REPUBLIKA E SHQIPËRISË
KËSHILLI I MINISTRAVE

# VENDIM

**Nr.** 1084 **, datë** 24.12.2020

**PËR**

## MIRATIMIN E STRATEGJISË KOMBËTARE PËR SIGURINË KIBERNETIKE DHE PLANIT TË VEPRIMIT 2020-2025

Në mbështetje të nenit 100 të Kushtetutës, me propozimin e Zëvendëskryeministrit, Këshilli i Ministrave

**VENDOSI:**

1. Miratimin e Strategjisë Kombëtare për Sigurinë Kibernetike dhe planit të veprimit 2020-2025, sipas tekstit që i bashkëlidhet këtij vendimi dhe është pjesë përbërëse e tij.

2. Ngarkohen Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike, ministritë e institucionet e tjera përgjegjëse të përcaktuara në strategji dhe në planin e veprimit për zbatimin e këtij vendimi.

Ky vendim hyn në fuqi pas botimit në "Fletoren zyrtare".

**KRYEMINISTRI**

**EDI RAMA**

**Në mungesë dhe me porosi**

**ZËVENDËSKRYEMINISTRI**

**ERION BRAÇE**

ZËVENDËSKRYEMINISTRI

ERION BRAÇE

## Strategjia Kombëtare për Sigurinë Kibernetike 2020-2025

Strategjia Kombëtare për Sigurinë Kibernetike, që duhej t'i ishte bashkëlidhur vendimit nr. 1084, datë 24.12.2020, të Këshillit të Ministrave, "Për miratimin e Strategjisë Kombëtare për Sigurinë Kibernetike dhe planit të veprimit, 2020–2025", botuar në Fletoren Zyrtare nr. 233, datë 30.12.2020.

PËRMBAJTJA



PJESA I: KONTEKSTI STRATEGJIK

1. HYRJE

Në dekadat e fundit, zhvillimi i internetit, si dhe ndryshimet inovative në teknologji, kanë sjellë ndryshime rrënjësore dhe sfida në çdo shoqëri në mbarë botën. Jetët tona të përditshme, të drejtat e njeriut, ekonomitë dhe ndërveprimet shoqërore, ndikohen thellësisht nga teknologjitë e informacionit dhe komunikimit. Një hapësirë e

përbashkët dhe e lirë kibernetike, promovon përfshirjen sociale dhe politike, thyen barrierat e komunikimit midis vendeve, komuniteteve dhe qytetarëve, siguron transparencë, duke lejuar ndërveprimin dhe shkëmbimin e informacionit dhe ideve në kohë reale në të gjithë globin. Të gjitha zhvillimet dhe rritja e përdorimit të teknologjive së informacionit dhe komunikimit, vijnë me përfitime të mëdha dhe në të njëjtën kohë sjellin kërcënime, prandaj mbrojtja kibernetike dhe siguria janë vendimtare.

Në hapësirën kibernetike, ekzistojnë përpjekje të vazhdueshme nga individë dhe grupe të ndryshme me interesa keqdashës, të cilat ndikojnë në mbarëvajtjen dhe funksionimin e shteteve. Ndërhyrjet e privatësisë, vjedhjet e identitetit, janë gjithashtu një problem në rritje dhe shumë shqetësues për të gjithë shoqërinë.

Nga njëra anë, qeveria po investon gjithnjë e më shumë në infrastrukturën digjitale, për të ofruar shërbime digjitale për qytetarët. Nga ana tjetër, qytetarët po e përdorin internetin gjithnjë e më shumë për shkak të avantazheve që ofron.

Shqipëria, si një vend në zhvillim, mbështetet, gjithashtu, në teknologjinë e informacionit, duke synuar rritjen e nivelit të jetesës dhe përmirësimin e shërbimeve publike. Krahas përfitimeve nga përdorimi i teknologjive të reja digjitale, përdorimi i internetit sjell problematikat e veta në lidhje me sigurinë kibernetike. Kërcënimet kibernetike, duke përfituar nga dobësitë teknologjike ose mungesa e njohurive në përdorimin e mirë të këtyre mjeteve, janë gjithnjë e më shumë në rritje, duke cenuar sigurinë e sistemeve të informacionit.

Një prej sfidave aktuale dhe të vazhdueshme për të gjitha vendet është ndërtimi i një shoqërie të zhvilluar digjitale dhe të mbrojtur kibernetikisht, të pajisur me njohuritë dhe aftësitë e nevojshme, për të maksimizuar përfitimet dhe për të menaxhuar rreziqet.

Në "Strategjinë e Sigurisë Kombëtare, 2014–2020" dhe në "Dokumentin e Politikave për Sigurinë Kibernetike, 2014–2017", Shqipëria ka ndërmarrë hapa të rëndësishëm, për të përmirësuar situatën e sigurisë kibernetike. Krahas zhvillimeve, në fushën e teknologjisë së informacionit dhe revolucionit mbi digjitalizimin e shërbimeve publike, është plotësuar dhe përmirësuar kuadri ligjor për sigurinë kibernetike.

Falë këtij progresi, Shqipëria është përmirësuar në Indeksin Global të Sigurisë Kibernetike krahasuar me vitin 2017, nga 89, në 62, në mbarë botën dhe 36 në nivel evropian.

Gjithsesi, ky progres, ende nuk ka arritur në shkallën dhe ritmin e ndryshimit të nevojshëm për të qëndruar, përpara lëvizjes dhe evolucionit të shpejtë, që vjen nga kërcënimet e ndryshme kibernetike. Pa dyshim, sulmet kibernetike janë ndër kërcënimet më të rëndësishme të sigurisë për botën moderne dhe për këtë arsye siguria kibernetike, është bërë një pjesë e rëndësishme e sigurisë kombëtare. Për këtë arsye, hartimi i Strategjisë Kombëtare e Sigurisë Kibernetike 2020–2025", është një domosdoshmëri, për ngritjen e mekanizmave të duhur institucionalë, me qëllim rritjen e nivelit të sigurisë kibernetike në vend.

Në përmbushje të angazhimeve qeveritare, si dhe në koherencë të plotë me zhvillimet strategjike të vendeve të zhvilluara, për një mjedis kibernetik sa më të sigurt, kjo Strategji do të mbështetet në parimet themelore të mëposhtme:

- zbatimi i vlerave të njëjta themelore në botën fizike dhe digjitale;
- mbrojtja e të drejtave themelore, liria e shprehjes, të dhënat personale dhe privatësia;
- qasja për të gjithë;
- qeverisje demokratike dhe efikase;
- përgjegjësi e përbashkët në garantimin e sigurisë kibernetike.

2. VLERËSIMI I SITUATËS AKTUALE NË SHQIPËRI

Vlerësimi i situatës aktuale për sigurinë kibernetike në Shqipëri është kryer në bashkëpunim me institucionet përgjegjëse dhe është mbështetur në 4 shtylla si më poshtë:

1. Situata e sigurisë kibernetike;
2. Korniza ligjore e sigurisë kibernetike;
3. Internet i sigurt për fëmijët;
4. Edukimi, hulumtimi dhe trajnimi në sigurinë kibernetike

**2.1. Situata e sigurisë kibernetike**

*2.1.1 Infrastrukturat kritike të informacionit*

"Strategjia e Sigurisë Kombëtare", e miratuar në vitin 2014, ka përcaktuar kornizën dhe shtyllat në nivel kombëtar për rritjen e sigurisë në vend. Si një vend në zhvillim pa infrastrukturën e nevojshme ligjore për sigurinë kibernetike, kjo fushë është zhvilluar vetëm dy vitet e fundit, gjatë së cilëve janë identifikuar infrastrukturat kritike dhe të

rëndësishme të informacionit në sektorin publik dhe atë privat. Gjithashtu, janë hartuar masat minimale të sigurisë që duhet të aplikohen, për rritjen e nivelit të sigurisë kibernetike në këto infrastruktura dhe është ndërtuar mekanizmi metodologjik, për ngritjen dhe funksionimin e CSIRT-eve sektorialë në nivel kombëtar.

Kuadri ligjor i lidhur me sigurinë e komunikimeve elektronike, plotësohet me rregullimet ligjore për sigurinë dhe integritetin e rrjeteve të komunikimeve elektronike, rrjetet e telekomunikacionit, të cilat janë pjesë e ligjit nr. 9918, datë 19.5.2008, "Për komunikimet elektronike në Republikën e Shqipërisë", të ndryshuar, i cili ka transpozuar direktivat e BE-së për komunikimet elektronike.

Korniza ligjore për sigurinë kibernetike ka përcaktuar, gjithashtu, Autoritetin Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK), si autoritet përgjegjës për mbikëqyrjen e zbatimit të ligjit.

Përkatësisht, situata aktuale lidhur me sigurinë në infrastrukturat kritike të informacionit, në **sektorin bankar**, me implementimin e ligjit për sigurinë, është përmirësuar krahasuar me dy vite më parë. Në këto infrastruktura, janë aplikuar masa sigurie të konsiderueshme, të cilat janë aprovuar nga AKCESK, si dhe janë ngritur CSIRT-et sektoriale, duke krijuar kështu një mjedis të sigurt kibernetik.

Siguria kibernetike, **në sektorin financiar,** e ndarë në dy shtylla, përkatësisht në atë publike dhe private, paraqitet si më poshtë:

Në infrastrukturat qeveritare kritike të informacionit që përdoren nga institucionet publike, përkatësisht të alokuara pranë qendrës së të dhënave qeveritare, dhe që menaxhohen nga Agjencia Kombëtare e Shoqërisë së Informacionit, aplikohen të gjitha masat e sigurisë konform legjislacionit në fuqi dhe standardit ISO 27001. AKSHI është CSRIT sektorial qeveritar dhe është certifikuar me këtë standard në vitin 2018 dhe mbi çdo infrastrukturë qeveritare nën administrim të AKSHI-t, aplikohen politikat e standardit ISO 27001.

Për sa u përket infrastrukturave kritike, që administrohen nga operatorë privat, janë në proces identifikimi dhe në disa raste edhe investimi për t'u ngritur.

**Në sektorin e shëndetësisë**, të ndarë në dy shtylla, në atë publik dhe atë privat, situata kibernetike paraqitet si më poshtë:

Infrastrukturat kritike të administruara nga operatorët/institucionet publike, kanë implementuar masat e miratuara, në zbatim të ligjit për sigurinë, të cilat kanë ndikuar në rritjen e nivelit të sigurisë kibernetike. Gjithashtu janë ngritur grupet përgjegjëse, për menaxhimin dhe trajtimin e incidenteve, të cilat në mungesë të kornizës ligjore, kanë qenë inekzistente.

Për sa u përket infrastrukturave të informacionit, që administrohen nga operatorë privatë, të cilat konsiderohen si infrastruktura kritike, në kuptim të kornizës ligjore të miratuar nga Komisioni Evropian, për rrjetet dhe infrastrukturat e informacionit, janë të paidentifikuara dhe sipas studimit të situatës, nga autoriteti përgjegjës, nuk përmbushin, gjithashtu, elementet e sigurisë, që duhet të garantojë një infrastrukturë kritike.

**Sektori energjetik.** Aktualisht, të gjithë operatorët e sistemit energjetik si në prodhim, në transmetim dhe në shpërndarje janë, duke implementuar teknologji inovative të mbështetura mbi sisteme kompjuterike dhe rrjete transmetimi të të dhënave, për menaxhimin dhe optimizimin e proceseve teknologjike. Në të tria elementet e sistemit energjetik është implementuar ose planifikohet të implementohet sistemi SCADA, si dhe kanë qendrat e tyre të operimit dhe të ruajtjes së sistemeve kompjuterike dhe, po ashtu, rrjetet e transmetimit të të dhënave. Gjithashtu, bashkë me leximin dhe analizimin e të dhënave të sistemeve energjetike në distancë, parashikohet që shumë shpejt të implementohen edhe modulet e operimit, të cilat automatizojnë procese të cilat aktualisht kryhen manualisht nga operatori. Kalimi në sisteme të pavarura, të cilat operojnë automatikisht padyshim do të kërkojë implementimin e masave dhe politikave të sigurisë, pasi impakti në rast të incidenteve kibernetike do të jetë shumë i madh. Kjo padyshim kërkon që fillimisht vetë operatorët në fushën e energjetikës në momentin e planifikimit të projekteve TIK dhe të automatizimit t'i kushtojnë një vëmendje të veçantë pjesës së sigurisë së sistemeve, si dhe të krijojnë procedura dhe kapacitete njerëzore të brendshme në funksion të sigurisë kibernetike.

