemma. These dilemmas relate to the reference object, the state and the person. The state as a traditional and territorial approach, while the individual is subject to the freedom, access and the right to exercise and benefit from technology and information innovations. The cyber-challenge relates to the state's report on the protection of its own statesmen and the holding of responsibilities to prevent, react and rebuild.
Key words: cybercrime and management, national security and cyber space, Albanian society and legitimacy.

NEW CHALLENGES AND ACHIEVEMENTS AGAINST CYBERCRIME IN THE WESTERN BALKANS AND ALL AROUND THE WORLD

- MSc. Qetsor GURRA

ABSTRACT
The focus of this topic is to address the risk of cybercrime. Initially, it will be treated the latest data from international organizations and state institutions. In this form it will be highlighted the most prominent issues by analyzing the sophisticated change that has suffered this ghostly criminal act recently. Next it will presented concrete picture in the region and international rank regarding the level of discovery, taking legislative measures, infrastructure and professionalism. Of particular importance will be the approach to the goals and objectives of the European Union being a standard example that should be taken into account in our country. Finally, the theme will come up with efficient recommendations taking into account the past six years of the Republic of Albania's graphs, which are a far-reaching reality to be desired. The treatment aims to highlight the different policies that embrace each country depending on development and well-being, helping us to consider alternative examples of improvement and change of situation in our favor.
Key words: cybernetics, implementation, eficence, legal provisions, improvement etc.

INTERNATIONAL COOPERATION ON THE PREVENTION OF CYBER ATTACKS

-PhD. Eldjona SHUKALLARI

ABSTRACT

Information and communications technology (ICT) presents one of the most critical modern challenges to global security. In a more digital and interconnected world, protecting EU citizens from cyber threats is the main priority. The new proposed measures aim to enhance cyber security co-operation within the EU and globally, foster innovation and invest in awareness building and capacity building. In parallel, the EU and NATO are carrying out coordinated exercises to test their ability to respond to cyber threats and hybrids.

The key cyber security threats require urgent international co-operation. Indeed, cyber threats are more diverse and complex, often targeting private companies and risking the technical integrity of the digital world.

Recent legislation, such as the European Parliament's 2016 Directive for the Safety Network and Information Security, was widely focused on threats to critical infrastructure and aimed to improve cyber security to protect so-called basic services such as online markets, search engines and information services that are vital to businesses, governments, and citizens.

The EU approach to cyber security gives priority to resolving disagreements in cyber space by peaceful devices. However, the EU will increase its capacity to respond to cyber threats. Where it is necessary, restrictive measures can be taken in response to malicious cyber activities ".

CYBER TERRORISM

-MSc. Enea SHEQI

ABSTRACT

Using the internet in the globalized world alongside all the positive innovations has brought some negative consequences. Cybercrime seems unavoidable, but the reaction to it is indispensable and immediate. Terrorist acts in recent times are on the rise and are trying to find new forms and ways. The use of electronic space to commit these crimes is serving even more terrorists around the world. The challenge to this work is comprehensive and the response to the prevention of cyber terrorism requires cooperation at international level to further combat the spread of this sophisticated crime. In this paper will be a thorough analysis of the cyber terrorism, the forms and ways of its execution, the Albanian and international legal framework fighting and preventing it, as well as the requirements for long-term strategic planning to protect order and national security. It will also be a cross-national comparison to take the best practices of fighting against terrorism and cybercrime.

Key words: Cyber terrorism, prevention, strategy, national security.

THE NEW CONCEPT OF VIRTUAL BORDERS AND NATIONAL PUBLIC SECURITY THREATS

- MSc. Valeria BARDHAJ

ABSTRACT

We are used to read, discuss, or write about traditional crimes like murder, theft, kidnapping, etc. With the evolution of science and technology especially in the facilities offered by the computer and the fact that the Internet is already a global communication tool, in recent years crime related to fraud, viral attacks, juvenile pornography, as well as hate crimes are highly increased.

Today cybercrime is considered one of the major problems and challenges of many governments. Albania is ranked as one of the countries where technology development is growing fast, and as a consequence the cybercrime risk is vast. Such a potential risk is absolutely a breach of national and public security. For this reason, the focus of this paper will be closely linked to policies designed to identify potential risks, based on legislation, conventions, and government-backed structures to combat this crime.

The virtual world has now turned into one of the favorite spaces of anyone, even the governments have described as a good means of communicating with the public using it to provide a range of public services.

Although digitalization has provided many facilities, by the other side the risk of pirate attacks has increased. These attacks harm the data exchange, the banking system, or even the public sector. International partners pointed out that Albania was not ready to cope with such a phenomenon, so one of the key conditions for EU integration was directly related to the development of cyber security policies (Chapter 24, Justice, Freedom and Security). Even as a fully-fledged NATO member, Albania is tasked with expanding cyber defense for national networks and infrastructures.

Cybercrime has far more powerful features in spreading and extremely complex (compared to traditional crimes), which cause difficulties in law enforcement.

In conclusion, this paper will focus on a series of successful recommendations and practices on raising the awareness of the state, law enforcement agencies and citizens about the threats of cybercrime.

Key words: national security, cyber security, legislation, digitalization.

CYBER SECURITY AND TERRORISM

-PhD. candidate Flora DAKO

ABSTRACT

Nowadays, information, handled in all possible forms, electronic or traditional, is a real asset for individuals as well as for private or state organisms and is considered as a strategic resource by which is being developed what today is called society of information. The way of receiving and giving information differs from one place to another due to the fact of the possibilities of implementing models and new ways of communication. We see that at a one-year timeframe, technology and information varies with unpredictable progress. We can call this a fearless need or a society's need for successive changes, but without thinking of the impact that these changes have on the security of our lives and our children as well. In telecommunication

technology across the globe most used is the internet, which serves as a source of data for any questions or queries we have. But in many cases search has been fatal in the destruction of personal, organizational or state data, through manipulation, deletion, modification, and surveillance of any information circulating in communication networks. Thus, the security of information is directly related to the sovereignty of the individual, social groups or a state, which is realized by the protection of critical infrastructures, systems and networks, the cultural heritage of the nation and goods, namely in protecting the values. If we are knowledgeable and have a culture in how to deal with changes in online communication, then we will be more prepared and able to avoid the devastating actions of any kind of information we have, from personal to the national one.

Key words: Communication, security, terrorism, defense

CYBERCRIME AND KEY TYPES OF CYBERCRIME

-Expert/MSc. Marco Saracchi, PhD. Bajram Ibraj, MSc. Patrizio Mazzacane

ABSTRACT

The procedure followed to combat cybercrime according to European standards GDPR EU 679/2016 and in accordance with international standards: ISO 27002: 2007, ISO 27001: 2005, NERC, NIST, BSI IT, ISO 15408.

The term cybercrime identifies a criminal activity characterized by the use of computer technology, whether hardware or software, to commit one or more crimes.

This is a criminal activity that includes the information technology structure, including illegal entry (unauthorized access), interception (by means of technical means of non-public broadcasting of computer data from or within a computer system), data interference (damage, deletion, deterioration, alteration, or elimination of computer data), interference systems (interference in the operation of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or deleting computer data), identity thefts and electronic scams.

Key Words: cybercrime, computer forensic, hacking, web intelligence, IT compliance, phishing.

BIOMETRIC SYSTEMS AND THEIR PROTECTION THROUGH SYNTHETIC MODELS: MEASUREMENT AND COMPARISON BETWEEN AUTOMATIC AND PERCEPTIVE TECHNIQUES OF ATTACKERS

- Associate Professor Edlira Martiri

ABSTRACT

In high-security environments, data protection and information leakage prevention remain one of the key challenges. For example, in biometric systems, its most sensible information, the template, is continuously exchanged, transferred, processed between and from the blocks of an information system managing the biometric material. In this system, the personal identifier of each subject, such as name, ID, or any other element, as well as its biometric template, are stored in the database module. The question we ask in this paper is: instead of having only one biometric characteristic for a user, can we keep a set of templates where only one is real and the others synthetic to disguise it? If a potential intruder acquires these templates by acquiring

the database material, is he able to reconstruct and distinguish synthetic templates from the real ones?
To this question we try to find answers in this paper. Here we present a biometric protection scheme, and to test that these two types are for indistinguishable for the intruder, we suppose an attack. To measure how successful the intruder is, we reconstruct and classify the pre-images by means of two techniques: visual and automatic. For the former, we have built a platform where human testers can classify several images rebuilt from real or synthetic patterns. From the viewpoint of the attacker experiments show that, compared to the automatic classifier, human testers perform better in precepting and distinguishing templates.
Keywords: biometric synthetic template; database leakage; human classification; face recognition; PCA