**Në sektorin e transportit**, i cili përbëhet nga disa shtylla, gjendja paraqitet si më poshtë:

Infrastrukturat kritike të informacionit mbi *transportin ajror*, përmbushin detyrimet e rregullave minimale të sigurisë, si dhe kanë ngritur në strukturën përkatëse CSIRT-in sektorial.

Infrastrukturat kritike të informacionit mbi *transportin rrugor*, nuk përmbushin asnjë detyrim të rregullave minimale të sigurisë, përfshi këtu edhe ngritjen e CSIRT-it sektorial përkatës.

Për sa u përket infrastrukturave të informacionit mbi *transportin detar*, të cilat konsiderohen si infrastruktura kritike në kuptim të kornizës ligjore të miratuar nga Komisioni Evropian, për rrjetet dhe infrastrukturat, janë ende të paidentifikuara.

Gjithashtu, **në sektorin e ujësjellësit,** të cilët administrohen nga pushteti lokal dhe cilësohen si infrastruktura kritike të informacionit, ende nuk janë identifikuar si të tilla në kuptim të legjislacionit në fuqi për sigurinë kibernetike dhe në to nuk aplikohen masa sigurie.

Për sa i përket infrastrukturës digjitale dhe rrjeteve dhe/ose shërbimeve të komunikimeve elektronike, duke marrë parasysh që pjesa më e madhe e kërcënimeve dhe sulmeve kibernetike vijnë përmes rrjeteve të komunikimeve elektronike, çështjet e sigurisë kibernetike në këtë sektor ndiqen dhe janë nën përgjegjësinë e Autoritetit të Komunikimeve Elektronike dhe Postare (AKEP). AKEP-i, bazuar në ligjin nr. 9918, datë 19.5.2008, "Për komunikimet elektronike në Republikën e Shqipërisë", më specifikisht, neni 122 dhe në rregulloren nr. 37, datë 29.10.2015, "Mbi masat teknike dhe organizative për të garantuar sigurinë dhe/ose integritetin e rrjeteve dhe/ose shërbimeve të komunikimeve elektronike", kërkon marrjen e masave të duhura teknike dhe organizative për të garantuar sigurinë dhe integritetin e rrjeteve dhe/ose të shërbimeve të komunikimeve elektronike nga ana e sipërmarrësve të komunikimeve elektronike që veprojnë nën Regjimin e Autorizimit të Përgjithshëm për të gjitha shërbimet, përfshirë këtu edhe shërbimin DNS që ata ofrojnë për pajtimtarët e tyre. AKEP-i ka kryer dhe kryen në vazhdimësi inspektime dhe audite pranë sipërmarrësve për të verifikuar implementimin dhe zbatimin e masave të duhura teknike dhe organizative të sigurisë dhe në bashkëpunim me AKCESK-në ndjek incidentet e sigurisë që raportohen nga sipërmarrësit e komunikimeve elektronike. AKEP-i është administrator i domainit ".al" dhe ka autorizuar 8 subjekte si regjistrarë të akredituar për ofrimin e shërbimit të regjistrimit të *domain name* nën zonën .al (*TLD name registries*). Me përfshirjen e këtij shërbimi në listën e infrastrukturave kritike dhe të rëndësishme të informacionit, subjekt i zbatimit të përcaktimeve të rregullores nr. 37, datë 29.10.2015, "Mbi masat teknike dhe organizative për të garantuar sigurinë dhe/ose integritetin e rrjeteve dhe/ose shërbimeve të komunikimeve elektronike" do të jenë dhe regjistrarët e akredituar nga AKEP-i për ofrimin e shërbimit të regjistrimit të *domain name* nën zonën .al.

Penetrimi i internetit në Shqipëri është ende në zhvillim dhe paraqitet në një nivel mesatar përdorimi. Rreth 67% e popullsisë si dhe rreth 40% e familjeve kanë pasur qasje në internet në vitin 2019.

**2.1.2 Krimi kibernetik**

Shqipëria, ashtu dhe si shtetet e tjera, është në shumë raste viktimë e veprimtarisë keqdashëse kibernetike, të kryer nga aktorë kriminalë, duke përfshirë aktorët shtetërorë dhe joshtetërorë, që mund të përdorin infrastrukturën e rrjetit në Shqipëri dhe jashtë saj. Së bashku me përmirësimin e internetit, Shqipëria ka parë, gjithashtu, shfaqjen e formave të ndryshme të krimit kibernetik. Format e zakonshme të krimit kibernetik që mbizotërojnë në Shqipëri, përfshijnë mashtrimet që lidhen me *Internet banking*, të tilla si: *phishing* dhe *spam*. Edhe kur individët përgjegjës, për veprimtaritë kriminale kibernetike kundër Republikës së Shqipërisë identifikohen, shpesh është e vështirë për agjencitë e zbatimit të ligjit në Republikën e Shqipërisë dhe organizatat ndërkombëtare, që t'i ndjekin ato kur ato janë në juridiksione të kufizuara.

Aktualisht vihet re se mungojnë mjetet e nevojshme për të marrë dhe krijuar inteligjencë kibernetike, duke përdorur burime njerëzore dhe logjistike të nevojshme për të ushtruar veprimtarinë ligjzbatuese.

Rritja e kapaciteteve për t'u përballur me sfidat kibernetike është thelbësore dhe si pasojë duhet të ndryshohen strukturat, qasja, kapacitetet teknike dhe logjistike etj.

Një hap i rëndësishëm përpara në zhvillimin e legjislacionit dhe marrjen e masave kundër krimit kibernetik, do të jetë edhe strategjia e parë kombëtare për krimin kibernetik, e cila do të

përgatitet nga autoritetet respektive dhe do të vihet në jetë në një kohë relativisht të shkurtër. Ky dokument do të mund të përcaktojë rrugën për të luftuar veprimtaritë kriminale në fushën kibernetike, si dhe mundësimin e më shumë mjeteve të përshtatshme në shërbim të kësaj lufte.

**2.2 Kuadri ligjor i sigurisë kibernetike**

Një qasje gjithëpërfshirëse kombëtare e sigurisë kibernetike, nuk mund të bëhet duke përdorur vetëm teknologjitë dhe shërbimet, por duhet të shoqërohet me një kornizë ligjore të mirë dhe aktuale, me fokus në natyrën dinamike të mjedisit të TIK-ut dhe natyrën evoluese të kërcënimeve kibernetike.

Struktura të ndryshme kombëtare dhe ndërkombëtare, realizojnë fushata ndërgjegjësimi për grupe të ndryshme interesi me qëllim mbrojtjen nga kërcënimet që vijnë nga krimi kibernetik dhe sulme të tjera të sigurisë në internet.

Një kuadër ligjor dhe rregullator që mbron format e ndryshme të abuzimit dhe krimit elektronik, është thelbësor për krijimin e një ambienti të besueshëm, për komunikimet dhe transaksionet elektronike.

Ligjet kryesore që lidhen me sigurinë dhe krimin kibernetik janë:

- ligji nr. 7895, datë 27.1.1995, "Kodi Penal i Republikës së Shqipërisë", i ndryshuar;
- ligji nr. 2/2017, "Për sigurinë kibernetike";
- ligji nr. 9918, datë 19.5.2008, "Për komunikimet elektronike në Republikën e Shqipërisë", i ndryshuar;
- ligji nr. 9887, datë 10.3.2008, "Për mbrojtjen e të dhënave personale", i ndryshuar;
- ligji nr. 8457, datë 11.2.1999, "Për informacionin e klasifikuar", i ndryshuar;
- ligji nr. 9880, datë 25.2.2008, "Për nënshkrimin elektronik", i ndryshuar;
- ligji nr. 107, datë 15.10.2015, "Për identifikimin elektronik dhe shërbimet e besuara", i ndryshuar.

Lidhur me sa më sipër, është i nevojshëm harmonizimi i legjislacionit në fushën e sigurisë kibernetike, me atë të BE-së, duke krijuar mekanizmin e plotë dhe të qartë të kodifikuar, për të adresuar saktë problematikat dhe për t'i zgjidhur ato.

Gjithashtu është e nevojshme të realizohet, aty ku është e mundur, qasja, nënshkrimi, ratifikimi dhe zbatimi i instrumenteve ndërkombëtare të sigurisë në internet, duke përfshirë shpërndarjen e burimeve të mjaftueshme, sipas prioriteteve kombëtare, duke marrë në konsideratë zhvillimet teknologjike dhe duke zbatuar parimin e teknologjisë neutrale.

***2.3 Internet i sigurt për fëmijët***

Përdorimi gjithnjë e në rritje i internetit nga fëmijët, është problematika më e madhe për sa i përket sigurisë së tyre në mjedis *online*, jo vetëm në Shqipëri. Siguria e fëmijëve në internet është një ndër prioritetet e Shqipërisë dhe e të gjitha institucioneve që e kanë në fokus të veprimtarisë së tyre.

Në vitin 2018–2019 u realizua nga *Unicef Albania*, si partneri strategjik dhe kryesor i qeverisë në mbrojtjen dhe të drejtat e fëmijëve, një studim mbi **"Eksperiencat e fëmijëve në përdorimin e Internetit në Shqipëri"**[79], i cili anketoi 1000 fëmijë të moshave 9–18 vjeç dhe prindërit e tyre, rezultatet paraprake të të cilit janë si më poshtë:

Mosha mesatare kur fëmijët e anketuar, kanë aksesuar internetin për herë të parë është 9 vjeç, nga ku 37% pohojnë se kanë përdorur internetin nga mosha 8-vjeçare ose/dhe më herët. Ndërsa 51% e fëmijëve të anketuar kanë gjithnjë akses *online* (sa herë që ata dëshirojnë).

Në përgjithësi, fëmijët e anketuar përdorin më shumë internetin dhe kanë më shumë aftësi teknologjike *online* se prindërit e tyre. Kjo përbën një pengesë që prindërit të shoqërojnë në mënyrë efektive eksperiencën e fëmijëve në internet, jo vetëm duke kontrolluar aksesin, por duke i ndihmuar fëmijët të zhvillojnë gjykim kritik mbi eksperiencat dhe përmbajtjet në internet.

Nga studimi rezultoi se gjatë kohës së lundrimit të tyre në internet fëmijët, janë hasur me situata të padëshiruara. Më konkretisht, 14% e fëmijëve të anketuar kanë përjetuar *online* diçka që i ka mërzitur, veçanërisht mosha 15–17 vjeç. 1 në 10 fëmijë (9%), ka pasur një përvojë seksuale të padëshiruar në internet.

Statistikat nga ky hulumtim tregojnë se fëmijët janë të ekspozuar nga përmbajtje të dëmshme *online* si imazhet e dhunës apo abuzimit (1 në 5 fëmijë),

[79] Studimi "Eksperiencat e fëmijëve në përdorimin e internetit në Shqipëri" do të publikohet në 2019 nga *Unicef Albania*. Gjetjet paraprake u prezantuan gjatë Samitit "VIRAL" të organizuar nga *Unicef Albania* në nëntor 2018: https://www.unicef.org/albania/viral-summit-better-Internet-children-and-adolescents-albania

përmbajtje që flasin për dhunë fizike (17% e fëmijëve) apo përmbajtje që flasin për vetëvrasje (1 në 10 fëmijë). 1 në 5 fëmijë kanë qenë subjekt i mesazheve denigruese dhe të urrejtjes drejt tyre, që është, gjithashtu, një indikator i situatave të mundshme të bullizmit *online*.

Ndërkohë, studimi tregon se fëmijët e kanë të vështirë të ndajnë situatat e vështira që përjetojnë dhe të kërkojnë ndihmë: 1 në 5 fëmijë nuk ia ka treguar askujt ndodhinë që e ka mërzitur ndërsa 75% e fëmijëve të anketuar e kërkojnë ndihmën dhe mbështetjen nga bashkëmoshatarët e tyre dhe jo nga të rriturit.

Më shumë se 20% e fëmijëve të anketuar, pranojnë të gjitha kërkesat për shoqëri në rrjetet sociale, ndërsa 25% e fëmijëve pranojnë se kanë bashkëvepruar *online* me dikë, që nuk e njohin në jetën reale dhe 16% e tyre, kanë takuar personalisht dikë, që e kanë njohur vetëm nëpërmjet internetit. Prindërit janë të informuar vetëm për 9% të rasteve të mësipërme.

Fëmijët e anketuar pohojnë se nuk kanë asnjë kontroll ose supervizim nga prindërit, kur shohin video *online* (78%), vizitojnë rrjetet sociale (58%), përdorin aplikacionet e mesazheve (57%) apo përdorin kamerën e kompjuterit ose telefonit (56%).