COMPUTER SPACE. THE SITUATION OF CYBER ATTACKS IN ALBANIA

- PhD. candidate Arqilea Koça, MSc. Arjan Muçaj

ABSTRACT
Extraordinary advances in technology and the global reach of the internet during the past 30 years have made computer crimes easier and more consequential.
As the world economy has become dependent on technology, it has become more and more exposed to cyber attacks.
Evolution of cyber crime has changed the traditional concepts in the judicial and national security fields. Most significantly, growth of the cyber sphere and advances in technology have led to fundamental change in the definition of criminal jurisdiction, by removing national borders on prosecution of cyber crimes.
National security has long built on military power, in particular military weapons and personnel, but in the age of technology the traditional soldier is being replaced by computer programs.
In 2015, American President Barack Obama declared the cyber threat as "one of the most serious economic and national security challenges [US] face as a nation."
As developing countries catch up to the western world in terms of their technological development they are increasingly facing the same fundamental economic and security threats.
This paper offers a general overview of the threats that cyber crime poses to Albania's national security and a comparative analysis of legal response to computer crime in Albania.
Keywords: cyber attack, computer crimes, cyberspace

OPEN RESOURCES CYBERNETIC INVESTIGATION: IMPACT ON NATIONAL SECURITY

- PhD. Hergis Jica

ABSTRACT
Law enforcement institutions have the primary role of maintaining order, law enforcement, citizen protection and the prevention, detection and investigation of crime. Open Source Investigation can provide significant skills for law enforcement

institutions and security services to supplement and improve their investigative capabilities as the ability to rapidly collect and correctly process, document and analyze data of open resources can be an important aid during investigations and used for strategic planning at national level to combat crime. Monitoring the network deliberately and legally and then analyzing and presenting data obtained from open sources should be considered as a mandatory requirement for any national security strategy. Law enforcement institutions at the same time need to consider collaborations with public and private partners including and through the implementation of new network data structures, equipment and methods for data security and protection for citizens. The open source investigation has gained considerable importance in recent years. Traditionally, information and its acquisition has been the secret detection method using a closed collection and analysis system. Although open sources are often used in the process of gathering information, their value is always seen as "medium". Classified information is increasingly valued and trusted. Systematic appropriation and the use of non-classified information was rarely seen as an intelligence priority but, today, the importance of open source inquiry has been widely accepted. Today, it is estimated that the open source investigation offers up to 90% of the information used by law enforcement institutions but with an indisputable value in terms of national security.

Keywords: source, security, cyber, information, investigation, national

AN INTEGRATED APPROACH TO CCTV FORENSIC INVESTIGATION

- MSc. Kastriot Gjoka, MSc. Bledar Kurti

ABSTRACT

Video evidence can be found at more locations than ever before, CCTV systems nowadays are almost everywhere. With the wide application of video surveillance, closed circuit television (CCTV) footage plays a key role in crime investigation; more crimes are now being solved by using security camera video records as evidence. Exporting video footage from security cameras, in some situations is complex process and requires advanced knowledge and techniques. Investigators may face different problems: the DVR device does not work; the device is password protected; the video files have been deleted or corrupted; the DVR's hard disk has been formatted, the file system or index got corrupted, etc.

Most of DVRs use proprietary file systems, which are recognized neither from operating systems (Windows, MAC, and Linux) nor from traditional forensic tools, so identification of video recordings on their hard drives is not easy.

During several years of researches, we have studied the structure of the video files for many DVR brands and models.

The method we will present, gives a definitive conclusion whether or not, a single frame from the video of interests exists in a DVR system, and if it does, carve it out in a readable format.

Our method does not rely on file system of hard drive or DVR index; it scans and analyzes the hard drive content at the frame level.

Using Python scripts or some powerful features of En Case we can automate the process of scanning for every possible period of seconds of video files, creating a list of overall results in any format (csv, txt , etc) with camera number, date and time for every second and the forensic path(offset). And if there is a time period of interest,

exporting video records in a readable format.
The big challenges for video forensic analysts are multiplexing. We will explain how to separate multiplexed video footage into individual camera views in semi automated way by using EnCase, or fully automating the process with Python scripts.
In many cases the quality of CCTV recordings is poor due to several factors and need to be processed and analyzed in order to restore specific defects or clarify image features to make them as clearly as possible. Filters to restore moving objects, zooming, improving dark areas, correcting the perspective of objects, etc, needs to be applied.

ISBN 978-9928-210-08-1
ISSN 2413-1334
AKADEMIA E SIGURISË

AKADEMIA E SIGURISË
Qendra Kërkimore Shkencore
Rruga e Elbasanit, Sauk, Tiranë

POLICIMI DHE SIGURIA
NËNTOR 2018
NR
12