Siç vihet re nga studimi, përdorimi i internetit nga fëmijët në mënyrë të pakontrolluar është në tregues shumë të lartë. Kjo problematikë shoqërohet shpesh herë edhe me pasoja të rënda. Mungesa e informacionit te prindërit lidhur me rreziqet që paraqet interneti i pasigurt, është në nivele të larta gjithashtu.

Lidhur me kontrollin prindëror, edhe pse ofrohet si mundësi teknike nga disa operatorë të ofrimit të shërbimit të internetit, nuk aplikohet. Gjithashtu, nga studimi i situatës në 7 rajone të vendit, i konstatuar nëpërmjet fushatave ndërgjegjësuese, në të cilën u përfshinë rreth 12.000 fëmijë të shkollave 9-vjeçare, në masë të madhe fëmijët konfirmojnë se prindërit e tyre, nuk kanë informacion të qartë mbi rreziqet e përdorimit të internetit të pasigurt nga fëmijët.

Një studim tjetër i realizuar në 2019 po nga zyra e *UNICEF Albania* "Faktori Web"[80] ka evidentuar një sërë mangësish ligjore dhe institucionale, të cilat pengojnë garantimin me efikasitet të sigurisë së fëmijëve në internet.

Studimi ka gjetur se megjithëse legjislacioni shqiptar në tërësi përputhet me standardet ndërkombëtare përkatëse mbi abuzimin seksual të fëmijëve, ai është shpesh i fragmentuar dhe i mungojnë përkufizime shumë të rëndësishme lidhur me abuzimin seksual të fëmijëve, angazhimin dhe detyrimin e tyre në aktivitete seksuale dhe në aktivitete të tjera të pahijshme. Parimi i mbrojtjes nga materialet e dëmshme dhe të paligjshme në internet pengohet nga dy faktorë: 1. Përkufizimi i materialit të dëmshëm është shumë i përgjithshëm dhe lë shumë hapësirë për gjykim individual; dhe 2. Mungesa e përkufizimeve të qarta të shfrytëzimit të fëmijëve në aktivitete seksuale e bën të vështirë identifikimin e akteve të paligjshme.

Një tjetër gjetje e rëndësishme lidhet me legjislacionin shqiptar që rregullon funksionimin e ofruesve të shërbimit të internetit, i cili është i paqartë, për sa u përket ngarkimit të autoriteteve administrative me kompetencat e bllokimit ose fshirjes së materialeve të caktuara. Kjo i pengon këto autoritete që t'i kuptojnë qartë rolet dhe funksionet e tyre, dhe që të kenë mekanizmat për ushtrimin e tyre. Në këtë fushë nevojitet legjislacion i qartë lidhur me kompetencat dhe procedurat ekzakte të autoriteteve administrative.

Lidhur me hetimin dhe ndjekjen penale të rasteve të abuzimit seksual me fëmijët në internet, studimi pohon se as policia dhe as prokuroria nuk janë plotësisht të pajisura me infrastrukturën e duhur për hetimin efikas të rasteve të abuzimit të fëmijëve në internet. Njësia për hetimin e krimit kibernetik pranë Policisë së Shtetit ka mungesë mundësish për kryerjen e mbikëqyrjes aktive *online*, duke cenuar aftësinë e tyre për të filluar hetimet *ex officio* dhe proaktive. Mungesa e reagimit të shpejtë nga ofruesit e shërbimit të internetit ndaj kërkesave të prokurorisë, si dhe vështirësitë në identifikimin e adresave IP të kundërvajtësve të pretenduar, ndikojnë në mënyrë shqetësuese në cilësinë dhe efikasitetin e përgjithshëm të hetimit, dhe

[80] UNICEF Albania, 2019, Faktori Web: Vlerësimi i kuadrit ligjor dhe gatishmërisë institucionale për trajtimin e abuzimit dhe shfrytëzimit seksual të fëmijëve në hapësirën kibernetike në Shqipëri: https://www.unicef.org/albania/sq/deklarata-shtypi/faktoriweb-vler%C3%ABsimi-i-kuadrit-ligjor-dhe-gatishm%C3%ABris%C3%AB-institucionale-p%C3%ABr

rrjedhimisht edhe në mundësinë për t'i vënë autorët para përgjegjësisë.

Studimi tregon se Njësitë e Mbrojtjes së Fëmijës, por dhe profesionistë të tjerë që merren me mbrojtjen e fëmijëve në internet kanë nevojë për ngritje kapacitetesh dhe mbështetje për adresimin e rasteve të abuzimit të fëmijëve në Internet. Gjithashtu, nuk ka të dhëna specifike të mbledhura dhe të publikuara për abuzimin e fëmijëve në internet.

***2.4. Edukimi, hulumtimi dhe trajnimi në fushën e sigurisë kibernetike***

Burimet njerëzore me aftësi dhe kualifikime të nevojshme në sigurinë kibernetike, kanë provuar të jenë një nga sfidat më të vështira për vendet në zhvillim, në drejtim të zbatimit të një CSIRT-i kombëtar dhe përmirësimit të gjendjes së përgjithshme kombëtare të sigurisë kibernetike. Është thelbësore që të sigurohet një nivel i mjaftueshëm edukimi, hulumtimi dhe trajnimi për sigurinë në internet, si dhe për të mbështetur nevojat e brendshme për profesionistët e sigurisë kibernetike.

Ekzistojnë disa programe studimi që ofrohen nga institucione të arsimit të lartë, në fushën e sigurisë kibernetike, të cilat janë në fillimet e tyre, por që kërkohet një përpjekje më e madhe për të arritur nivelin e nevojshëm, si dhe, gjithashtu ,nuk ka iniciativa kërkimore, për sigurinë kibernetike në Shqipëri. Njohuritë që studentët marrin në universitete, janë të pamjaftueshme për të përballuar kërkesat e tregut për punësim në këtë fushë. Përveç të tjerave edhe stafi akademik paraqet problematikat e veta, në kuptim të mbulimit të spektrit të plotë të kësaj fushe.

Si rrjedhojë hartimi i kurrikulave të mirëfillta për sigurinë kibernetike dhe thellimi i njohurive të stafit akademik është një nevojë imediate për të përballuar kërkesat e tregut.

Nga ana tjetër, rritja e kapaciteteve të burimeve njerëzore nëpërmjet trajnimeve të dedikuara për fushën e sigurisë kibernetike, në administratën publike dhe të gjithë sektorët publikë, është një nevojë tjetër e cila duhet të konsiderohet nga institucionet publike.

Gjithashtu, ekziston nevoja për një qasje të përbashkët, në edukimin e stafit qeveritar dhe publikut në lidhje me praktikat më të sigurta mbi ndërgjegjësimin për sigurinë kibernetike.

3. VIZIONI I STRATEGJISË

***3.1 Vizioni***

*Garantimi i sigurisë kibernetike në Republikën e Shqipërisë nëpërmjet ngritjes dhe funksionimit të mekanizmave bashkëveprues institucionalë: instrumenteve ligjore dhe teknike, si element kritik i mbrojtjes në hapësirën kibernetike, për infrastrukturat digjitale, transaksionet dhe komunikimet elektronike; nëpërmjet ngritjes së kapaciteteve profesionale, rritjes së vetëdijes mbarëkombëtare si dhe forcimit të bashkëpunimeve kombëtare dhe ndërkombëtare për një mjedis digjital të sigurt.*

***3.2 Treguesit e impaktit dhe treguesit e rezultatit***

Strategjia Kombëtare e Sigurisë Kibernetike do të monitorohet nëpërmjet matjes së indikatorëve bazë të përcaktuar në aneksin Pasaporta e indikatorëve. Me qëllim ndjekjen e realizimit të objektivave specifikë, të përkthyer në plan veprimi të detajuar, janë hartuar indikatorët bazë, të cilët do të shërbejnë si udhëzues për të monitoruar realizimin e Strategjisë.

Indikatorët janë konceptuar të tillë që të jenë të kuptueshëm, të matshëm dhe lehtësisht të krahasueshëm, sipas periudhave të monitorimit. Për çdo objektiv specifik janë planifikuar, 2 indikatorë bazë, të cilët mund të jenë të thjeshtë apo të përbërë, në varësi të nënobjektivave që do të matin.

## PJESA II
## QËLLIMI I POLITIKAVE DHE OBJEKTIVAT SPECIFIKE TË STRATEGJISË

Me qëllim rritjen e nivelit të sigurisë kibernetike në vend, Qeveria e Republikës së Shqipërisë duhet të përmbushë këto qëllime:

Garantimi i sigurisë kibernetike në nivel kombëtar, nëpërmjet mbrojtjes së infrastrukturave të informacionit, duke fuqizuar mjetet teknologjike dhe juridike.

Ndërtimi i një mjedisi të sigurt kibernetik, duke ndërgjegjësuar shoqërinë dhe duke ngritur kapacitetet profesionale.

Krijimi i mekanizmave të nevojshëm për sigurinë e fëmijëve në hapësirën kibernetike, duke përgatitur njëkohësisht brezin të ri të aftë për të përfituar nga përparësitë e teknologjisë së informacionit dhe për të përballuar sfidat e zhvillimit.

Rritja e bashkëpunimit kombëtar dhe ndërkombëtar në fushën e sigurisë kibernetike me partnerët strategjikë.

**4. Qëllimi i politikës 1. Garantimi i sigurisë kibernetike në nivel kombëtar, nëpërmjet mbrojtjes së infrastrukturave të informacionit, duke fuqizuar mjetet teknologjike dhe juridike**

Zhvillimet e vrullshme në të gjithë sektorët e ekonomisë të mbështetur fuqishëm dhe nga inovacionet teknologjike, e bëjnë shumë të vështirë për vendimmarrësit të kuptojnë dhe të minimizojnë rreziqet, që rrjedhin nga përdorimi i teknologjisë së informacionit dhe komunikimit. Këto rreziqe janë përgjegjësi e përbashkët globale dhe përfshijnë perspektiva kombëtare dhe ndërkombëtare. Përgjegjësia e përbashkët brenda vendit, përfshin si industrinë, ashtu edhe administratën dhe qytetarët.

Hartimi dhe aplikimi i politikave dhe i mjeteve për krijimin e një mjedisi të sigurt komunikimi, është komponenti më i vlefshëm për menaxhimin e incidenteve të sigurisë kibernetike, si dhe kryerjen e transaksioneve elektronike të sigurta në tregun e brendshëm, me qëllim garantimin e bashkëveprimit të sigurt elektronik midis autoriteteve publike dhe qytetarëve, bizneseve, duke rritur efektivitetin e shërbimeve *online* publike dhe private, të biznesit dhe tregtisë elektronike.

Mjedisi digjital është i ndjeshëm: sistemet dhe rrjetet e informacionit, mund të ndikohen nga incidentet e sigurisë, siç janë gabimet njerëzore, ngjarjet natyrore, dështimet teknike ose sulmet. Këto situata po rriten dhe po bëhen gjithnjë e më komplekse dhe mund të çojnë në humbje të mëdha financiare dhe të ndikojnë në mirëqenien e shoqërisë në përgjithësi.

Ndërtimi i besimit në mjedisin *online* është çelësi për zhvillimin ekonomik dhe social. Mungesa e besimit, në veçanti për shkak të mungesës së perceptuar të sigurisë kibernetike i bën konsumatorët të hezitojnë në përdorimin e transaksioneve elektronike.

***4.1 Objektivi specifik 1: Përmirësimi i kuadrit ligjor që normon dhe rregullon fushën e sigurisë kibernetike në vend, si dhe harmonizimi i i tij me direktivat dhe rregulloret e Bashkimit Evropian.***

Aktualisht, autoritetet e sigurisë në vend, kanë krijuar bazën ligjore mbi të cilën të ushtrojnë veprimtarinë e tyre. Pavarësisht hartimit të ligjeve e akteve nënligjore, rregulloreve dhe standardeve, nga analiza e kryer, si dhe nga vlerësimi i nivelit të maturimit të sigurisë kibernetike në vend, është evidentuar nevoja për rishikim të të gjithë kuadrit ligjor e rregullator, me qëllim harmonizimin e plotë me direktivat e Bashkimit Evropian, si dhe me qëllim koordinimin e brendshëm institucional.

Realizimi i këtij objektivi specifik synon të kryejë harmonizimin e legjislacionit shqiptar mbi sigurinë kibernetike me atë të BE-së. Gjithashtu, do të hartohet një procedurë kombëtare për veprim në rastet e gjendjeve të jashtëzakonshme të krijuara nga krizat kibernetike.

**Nënobjektivat:**

4.1.1 Përmirësimi i kuadrit rregullator për sigurinë kibernetike i harmonizuar me ligjet sektoriale, për të adresuar saktë çështjet dhe zgjidhur ato, duke përfshire, por pa u kufizuar: IoT, teknologjinë 5G, inteligjencën artificiale.

4.1.2 Përshtatja e vazhdueshme e standardeve dhe rregullave, sipas zhvillimeve të fushës, së sigurisë kibernetike.

4.1.3 Përmbushja e angazhimeve të marra si vend i Aleancës së Atlantikut të Veriut, për hapësirën kibernetike.

4.1.4 Përcaktimi i një procedure kombëtare për rastet e gjendjeve të jashtëzakonshme të krijuar nga krizat kibernetike, me qëllim marrjen e masave konkrete për zgjidhjen e situatës në kohe reale.

***4.2 Objektivi specifik 2: Ngritja dhe funksionimi i CSIRT-eve në të gjithë sektorët e industrisë në nivel kombëtar***

Bazuar në ligjin "Për sigurinë kibernetike" dhe detyrimeve që rrjedhin prej tij, me qëllim garantimin e sigurisë së sistemeve të informacionit dhe komunikimit, është detyrim identifikimi dinamik i infrastrukturave kritike e të rëndësishme të informacionit, si dhe më tej ngritja e ekipeve të përgjigjeve ndaj incidenteve (CSIRT). Aktualisht kanë filluar të merren masat e para për ngritjen e tyre në disa prej infrastrukturave tashmë të përcaktuara me vendim, por ky është një proces në vijueshmëri , i cili monitorohet nga AKCESK-i.

Realizimi i këtij objektivi të politikës 1 do të matet me numrin e CSIRT-eve. Të gjithë operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit duhet të kenë CSIRT-et përkatëse , të cilat duhet të zbatojnë të gjitha kërkesat minimale të miratuara dhe audituara nga AKCESK-u.

**Nënobjektivat:**

4.2.1 Krijimi i kushteve optimale të punës për funksionimin e CSIRT-eve, në përmbushje të detyrave të veta, për të garantuar sigurinë kibernetike në infrastrukturat kritike e të rëndësishme të informacionit.

4.2.2 Ngritja e kapaciteteve të CSIRT-eve nëpërmjet trajnimeve dhe stërvitjeve kibernetike.

***4.3 Objektivi specifik 3: Fuqizimi dhe implementimi i masave të sigurisë në infrastrukturat kritike dhe të rëndësishme të informacionit***

Bazuar në vlerësimet e bëra gjatë viteve 2018–2019 nga autoriteti përgjegjës i fushës së sigurisë kibernetike, tek infrastrukturat kritike e të rëndësishme të informacionit, mbetet si një detyrë parësore, shtimi dhe fuqizimi i implementimit të masave të sigurisë. Institucionet publike e private duhet të përmirësojnë procedurat e tyre, hartimin e planeve strategjike për mbrojtjen kibernetike nga sulmet apo krimi kibernetik, si dhe planet për menaxhimin e riskut në rastet kur ndodhin këto sulme. Objektiv i kësaj Strategjie është nxitja dhe detyrimi që të gjitha infrastrukturat kritike e të rëndësishme të informacionit të hartojnë planet strategjike në rastet e sulmeve kibernetike, si dhe të marrin masa për të përballuar këto sulme dhe për të rikuperuar dëmin apo për të eliminuar atë tërësisht.

Realizimi i këtij objektivi specifik do të kërkojë që të gjithë operatorët e infrastrukturave kritike e të rëndësishme të informacionit, të cilët kanë CSIRT-et e tyre, të implementojnë sisteme të specializuar në identifikimin e sulmeve kibernetike, parandalimin e tyre, analizimin e rikuperimin e dëmeve nga këto sulme, si dhe nxjerrjen e mësimeve për të ardhmen. Gjithashtu, operatorët duhet të kryejnë analizat e menaxhimit të riskut, si dhe vetëvlerësimet në lidhje me nivelin e maturimit të sigurisë kibernetike në infrastrukturat që administrojnë.

**Nënobjektivat:**

4.3.1 Përdorimi i zgjidhjeve *hardware* dhe *software* të avancuara për identifikimin, parandalimin dhe menaxhimin e incidenteve kibernetike.

4.3.2 Analizimi i infrastrukturave kritike dhe të rëndësishme të informacionit për vlerësimin e menaxhimin e riskut në to.

4.3.3 Hartimi i planeve strategjike për mbrojtjen e hapësirës kibernetike nga incidente të mundshme.

4.3.4 Realizimi i vetëvlerësimeve në infrastrukturat kritike dhe të rëndësishme të informacionit për matjen e nivelit të maturimit të sigurisë kibernetike.

***4.4 Objektivi specifik 4: Përmirësimi i infrastrukturave të informacionit për të luftuar krimin kibernetik, radikalizimin dhe ekstremizmin e dhunshëm.***

Interneti është një mjet që nga njëra anë ndikon në zhvillimin e shoqërisë, në lehtësimin e procedurave dhe akses të shpejtë në të dhëna, por nga tjetër është një mjet për individë/grupe keqbërëse që kryejnë krime kibernetike apo që përpiqen të radikalizojnë individë nga shtresa vulnerabël apo të marxhinalizuara me qëllime ekstremiste e për të kryer akte të dënueshme nga shoqëria. Lidhur me këtë fenomen është e nevojshme që të merren një sërë masash nga institucionet publike dhe private për t'i luftuar ato dhe për t'i mbajtur nën kontroll deri në minimizim të tyre.

Për të realizuar sa më lart, do të synohet ngritja e mekanizmave për të rregulluar e ofruar internet të sigurt në ambientet publike. Gjithashtu do të synohen bashkëpunime me organizatat e shoqërisë civile dhe bizneset me qëllim mbajtjen nën kontroll dhe evidentimin e elementeve kontaminues që qarkullojnë në internet e që cenojnë sigurinë kibernetike në vend. Pra do të ngrihen dy mekanizma për të monitoruar fenomenet e mësipërme.

**Nënobjektivat:**

4.4.1 Monitorimi dhe parandalimi i fenomeneve, që nxisin ekstremizmin e dhunshëm dhe radikalizimin në shtresat vulnerabël në hapësirën kibernetike.

4.4.2 Evidentimi në vazhdimësi i elementeve kontaminues, që qarkullojnë në internet, që cenojnë sigurinë kibernetike në vend.

4.4.3 Ngritja e mekanizmave për rregullimin e internetit të sigurt në ambientet publike, të certifikuar nga autoriteti rregullues i fushës së sigurisë kibernetike.

4.4.4 Ngritja e kapaciteteve të autoriteteve përgjegjëse kundër krimit kibernetik.

4.4.5 Rritja e bashkëpunimit rajonal në luftën kundër krimit kibernetik.

**5. Qëllimi i politikës 2**: **Ndërtimi i një mjedisi të sigurt kibernetik, duke edukuar dhe ndërgjegjësuar shoqërinë në ngritjen e**

**kapaciteteve profesionale në fushën e sigurisë së informacionit**

Ekzistenca e aftësive dhe kapaciteteve profesionale për t'u përgjigjur dhe për të menaxhuar incidente të sigurisë kibernetike nuk është më opsion në ditët e sotme.

Rritja e kapaciteteve në fushën e sigurisë kibernetike ka për qëllim përgjigjen në mënyrë efektive ndaj krimit kibernetik. Ky është një komponent integral i bashkëpunimit ndërkombëtar që mund të rrisë harmonizimin me vizionin e BE-së për një hapësirë kibernetike globale, të hapur, të lirë e të sigurt për të gjithë, duke siguruar respektimin e të drejtave të njeriut.

Metodat e përdorura për rritjen e kapaciteteve dhe ndërgjegjësimin e shoqërisë janë thelbësore për të përcaktuar efektivitetin e ndërtimit të një mjedisi të sigurt.

5.1 Objektivi specifik 1: Rritja e kapaciteteve profesionale në fushën e sigurisë së informacionit nëpërmjet rishikimit të kurrikulave arsimore.

**Nënobjektivat:**

5.1.1 Hartimin e programeve të studimit në arsimin e lartë në fushën e sigurisë kibernetike, me qëllim krijimin e gjeneratës së re të ekspertëve të sigurisë kibernetike.

5.1.2 Hartimi i rekomandimeve për integrimin në kurrikula universitare të informacioneve në lidhje me internetin e sigurt.

5.1.3 Rritja e kapaciteteve kërkimore dhe inovative në fushën e sigurisë kibernetike

***5.2 Objektivi specifik 2: Rritja e ndërgjegjësimit dhe e aftësive profesionale të institucioneve publike dhe private për sigurinë kibernetike.***

**Nënobjektivat:**

5.2.1 Trajnime periodike për thellimin e njohurive në sigurinë kibernetike, sipas dinamikës së fushës, për stafin administrativ në nivel qendror dhe në nivel lokal.

5.2.2 Rritja dhe mbështetja e kapaciteteve kërkimore dhe risive të biznesit nëpërmjet nxitjes së ngritjes së qendrave kërkimore shkencore në fushën e sigurisë kibernetike.

5.2.3 Rritja e kapaciteteve të CSIRT-eve në nivel kombëtar dhe nivelit ekzekutiv të administratës publike nëpërmjet trajnimeve dhe stërvitjeve kibernetike.

5.3 Objektivi specifik 3: Rritje e ndërgjegjësimit të shoqërisë, për sigurinë kibernetike dhe për kërcënimet kibernetike.

**Nënobjektivat:**

***5.3.1 Organizimi i fushatave ndërgjegjësuese nga autoriteti përgjegjës, për sigurinë kibernetike, me grupe interesi të ndryshme, duke përdorur hapësirat e duhura për realizimin e tyre, përfshirë edhe mediat audiovizive apo edhe ato sociale.***

5.3.2 Krijimin e një platforme edukative *online*, për sigurinë kibernetike, për të rritur ndërgjegjësimin në grup-mosha të ndryshme të shoqërisë, për përdorimin e internetit të sigurt dhe të infrastrukturës digjitale.

**6. Qëllimi i politikës 3: Krijimi i mekanizmave të nevojshëm për sigurinë e fëmijëve në hapësirën kibernetike, duke përgatitur njëkohësisht brezin e ri të aftë për të përfituar nga përparësitë e teknologjisë së informacionit dhe për të përballuar sfidat e zhvillimit**

Ofrimi i internetit të sigurt për fëmijët dhe të rinjtë në Shqipëri mbetet një nga objektivat strategjikë të qeverisë shqiptare, siç është shprehur dhe në Agjendën Kombëtare për të Drejtat e Fëmijëve 2017–2020. Për një numër të konsiderueshëm të fëmijëve, sot interneti, telefonat celularë, dhe teknologjitë e tjera të informacionit janë bërë pjesë e jetës së përditshme. Familja (prindërit), bashkëmoshatarët dhe shkolla janë tri mjediset e socializimit të fëmijëve, ndërsa mjedisi digjital është bërë i katërti. Për ta, dallimi midis *online* dhe *offline*, gjithnjë e më shumë bëhet i pakuptimtë, dhe ata lëvizin pa ndërprerje ndërmjet të dy mjediseve. Mbrojtja e fëmijëve në internet kërkon veprime specifike dhe të artikuluara në mënyrë të qartë. Njëkohësisht mbrojtja e fëmijëve duhet të jetë proporcionale me rreziqet që fëmijët hasin, dhe nuk duhet të pengojë përdorimin e teknologjive të informacionit për rritjen, edukimin dhe zhvillimin e fëmijëve. Politikat e qeverisë duhet të krijojnë një mjedis digjital, i cili i përgjigjet nevojave të fëmijëve, duke garantuar njëkohësisht mbrojtjen dhe respektimin e të drejtave të tyre. Për këtë arsye, ndërmarrja e hapave të menjëhershëm për të krijuar mjedise digjitale të sigurta është e rëndësishme, duke garantuar njëkohësisht

respektimin e të drejtave dhe arritjen e potencialit maksimal të zhvillimit të fëmijëve.

***6.1 Objektivi specifik 1: Forcimi i kuadrit ligjor për rritjen e sigurisë së fëmijëve në internet***

**Nënobjektivat:**

6.1.1 Hartimi i një baze ligjore të posaçme për mbledhjen e të dhënave të incidenteve të raportuara të dhunës, bullizimit dhe abuzimit *online* të fëmijëve në shkolla.

6.1.2 Përmirësimi i Kodit Penal, për ta sjellë në linjë me legjislacionin ndërkombëtar për mbrojtjen e fëmijëve nga abuzimi seksual në internet.

6.1.3 Ndryshimi i dispozitave procedurale penale në Kodin e Procedurës Penale dhe miratimi i akteve rregullatore lidhur me parashkrimin e veprave penale lidhur me abuzimin seksual të fëmijëve, si dhe procedurat dhe afatet e nevojshme për të rritur efikasitetin e hetimit, prioritizimin e rasteve dhe analizën e provave lidhur me rastet e abuzimit seksual të fëmijëve nëpërmjet internetit dhe teknologjive të komunikacionit.

6.1.4 Plotësimi dhe qartësimi i legjislacionit në lidhje me njoftimin dhe heqjen dhe bllokimit të materialeve të paligjshme *online*.

***6.2. Objektivi specifik 2: Parandalimi i abuzimit seksual të fëmijëve në internet nëpërmjet rritjes së ndërgjegjësimit dhe krijimit të hapësirave të sigurta për lundrimin në internet***

**Nënobjektivat:**

6.2.1 Përmirësimi dhe krijimi i programeve për ndërgjegjësimin mbi sigurinë në internet në sistemin edukativ.

6.2.2 Krijimi dhe mbështetja e rrjetit *online* të mësuesve të TIK-ut për të promovuar çështjen e mbrojtjes së fëmijëve në internet.

6.2.3 Krijimi ose përmirësimi i hapësirave publike me internet të sigurt për fëmijët dhe familjet nëpërmjet nismave për të ofruar aksesim falas të internetit por njëkohësisht informacion të filtruar me qëllim mbrojtjen e fëmijëve dhe të rinjve nga përmbajtjet abuzuese *online*.

6.2.4 Aplikimi i filtrave në shkollat publike dhe private për të parandaluar aksesin e fëmijëve në faqe të papërshtatshme dhe të paligjshme, si dhe informimi në vijueshmëri i mësuesve të TIK për raportimin e incidenteve.

6.2.5 Identifikimi, mbështetja dhe promovimi i talenteve për të krijuar zgjidhje teknike që ndihmojnë në mbrojtjen dhe sigurinë *online*.

*6.3* ***Objektiv specifik 3: Hetimi efektiv dhe sjellja para drejtësisë e autorëve të krimeve kibernetike ndaj fëmijëve, me fokus abuzimin dhe shfrytëzimin seksual***

**Nënobjektivat:**

6.3.1 Sigurimi i sigurimit të mjeteve teknike që ndihmojnë policinë dhe organet përkatëse në analizimin dhe zbulimin e rasteve të dhunës *online,* veçanërisht lidhur me imazhet e abuzimit seksual me fëmijët

6.3.2 Krijimi i programeve të trajnimit për personelin e gjyqësorit, prokurorisë dhe policisë, në lidhje me mbrojtjen e fëmijëve në internet dhe sigurinë kibernetike, duke përfshirë evidenca të përdorimit digjital dhe ndihmën e ndërsjellë juridike.

6.3.3 Ngritja e një sistemi kursesh pranë Shkollës se Magjistraturës dhe Akademisë së Sigurisë, në lidhje me çështjet që kanë të bëjnë më krimet ndaj fëmijëve *online* dhe mënyrat e mbrojtjes së tyre në internet.

6.3.4 Krijimi i mekanizmave për standardizimin e punës së analizimit të provave digjitale nga struktura e krimit kibernetik në Policinë e Shtetit.

6.3.5 Krijimi i një grupi pune së bashku me strukturat e krimit kibernetik në Policinë e Shtetit dhe industrinë për të zgjidhur problemet e hetimit dhe identifikimit të personave të dyshuar për abuzim me fëmijët *online*, me fokus të veçantë identifikimin e përdoruesve fundorë nëpërmjet adresave IP.

***6.4 Objektivi specifik 4: Rritja e ndërgjegjësimit dhe edukimi tek të gjitha segmentet e shoqërisë për përdorimin e sigurt të internetit nga fëmijët***

**Nënobjektivat:**

6.4.1 Fushata ndërgjegjësimi me prindërit dhe edukatorët në lidhje me rreziqet dhe problemet me të cilat përballen fëmijët në internet.

6.4.2 Zhvillimi i programeve të trajnimit me mësuesit e TIK-ut, në lidhje me çështjet e internetit të sigurt.

6.4.3 Zhvillimi i programeve të trajnimit për Punonjësit e Mbrojtjes së Fëmijës lidhur me trajtimin e rasteve të fëmijëve në nevojë për mbrojtje ku rreziku i dhunës, abuzimit, shfrytëzimit

apo i neglizhimit lidhet me internetin dhe teknologjitë e informacionit.

***6.5 Objektivi specifik 5: Forcimi i bashkëpunimit ndërsektorial për mbrojtjen e fëmijëve në internet***

**Nënobjektivat:**

6.5.1 Promovimi nëpërmjet bashkëpunimit me të gjitha ISP-të i mekanizmave ekzistues të aplikuar në platformat e tyre për sigurinë e fëmijëve në internet.

6.5.2 Integrimi nga të gjitha ISP-të në platformat e tyre të listës IWF *(Internet Watch Foundation Hash List)*, që ndalon çdo individ të hedhë, shkarkojë apo shikojë imazhe apo video të abuzimit seksual të fëmijëve, si dhe krijimin e aksesit të strukturave të hetimit të krimit kibernetik në Policinë e Shtetit në këtë listë.

6.5.3 Ngritja e një Komiteti Teknik Këshillues për Sigurinë e Fëmijëve në internet, pranë Këshillit Kombëtar për të Drejtat dhe Mbrojtjen e Fëmijëve.

**7. Qëllimi i politikës 4: Rritja e bashkëpunimit kombëtar dhe ndërkombëtar në fushën e sigurisë kibernetike me partnerët strategjikë**

Koordinimi dhe bashkëpunimi i të gjithë aktorëve është elementi bazë për garantimin e suksesit. Për shkak të dinamikës dhe shpejtësisë me të cilën zhvillohet Teknologjia e Informacionit dhe Komunikimit (TIK) bashkëpunimi me sektorin privat duhet të forcohet. Vetëm nëpërmjet një bashkëpunimi të ngushtë mund të rritet siguria dhe zhvillimi i TIK-ut në administratën shtetërore në koherencë me zhvillimet dhe trendin e teknologjisë.

Rritja e bashkëpunimit dhe koordinimit ndërmjet institucioneve shtetërore do të forcohet për të garantuar ndërveprimin dhe koordinimin në forcimin e sigurisë dhe minimizimin e dëmeve nga sulmet kibernetike.

Shqipëria mbështet dhe do të jetë pjesë e iniciativave ndërkombëtare, të cilat synojnë rritjen dhe forcimin e sigurisë. Në mënyrë të veçantë do të forcohet bashkëpunimi me NATO-n dhe BE-në, duke u bërë pjesë aktive e iniciativave të përbashkëta për sigurinë kibernetike. Anëtarësimi i Shqipërisë në organizmat dhe forumet e sigurisë kibernetike të njohura ndërkombëtare dhe rritja e bashkëpunimit është prioritet.

Në cilësinë e vendit anëtar të NATO-s, Shqipëria njeh hapësirën kibernetike si domainin e pestë të luftës, së bashku me tokën, detin, ajrin dhe hapësirën. Hapësira kibernetike paraqet sfida dhe siguria në këtë hapësirë arrihet vetëm, duke menduar në nivel global dhe duke punuar ngushtë në nivel ndërkombëtar.

***7.1 Objektivi specifik 1: Forcimi i bashkëpunimit institucional në nivel kombëtar***

**Nënobjektivat:**

7.1.1 Rritja e bashkëpunimit dhe koordinimit ndërmjet institucioneve shtetërore për të garantuar sigurinë në nivel kombëtar në hapësirën kibernetike.

7.1.2 Krijimi i një instrumenti për shkëmbimin e informacionit përmes pikave të kontaktit të dedikuara nga institucionet përkatëse, në raste të kërcënimeve kibernetike.

7.1.3 Ngritja e një strukture fleksibël me ekspertët më të mirë të sigurisë kibernetike në vend, me qëllim mbështetje në raste krizash kibernetike, testimi dhe vlerësimi të nivelit të sigurisë kibernetike në nivel kombëtar.

***7.2 Objektivi specifik 2: Forcimi i bashkëpunimit ndërkombëtar në fushën e sigurisë dhe mbrojtjes kibernetike dhe luftës kundër ekstremizmit të dhunshëm dhe radikalizimit***

**Nënobjektivat:**

7.2.1 Zhvillimi i mekanizmave dhe i procedurave efikase, për bashkëpunim ndërkombëtar, në rast të incidenteve kibernetike, sulmeve dhe krizave, sipas parimeve të vendosura ndërkombëtarisht.

7.2.3 Forcimi i bashkëpunimit dhe shkëmbimi i informacionit me NATO-n/OSBE-në dhe organizata/forume të tjera ndërkombëtare.

## PJESA IV
## ZBATIMI, PËRGJEGJËSIA E INSTITUCIONEVE, LLOGARIDHËNIA

Hartimi i Strategjisë Kombëtare të Sigurisë Kibernetike, 2020–2025, mbështetet në Strategjinë e Sigurisë Kibernetike të Bashkimit Evropian dhe është në vijim të Dokumentit të Politikave për Sigurinë Kibernetike, 2015–2017.

- Metodologjia u përcaktua të jetë me pjesëmarrje të të gjitha institucioneve publike kontribuese në sigurinë kibernetike të vendit, si dhe gjithëpërfshirëse, duke i ofruar një numri të madh aktorësh mundësinë për të kontribuar.

- Strategjia u mbështet në angazhimet dhe standardet e BE-së dhe organizmave të tjerë ndërkombëtarë, si dhe mbi dy vlerësimet e kryera nga ITU dhe *Oxford University*, me mbështetjen e Bankës Botërore.

- Angazhimi i institucioneve publike dhe private i jep kësaj Strategjie mundësinë për të qenë objektive dhe e realizueshme. Grupi ndërinstitucional i punës, si dhe të gjithë aktorët e përfshirë në konsultime dhanë komente të vlefshme, duke e rishikuar disa herë draftin e përgatitur me qëllim miratimin e një strategjie gjithëpërfshirëse, ku secili të gjejë veten e të japë kontributin e tij në garantimin e sigurisë kibernetike të vendit.

- Kjo Strategji nuk është një strategji vetëm për institucionet, por është një strategji që nxit dhe mbështet mbrojtjen kibernetike edhe të individit, qytetarëve dhe, veçanërisht, fëmijëve si e ardhmja e këtij vendi. Në të evidentohen edhe masa për të luftuar jo vetëm krimin kibernetik, por edhe nxitjen e terrorizmit dhe ekstremizmit të dhunshëm nëpërmjet hapësirës kibernetike.

Plani i veprimit që shoqëron Strategjinë Kombëtare të Sigurisë Kibernetike, 2020–2025 u përgatit, bazuar në:

a) gjetjet e rekomandimet e raportit të vlerësimit të zbatimit të Dokumentit të Politikave për Sigurinë Kibernetike 2015–2017;

b) gjetjet e rekomandimet e dhëna në raportet e vlerësimit nga ITU[81] dhe *Oxford University*[82]*;*

c) në planet buxhetore të institucioneve publike për periudhën 2020–2022.

Sikurse paraqitet edhe në objektivat specifikë dhe aktivitetet kryesore të propozuara në këtë Strategji dhe Planin e Veprimit, rolin koordinues duhet ta kryejë Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike në bashkëpunim me Agjencinë Kombëtare të Shoqërisë së Informacionit.

Gjithashtu, në këtë dokument janë marrë parasysh detyrimet që lindin nga procesi i integrimit evropian dhe rekomandimet e lëna, nga *NIS Direktive* dhe përshtatja që po bëhet në BE për ENISA si EU CERT, si dhe angazhimet si vend anëtar i NATO.

Të gjitha masat/aktivitetet e propozuara, pasi u vlerësuan dhe plotësuan edhe nga grupi ndërinstitucional i punës, përgjegjës për hartimin e Strategjisë, u detajuan më tej gjatë vlerësimit të efekteve financiare për zbatimin e kësaj Strategjie Kombëtare dhe Planit të saj të Veprimit 2020–2025, me nevojën për rishikim çdo dy vjet, bazuar në dinamikën e zhvillimit të sektorit.

Secili institucion përgjegjës për aktivitetet duhet të planifikojë realizimin e tyre duke garantuar buxhetet e planifikuara, burimet njerëzore dhe kapacitetet teknike me qëllim realizimin e tyre.

Çdo vit do të bëhet vlerësimi i zbatimit të aktiviteteve dhe arritjes së objektivave të identifikuar nëpërmjet realizimit të indikatorëve. Institucionet përgjegjëse për realizimin e aktiviteteve dhe arritjes së rezultateve kanë detyrimin e raportimit sipas standardeve raportuese. Koordinatori i Strategjisë duhet të përgatitë raportin vjetor dhe ta publikojë.

## PJESA V
## PLANI I VEPRIMIT DHE BURIMET FINANCIARE PËR ZBATIM

*Metodologjia e kostimit të aktiviteteve*

Shpenzimet e nevojshme për zbatimin e PKV-së janë nxjerrë duke kostuar secilin nga aktivitet e këtij plani veprimi. Metodologjia e zbatuar për llogaritjen e kostove paraqet një kombinim të metodave që mund të përdoren në rastet e strategjive me shumë aktorë.

Metodologjia kryesore e përdorur është kostimi i bazuar në aktivitete *(Activity Based Costing-ABC)*, ku për çdo aktivitet evidentohet institucioni përgjegjës si dhe burimi i mbulimit të kostove dhe alokon burimet për të gjitha produktet dhe shërbimet në bazë të konsumit aktual për secilin aktivitet

Buxheti u hartua mbështetur në koston e secilit aktivitet të pasqyruar në planin e veprimit, kohështrirjen dhe frekuencën e zbatimit të tij, si dhe numrin e përfituesve për aktivitete të caktuara.

Për llogaritjen e shpenzimeve për aktivitetet kryesore është vepruar si më poshtë:

- Llogaritja e shpenzimeve për burime njerëzore bazohet në kohën e parashikuar për realizimin e veprimtarisë dhe një page mesatare ditore të një kategorie të caktuar të nëpunësve civilë,

81 https://cesk.gov.al/Publikime/2019/Albania_Assessment_ReportITU.pdf

82 https://cesk.gov.al/Publikime/2019/AlbaniaCMMReport.pdf

- Llogaritja e shpenzimeve për shërbime.

Për këto aktivitete janë mbajtur parasysh kostot e shërbimeve të institucioneve përkatëse, bazuar në standardet e miratuara.

- Llogaritja e shpenzimeve për aktiviteteve që lidhen me hartimin dhe rishikimin e legjislacionit, monitorimin dhe funksionimin e strukturave të përhershme etj.

Për këto aktivitete gjatë llogaritjeve janë mbajtur parasysh shpenzimet e vazhdueshme që do të ndodhin, për shembull për pagat, kontributet e sigurimeve shoqërore, ekspertizë të huaj (kur është parashikuar në plan) dhe mjete konsumi.

- Llogaritja e shpenzimeve për aktiviteteve që lidhen me studime, fushata ndërgjegjësuese programe trajnimi ekspertiza thuaja etj., llogaritja e kostove është bërë sipas iniciativave specifike të ngjashme, si dhe sipas natyrës së aktiviteteve dhe kostove që ofron tregu për shërbime të tilla.

- Në llogaritjen e shpenzimeve për trajnime është mbajtur në konsideratë kosto e trajnimit për një person. Si kosto për njësi janë përdorur kostot e ASPA-s dhe/ose kostot e aplikuara për trajnime të ngjashme në të shkuarën.

- Për atë pjesë të aktiviteteve ku informacioni nuk ishte i plotë (si në rastin e projekteve apo studimeve) është ndjekur metoda e vlerësimit për analogji ose me fjalë të tjera janë marrë në konsideratë shpenzimet e bëra për aktivitete të ngjashme që kanë qenë përfshirë në planet buxhetore të mëparshme.

*Buxheti dhe burimet financiare për zbatimin e planit të veprimit*

Strategjia Kombëtare e Sigurisë Kibernetike do të zbatohet në periudhën 2020-2025. Për të mundësuar zbatimin e saj janë llogaritur shpenzimet e nevojshme për zbatimin e secilit aktivitet, objektiv specifik dhe qëllimit të politikave.

Buxheti i përgjithshëm për zbatimin e Strategjisë është reflektuar në disa forma:

- Buxheti i përgjithshëm sipas viteve për secilin aktivitet, objektiv specifik, qëllim strategjik dhe burimeve të financimit

- Buxheti i detajuar sipas aktiviteteve, burimeve të financimit dhe institucioneve përgjegjëse

| Politika | Specific objective | Sub- Objective | Institucioni përgjegjës | Results | Kosto totale | Kostot në Lek | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Viti 2021 | Viti 2022 | Viti 2023 | Viti 2024 | Viti 2025 | PBA | Donatore | Te tjere | Hendeku |
| Qëllimi Politikës 1 | Objektivi Specifik A - Përmirësimi i kuadrit ligjor që normon dhe rregullon fushën e sigurisë kibernetike në vend, si dhe harmonizimi i tij me direktivat dhe rregulloret e Bashkimit Europian. | A.1 Përmirësimi i kuadrit rregullator për sigurinë kibernetike i harmonizuar me ligjet sektoriale, për të adresuar sakte çështjet dhe zgjidhur ato duke perfshire, por pa u kufizuar: Cloud computing, IoT, teknologjine 5G, Intelligencen Artificiale. | AKCESK | A.1.1. VKM "Per Disa shtesa dhe ndryshime në VKM 69/2016 për Miratimin e Rregullores së Identifikimit Elektronik dhe Shërbimeve të Besuara" e hartuar dhe e miratuar | 78,000 | 62,400 | 15,600 | - | | 78,000 | | | - |
| | | | AKCESK | A.1.2 VKM "Per disa shtesa dhe ndryshime ne VKM Nr. 222, datë 26.04.2018, "Për miratimin e Listës së Infrastrukturave Kritike të Informacionit dhe të Listës së Infrastrukturave të Rëndësishme të Informacionit" e hartuar dhe e miratuar | 78,000 | 62,400 | 15,600 | - | | 78,000 | | | - |
| | | | AKCESK | A.1.3. Aktet ligjore e nënligjore për krimin kibernetik të hartuara e miratuara, duke marrë në konsideratë kornizën ligjore të aplikueshme në Republikën e Shqipërisë dhe BE-së. | 78,000 | 62,400 | 15,600 | - | | 78,000 | | | - |
| | | | AKCESK | A.1.4 Analiza e hendekut ligjor dhe institucional për Direktivat dhe Rregulloret e EU që normojnë fushën e sigurisë kibernetike | 61,200 | 61,200 | - | - | | 61,200 | | | - |
| | | | AKCESK | A.1.5. Legjislacioni i përafruar i miratuar | 140,400 | 46,800 | 46,800 | 46,800 | | 140,400 | | | - |
| | | | AKCESK | A.1.6. Rregullorja per ofrimin e Internetit te sigurt në hapësirat publike e hartuar dhe miratuar | 187,200 | 62,400 | 62,400 | 62,400 | | 187,200 | | | - |
| | | | | **Subtotal A.1.** | **622,800** | **357,600** | **156,000** | **109,200** | - | - | **622,800** | **0** | **0** | **-** |
| | | A.2.Përshtatja e vazhdueshme e standardeve dhe rregullave sipas zhvillimeve të fushës, së sigurisë kibernetike. | PSH | A.2.1. Procedurat për identifikimin e krimit kibernetik të hartuara | - | - | - | - | | - | | | | - |
| | | | PSH | A.2.2 Procedurat për identifikimin e incidenteve kibernetike të hartuara | - | - | - | - | | - | | | | - |
| | | | PSH | A.2.3 Raporte periodike për matjen e përshtatshmërisë dhe eficencën e rregullores kombëtare për krimin kibernetik | - | - | - | - | | - | | | | - |
| | | | PSH | A.2.4. Strategjitë dhe politikat për mbrojtjen kibernetike të sistemeve të klasifikuara të hartuara e miratuara. | - | - | - | - | | - | | | | - |
| | | | PSH | A.2.5. Procedura dhe standartet teknike për mbrojtjen kibernetike të sistemeve të klasifikuara të zhvilluara | - | - | - | - | | - | | | | - |
| | | | | **Subtotal A.2.** | - | - | - | - | - | - | - | **0** | **0** | - |
| | | A.3. Përmbushja e angazhimeve të marra si vend i Aleancës së Atlantikut të Veriut, për hapësirën kibernetike. | PSH | A.3.1.Harmonizimi i politikave vendore me ato ndërkombëtare që lidhen me krimin kibernetik | - | - | - | - | | - | | | | - |
| | | | AKCESK | A.3.2. Harmonizimi i politikave kombëtare me politikat e Aleancës që lidhen me mbrojtjen kibernetike | 244,800 | 81,600 | 81,600 | 81,600 | | 244,800 | | | | - |
| | | | AKCESK | A.3.3. Pjesëmarrja aktive në takimet periodike të iniciativave të NATO-s si CDMB, MISP etj. | 2,925,000 | 975,000 | 975,000 | 975,000 | | 2,925,000 | | | | - |
| | | | AKCESK | me institucionet kombëtare të sigurisë dhe të mbrojtjes | 3,412,500 | 1,137,500 | 1,137,500 | 1,137,500 | | 3,412,500 | | | | - |
| | | | | **Subtotal A.3.** | - | - | - | - | | | - | - | - | - |
| | | A.4. Përcaktimi i një procedure kombëtare për rastet e gjendjeve të jashtëzakonshme të krijuar nga krizat kibernetike, me qëllim marrjen e masave konkrete për zgjidhjen e situatës në kohe reale. | AKCESK | A.4.1. Metodologjia për vlerësimin e rrezikut në nivel kombëtar e hartuar dhe miratuar. | 244,800 | 81,600 | 81,600 | 81,600 | | 244,800 | | | | - |
| | | | | **Subtotal A.4.** | **244,800** | **81,600** | **81,600** | **81,600** | - | - | **244,800** | **0** | **0** | - |
| | **Subtotal A.** | | | | **867,600** | **439,200** | **237,600** | **190,800** | - | - | **867,600** | - | - | - |
| | Objektivi Specifik B - Ngritja dhe funksionimi i CSIRT-eve në të gjithë sektorët e industrisë në nivel kombëtar | B.1. Ngritja e CSIRT-it Kombëtar dhe CSIRT-ve të reja sektoriale, në infrastrukturat kritike dhe të rëndësishme të Informacionit, si dhe fuqizimi I atyre ekzistuese | DSIK | B.1.1. Ngritja e strukturës pranë DSIK e cila do të luajë rolin e Autoritetit Kombëtar të Mbrojtjes Kibernetike per sistemet ku trajtohet informacion i klasifikuar "sekret shtetëror", mbështetur në VKM nr.542 datë 25.07.2019 "Për miratimin e rregullores "Për sigurimin e informacionit të klasifikuar që trajtohet në sistemet e komunikimit dhe të informacionit (SKI)" | 18,450,724 | 5,464,108 | 6,493,308 | 6,493,308 | - | - | 18,450,724 | | | - |
| | | | AKCESK | B.1.2. Procedurat per funksionimin e CSIRT Kombetar të hartuara dhe miratuara | - | - | - | - | | | - | | | - |
| | | | AKCESK | B.1.3. Struktura dhe përgjegjësitë e CSIRT Kombëtar të miratuara. | 91,800 | 61,200 | 30,600 | - | | | 91,800 | | | - |
| | | | AKCESK | funksional | - | - | - | - | | | - | | | - |
| | | | AKCESK | B.1.5. Kapacitetet vlerësuese dhe monitoruese të CSIRT-eve sektoriale të zhvilluara | 52,000 | 52,000 | - | - | | | 52,000 | | | - |
| | | | AKSHI | B.1.6. Optimizimi dhe zgjerimi i infrastrukturave të sigurisë | 106,525,000 | 28,037,000 | 53,647,000 | 24,841,000 | | | 106,525,000 | | | - |
| | | | AKSHI | Gov NET | 107,880,000 | 29,389,000 | 53,649,000 | 24,842,000 | | | 107,880,000 | | | - |
| | | | | **Subtotal B.1.** | **232,999,524** | **63,003,308** | **113,819,908** | **56,176,308** | - | - | **233,867,124** | - | - | - |
| | | B.2. Krijimi i kushteve optimale të punës për funksionimin e CSIRT-eve, në përmbushje të detyrave të veta, për të garantuar sigurinë kibernetike | AKSHI | B.2.1 Procedurat per funksionimin e CSIRT qeveritar të hartuara | 46,800 | 46,800 | - | - | | | 46,800 | | | - |
| | | | AKCESK | CSIRT-eve sektoriale të zhvilluara. | 61,200 | 61,200 | - | - | | | 61,200 | | | - |
| | | | | Subtotal B.2. | **108,000** | 108,000 | - | - | - | - | 108,000 | - | - | - |
| | | B.3. Ngritja e kapaciteteve të CSIRT-eve, nëpërmjet trajnimeve dhe stërvitjeve kibernetike. | AKCESK | Implementuara | 62,400 | 62,400 | - | - | | | 62,400 | | | - |
| | | | AKCESK | ne vit: | 920,000 | 920,000 | - | - | | | 920,000 | | | - |
| | | | | Subtotal B.3. | **982,400** | 982,400 | - | - | - | - | 982,400 | | | - |
| | **Subtotal B.** | | | | **234,089,924** | **64,093,708** | **113,819,908** | **56,176,308** | - | - | **234,957,524** | - | - | - |
| | Objektivi Specifik C -Fuqizimi dhe implementimi I masave të sigurisë në infrastrukturat kritike dhe të rëndësishme të informacionit | C.1. Përdorimi i zgjidhjeve hardware dhe software të avancuara për identifikimin, parandalimin,dhe menaxhimin e incidenteve kibernetike. | AKSHI | C.1.1. Realizimi i hulumtimeve për forcimin e prioriteteve kombëtare si një bazë për të parashikuar investimet për zhvillimin e sigurisë kibernetike. | 124,800 | - | - | - | | | - | | | 124,800 |
| | | | | Subtotal C.1. | - | - | - | - | - | - | - | - | - | - |
| | | C.2. Analizimi I infrastrukturave kritike dhe të rëndësishme të informacionit për vlerësimin e menaxhimin e riskut në to. | AKCESK | C.2.1. Procedura per zvogëllimin dhe menaxhimin e rrezikeve në hapësirën kibernetike e hartuar dhe e miratuar | 124,800 | 62,400 | 62,400 | - | | | 124,800 | | | - |
| | | | | Subtotal C.2. | **124,800** | 62,400 | 62,400 | - | - | - | 124,800 | - | - | - |
| | | C.3. Hartimi i planeve strategjike për mbrojtjen e hapësirës kibernetike nga incidente të mundshme. | AKCESK | C.3.1 Procedurat, politikat dhe planet për mbrojtjen e hapësirës kibernetike nga incidentet kibernetike të hartuara dhe të miratuara. | 187,200 | 62,400 | 62,400 | 62,400 | | | 187,200 | | | - |
| | | | AKCESK | sigurimin e mbrojtjes, testimin dhe vlerësimin e niveli të sigurisë së hapësirës kibernetike. | 140,400 | 46,800 | 46,800 | 46,800 | | | 140,400 | | | - |
| | | | | Subtotal C.3. | **327,600** | 109,200 | 109,200 | 109,200 | - | - | 327,600 | - | - | - |
| | | C.4 Realizimi i vlerësimeve ne infrastrukturat kritike dhe të rëndësishme të informacionit për | AKCESK | për nivelin e maturimit te Sigurise Kibernetike | 187,200 | 62,400 | 62,400 | 62,400 | | | 187,200 | | | - |
| | | | | Subtotal C.4. | 187,200 | 62,400 | 62,400 | 62,400 | - | - | 187,200 | - | - | - |
| | **Subtotal C.** | | | | **639,600** | **234,000** | **234,000** | **171,600** | - | - | **639,600** | - | - | - |
| | Objektivi Specifik D - Përmirësimi I infrastrukturave të informacionit për të luftuar | D.1. Monitorimi dhe parandalimi i fenomeneve, që nxisin ekstremizmin e dhunshëm dhe radikalizimin në shtresat vulnerabël në hapësirën | CVE | gjenerohen nga faqet web ne gjuhen shqipe me qëllim sinjalizimin, analizimin dhe ne vijim | - | - | - | - | | | - | | | - |
| | | | CVE | radikalizimit dhe ekstremizmit te dhunshem online" me target grupe te ndryshme sipas | - | - | - | - | | | - | | | - |
| | | | | **Subtotal D.1.** | - | - | - | - | - | - | - | - | - | - |
| | | D.2 Evidentimi në vazhdimësi I elementeve kontaminues, që qarkullojnë në Internet, që cënojnë sigurinë kibernetike në vend | PSH | D.2.1. Kapacitetet ekzistuese të mbrojtjes kibernetike të identifikuara | - | - | - | - | | | - | | | - |
| | | | | **Subtotal D.2.** | - | - | - | - | - | - | - | - | - | - |
| | | D.3 Ngritja e mekanizmave për rregullimin e Internetit të sigurt në ambientet publike, të certifikuar nga autoriteti rregullues I fushës së sigurisë kibernetike | AKCESK | D.3.1 Mekanizmat suportues për Teknologjinë e Informacionit dhe Komunikimit dhe sigurinë kibernetike të hartuara. | 234,000 | 78,000 | 78,000 | 78,000 | | | 234,000 | | | - |
| | | | | **Subtotal D.3** | **234,000** | **78,000** | **78,000** | **78,000** | - | - | **234,000** | - | - | - |
| | | | AKSHI | D.4.1 Analiza e kapaciteteve aktuale të autoriteteve përgjegjëse dhe identifikimi I gap-eve | 187,200 | - | - | - | | | - | | | 187,200 |
| | | | AKSHI | kapacitetove të autoriteteve përgjegjëse | 187,200 | - | - | - | | | - | | | 187,200 |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| krimin kibernetik, radikalizmin dhe ekstremizmin e dhunshëm | | AKSHI | D.4.2 Krijimi i një sistemi të mbrojtjes kibernetike për infrastrukturën kritike të informacionit të sektorit qeveritar. | | | | | | | | | | | - |
| | | | Ngritja e sistemit te kontrollit te aksesit ne rrjetin GovNet | 23,985,000 | 20,910,000 | 3,075 | - | - | - | | | | | - |
| | | | Risk assessment program + threat response and remediation | 86,100,000 | 86,100,000 | - | - | - | - | | | | | - |
| | D.4 Ngritja e kapaciteteve të autoriteteve përgjegjëse kundër krimit kibernetik. | | Designated Support Engineering Cybersecurity | 13,530,000 | 13,530,000 | | - | - | - | | | | | - |
| | | | Staff training | 7,380,000 | 4,920,000 | 2,460,000 | - | - | - | | | | | - |
| | | | ISO 27001 Information security procedures review | 8,610,000 | 8,610,000 | | - | - | - | | | | | - |
| | | | Sherbim monitorimi i qarkullimit te informacioneve sensitive ne world wide web | 60,885,000 | 40,590,000 | 20,295,000 | - | - | - | | | | | - |
| | | | Test Center of malicious programs and suspicious applications (Malware Testing Center MTC) developed and functional | 6,150,000 | 6,150,000 | | - | - | - | | | | | - |
| | | | HoneyPot Systems developed and operational for detecting, analyzing and preventing potential cyberattacks | 79,950,000 | 79,950,000 | | - | - | - | | | | | - |
| | | | **Subtotal D.4** | **286,964,400** | **260,760,000** | **22,758,075** | **-** | **-** | **-** | **-** | **-** | **-** | **374,400** | |
| | D.5 Rritja e bashkëpunimit rajonal në luftën kundër krimit kibernetik | FSH | kibernetik midis entiteteve kombëtare përkatëse dhe shërbimeve të tjera të sigurisë të | - | - | - | - | | | - | | | | - |
| | | FSH | luftën kundër krimit kibernetik. | - | - | - | - | | | - | | | | - |
| | | | **Subtotal D.5** | **-** | **-** | **-** | **-** | **-** | **-** | **-** | **-** | **-** | **-** | |
| | **Subtotal D.** | | | **287,198,400** | **260,838,000** | **22,836,075** | **78,000** | **-** | **-** | **234,000** | **-** | **-** | **374,400** | |
| **Total 1** | | | | **522,795,524** | **325,604,908** | **137,127,583** | **56,616,708** | **-** | **-** | **236,698,724** | **-** | **-** | **374,400** | |

| Qëllimi i politikës 2 | Specific objective | Sub- Objective | Institucioni përgjegjës | Results | Kosto totale | Kostot në Lek | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Viti 2021 | Viti 2022 | Viti 2023 | Viti 2024 | Viti 2025 | PBA | Donatore | Te tjere | Hendeku |
| | Objektivi Specifik A - Rritja e kapaciteteve profesionale në fushën e sigurisë së informacionit nëpërmjet rishikimit të kurrikulave arsimore | A.1 -Hartimi I programeve studimore në arsimin e lartë në fushën e sigurisë kibernetike, me qëllim krijimin e gjeneratës së re të ekspertëve të | AKCESK | A.1.1. Programet studimore të hartuara për punonjësit e administratës publike. | 187,200 | 62,400 | 62,400 | 62,400 | | | 187,200 | | | - |
| | | | AKCESK | A.1.2. Programet studimore të hartuara për stafin menaxherial ne sektorin publik. | 187,200 | 62,400 | 62,400 | 62,400 | | | 187,200 | | | - |
| | | | AKCESK | kibernetike | 3,148,800 | 807,600 | 807,600 | 1,533,600 | | | 3,148,800 | | | - |
| | | | | **Subtotal A.1.** | **3,523,200** | **932,400** | **932,400** | **1,658,400** | **-** | **-** | **3,523,200** | **-** | **-** | **-** |
| | | A.2. Hartimi I rekomandimeve për integrimin në kurrikula universitare të informacioneve në lidhje me Internetin e Sigurt. | TBD (pas 2022) | A.2.1. Ngritja e qendrës kërkimore shkencore në fushën e sigurisë kibernetike. | - | - | - | - | | | - | | | - |
| | | | TBD (pas 2022) | lidhura me sigurinë kibernetike. | - | - | - | - | | | - | | | - |
| | | | | **Subtotal A.2.** | **-** | **-** | **-** | **-** | **-** | **-** | **-** | **-** | **-** | **-** |
| | | A.3. Rritja e kapaciteteve kërkimore dhe inovative në fushën e sigurisë | AKCESK | dhe përgjegjësisë individuale në lidhje me mbrojtjen dhe sigurinë kibernetike. | - | - | - | - | | | - | | | - |
| | | | | **Subtotal A.3.** | **-** | **-** | **-** | **-** | **-** | **-** | **-** | **-** | **-** | **-** |
| | | **Subtotal A.** | | | **3,523,200** | **932,400** | **932,400** | **1,658,400** | **-** | **-** | **3,523,200** | **-** | **-** | **-** |
| | Objektivi Specifik B - Rritja e ndërgjegjësimit dhe e aftësive profesionale të Institucioneve publike dhe private për sigurinë kibernetike. | B.1. Trajnime periodike, per theellimin e njohurive në sigurinë kibernetike, sipas dinamikës së fushës, për stafin administrativ në nivel qendror dhe në | AKCESK | B.1.1. Kurrikulat për trajnime mbi sigurinë kibernetike të hartuara | 187,200 | 62,400 | 62,400 | 62,400 | | | 187,200 | | | - |
| | | | AKCESK | B.1.2 Realizimi i trajnimeve për sigurinë kibernetike me stafin administrativ në nivel qendror | 4,238,400 | 1,412,800 | 1,412,800 | 1,412,800 | | | 4,238,400 | | | - |
| | | | AKCESK | B.1.3 Realizimi i trajnimeve për sigurinë kibernetike me stafin administrativ në nivel lokal | 4,209,600 | 1,403,200 | 1,403,200 | 1,403,200 | | | 4,209,600 | | | - |
| | | | | **Subtotal B.1.** | **8,635,200** | **2,878,400** | **2,878,400** | **2,878,400** | **-** | **-** | **8,635,200** | **-** | **-** | **-** |
| | | B.2. Rritja dhe mbështetja e kapaciteteve kërkimore dhe risive të biznesit nëpërmjet mitjes së ngritjes së qendrave kërkimore shkencore në fushën e sigurisë kibernetike | AKCESK | B.2.1 Analiza e situatës aktuale | 234,000 | 78,000 | 78,000 | 78,000 | | | 234,000 | | | - |
| | | | AKCESK | B.2.2 Hartimi i rekomandimeve për biznesin | 187,200 | 62,400 | 62,400 | 62,400 | | | 187,200 | | | - |
| | | | AKCESK | B.2.3 Monitorimi dhe vlerësimi i zbatimit të rekomandimeve në risitë e biznesit | 81,600 | 81,600 | - | - | | | 81,600 | | | - |
| | | | | **Subtotal B.2.** | **502,800** | **222,000** | **140,400** | **140,400** | **-** | **-** | **502,800** | **-** | **-** | **-** |
| | | B.3. Rritja e kapaciteteve të CSIRT-eve në nivel kombëtar dhe nivelit ekzekutiv të administratës publike nëpërmjet trajnimeve dhe stërvitjeve kibernetike. | AKCESK | B.3.1 Hartimi i moduleve të trajnimit | 124,800 | 62,400 | 62,400 | - | | | 124,800 | | | - |
| | | | AKCESK | B.3.2 Organizimi i stërvitjeve kibernetike | 2,547,200 | 1,242,400 | 1,242,400 | 62,400 | | | 2,547,200 | | | - |
| | | | | **Subtotal B.3.** | **2,672,000** | **1,304,800** | **1,304,800** | **62,400** | **-** | **-** | **2,672,000** | **-** | **-** | **-** |
| | | **Subtotal B.** | | | **11,810,000** | **4,405,200** | **4,323,600** | **3,081,200** | **-** | **-** | **11,810,000** | **-** | **-** | **-** |
| | Objektivi Specifik C - Rritja e ndërgjegjësimit të shoqërisë, për sigurinë kibernetike dhe kërcënimet kibernetike. | C.1 Rritja e ndërgjegjësimit të shoqërisë për sigurinë kibernetike, duke përdorur hapësirat e duhura për realizimin e tyre, përfshirë edhe mediat audiovizive apo edhe ato | AKCESK | C.1.1 Hartimi I materialeve ndërgjegjësuese | - | - | - | - | | | - | | | - |
| | | | AKCESK | C.1.2 Organizimi I fushatave të ndërgjegjësimit | - | - | - | - | | | - | | | - |
| | | | AKCESK | C.1.3 Realizimi I fushatave publicitare / spoteve në media audiovizive për ndërgjegjësim | - | - | - | - | | | - | | | - |
| | | | | **Subtotal C.1** | **-** | **-** | **-** | **-** | **-** | **-** | **-** | **-** | **-** | **-** |
| | | C.2 Krijimin e një platforme edukative online, për sigurinë kibernetike, për të | AKCESK | C.2.1 Hartimi I materialeve të platformës | - | - | - | - | | | - | | | - |
| | | | AKCESK | C.2.2 Platforma e zhvilluar dhe funksionale | - | - | - | - | | | - | | | - |
| | | rritur ndërgjegjësimin në grupmosha të ndryshme të shoqërisë, për përdorimin e internetit të sigurt dhe të infrastrukturës digjitale | | **Subtotal C.2** | **-** | **-** | **-** | **-** | **-** | **-** | **-** | **-** | **-** | **-** |
| | | **Subtotal C.** | | | **-** | **-** | **-** | **-** | **-** | **-** | **-** | **-** | **-** | **-** |
| **Total 2** | | | | | **589,730,000** | **527,013,600** | **50,928,150** | **4,895,600** | **-** | **-** | **15,801,200** | **-** | **-** | **748,800** |

| Qëllimi i politikës 3 | Specific objective | Sub- Objective | Institucioni përgjegjës | Results | Kosto totale | Kostot në Lek | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Viti 2021 | Viti 2022 | Viti 2023 | Viti 2024 | Viti 2025 | PBA | Donatore | Te tjere | Hendeku |
| | Objektivi Specifik A - Forcimi i kuadrit ligjor për rritjen e sigurisë së fëmijëve në Internet. | A.1 - Hartimi I një udhëzimi të posaçëm (dhe rregullores shoqëruese) për mbledhjen e të dhënave të incidenteve të raportuara të dhunës, bullizmit dhe abuzimit online të fëmijëve në shkolla. | MASR | A.1.1. Udhëzimi për mbledhjen e të dhënave të incidenteve të raportuara të dhunës,bullizmit dhe abuzimit online në shkolla I hartuar dhe miratuar. | - | - | - | - | | | - | | | - |
| | | | MASR | dhunës,bullizmit dhe abuzimit online në shkolla e hartuar dhe miratuar | - | - | - | - | | | - | | | - |
| | | | MASR | A.1.3 Metodologjia e mbledhjes se rasteve te incidenteve ne sholla e hartuar dhe miratuar | - | - | - | - | | | - | | | - |
| | | | MASR | A.1.4 Raportet e Institucionet arsimore vendore, përgjegjëse për arsimin parauniversitar | - | - | - | - | | | - | | | - |
| | | | | Subtotal A.1. | - | - | - | - | - | - | - | - | - | - |
| | | A.2. Përmirësimi I kuadrit rregullator për ta sjellë në linjë me legjislacionin ndërkombëtar për mbrojtjen e fëmijëve nga abuzimi seksual në internet | AKCESK | A.2.1. Analiza e hendekut ligjor kombetar për mbrojtjen e fëmijëve nga abuzimi seksual në internet | 124,800 | - | 124,800 | - | | | 124,800 | | | - |
| | | | AKCESK | A.2.2 Hartimi I rekomandimeve për harmonizimin me legjislacionin ndërkombëtar të fushës. | 62,400 | - | 62,400 | - | | | 62,400 | | | - |
| | | | AKCESK | A.2.3 Aktet ligjore të hartuara e të miratuara | 46,800 | - | 46,800 | - | | | 46,800 | | | - |
| | | | | Subtotal A.2. | 234,000 | - | 234,000 | - | - | - | 234,000 | - | - | - |
| | | A.3. Plotësimi dhe qartësimi I legjislacionit në lidhje me njoftimin dhe heqjen dhe bllokimit të materialeve të paligjshme online | AKCESK | A.3.1. Analiza dhe identifikimi I gapeve të nivel kombetar | 124,800 | 124,800 | - | - | | | 124,800 | | | - |
| | | | AKCESK | A.3.2 Hartimi I protokollit te nevojshem per koordinimin nderinstitucional | 62,400 | 62,400 | - | - | | | 62,400 | | | - |
| | | | AKCESK | A.3.3 Protokolli I hartuar dhe miratuar | 46,800 | 46,800 | - | - | | | 46,800 | | | - |
| | | | | **Subtotal A.3.** | **234,000** | **234,000** | **-** | **-** | **-** | **-** | **234,000** | **-** | **-** | **-** |
| | | **Subtotal A.** | | | **468,000** | **234,000** | **234,000** | **-** | **-** | **-** | **468,000** | **-** | **-** | **-** |
| | Objektivi Specifik B - Parandalimi I abuzimit seksual të fëmijëve në Internet nëpërmjet rritjes së ndërgjegjësimit | B.1. Integrimi I programit 'Edukatorët bashkëmoshatarë për sigurinë | MASR | sigurinë online' në shkollat 9-vjeçare | - | - | - | - | | | - | | | - |
| | | | | **Subtotal B.1.** | **-** | **-** | **-** | **-** | **-** | **-** | **-** | **-** | **-** | **-** |
| | | B.2. Krijimi dhe mbeshtetja e rrjetit online të mësuesve të TIK për të promovuar cështjen e mbrojtjes së | MASR | B.2.1.Krijimi I rrjetit të mësuesve TIK online | - | - | - | - | | | - | | | - |
| | | | MASR | B.2.2.Zhvillimi I platformës së komunikimit midis tyre | - | - | - | - | | | - | | | - |
| | | | | **Subtotal B.2.** | **-** | **-** | **-** | **-** | **-** | **-** | **-** | **-** | **-** | **-** |
| | | B.3 Krijimi I hapësirave publike me Internet të sigurtë për fëmijët dhe familjet nëpërmjet nismës 'Friendly WI-FI' në 5 Bashki të vendit, duke | AKCESK | B.3.1 Hartimi I udhëzimit për Internet të sigurtë në hapësira publike | 182,000 | 78,000 | 78,000 | 26,000 | | | 182,000 | | | - |
| | | | AKCESK | B.3.2 Monitorimi I aplikimit të udhëzimit | 31,200 | 31,200 | - | - | | | 31,200 | | | - |
| | | | | **Subtotal B.3.** | **213,200** | **109,200** | **78,000** | **26,000** | **-** | **-** | **213,200** | **-** | **-** | **-** |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| dhe krijimit të hapësirave të sigurta për fundrimin në Internet | B.4 Aplikimi i filtrave në shkollat publike dhe private për të parandaluar aksesin e fëmijëve në faqe të papërshtatshme dhe të | MASR | B.4.1 Raportet e mirëmbajtjes dhe kontrollit të vlefshmërisë së filtrave | - | - | - | - | | | - | | | - |
| | | MASR | Mësuesit e TIK pranë Institucioneve arsimore vendore, përgjegjëse për arsimin | - | - | - | - | | | - | | | - |
| | | | **Subtotal B.4.** | - | - | - | - | - | - | - | - | - | - |
| | B.5 Identifikimi, mbështetja dhe promovimi i talenteve për të krijuar zgjidhje teknike që ndihmojnë në | MASR | B.9.1 Hartimi i metodologjive për identifikimin e talenteve të reja | - | - | - | - | | | - | | | - |
| | | MASR | B.9.2 Monitorimi i aplikimit të metodologjisë së hartuar | - | - | - | - | | | - | | | - |
| | | | **Subtotal B.5.** | - | - | - | - | - | - | - | - | - | - |
| | **Subtotal B.** | | | 213,200 | 109,200 | 78,000 | 26,000 | - | - | 213,200 | - | - | - |
| | C.1.Sigurimi i mjeteve teknike që ndihmojnë policinë dhe organet përkatëse në analizimin dhe zbulimin e rasteve të dhunës online vecanerisht lidhur me imazhet e abuzimit seksual me fëmijët | Policia e Shtetit | C.1.1. Analiza e situatës aktuale në përgjigjet ndaj rasteve të dhunës | - | - | - | - | | | - | | | - |
| | | Policia e Shtetit | raportuara | - | - | - | - | | | - | | | - |
| | | | **Subtotal C.1.** | - | - | - | - | - | - | - | - | - | - |
| Objektivi Specifik C - Hetimi efektiv dhe sjellja para drejtësisë e autorëve të krimeve kibernetike ndaj fëmijëve, me fokus abuzimin dhe shfrytëzimin seksual | C.2. Krijimi i programeve të trajnimit për personelin e gjyqësorit, prokurorisë dhe Policisë në lidhje me mbrojtjen e fëmijëve në Internet dhe | MB/AKCESK | C.2.1. Hartimi i kurrikulave të trajnimit | 124,800 | 62,400 | 62,400 | - | | | 124,800 | | | - |
| | | MB/AKCESK | C.2.2 Organizimi i programeve të trajnimit | 1,600,000 | 560,000 | 560,000 | 480,000 | | | 1,600,000 | | | - |
| | | | **Subtotal C.2.** | **1,724,800** | **622,400** | **622,400** | **480,000** | - | - | **1,724,800** | - | - | - |
| | C.3. Ngritja e një sistemi kursesh pranë Shkollës se Magjistraturës dhe Akademisë së Sigurisë në lidhje me | AKCESK | C.3.1 Hartimi i kurrikulave të trajnimit | 124,800 | 62,400 | 62,400 | - | | | 124,800 | | | - |
| | | AKCESK | C.3.2 Organizimi i programeve të trajnimit | 1,600,000 | 560,000 | 560,000 | 480,000 | | | 1,600,000 | | | - |
| | | | **Subtotal C.3.** | **1,724,800** | **622,400** | **622,400** | **480,000** | - | - | **1,724,800** | - | - | - |
| | C.4 Krijimi i mekanizmave për standardizimin e punës së analizimit të provave digitale nga Policia e Shtetit. | PSH | C.4.1 Analiza e situatës aktuale mbi mekanizmat për analizimin e provave digitale | 124,800 | 62,400 | 62,400 | - | | | 124,800 | | | - |
| | | PSH | C.4.2 Hartimi i rekomandimeve | 62,400 | 62,400 | - | - | | | 62,400 | | | - |
| | | PSH | C.4.3 Monitorimi i zbatueshmërisë së mekanizmave të krijuar | 46,800 | 46,800 | - | - | | | 46,800 | | | - |
| | | | **Subtotal C.4.** | **234,000** | **171,600** | **62,400** | - | - | - | **234,000** | - | - | - |
| | C.5 Krijimi i një grupi pune së bashku me industrinë për të zgjidhur problemet e hetimit dhe identifikimit të personave të dyshuar për abuzim me fëmijët online, me fokus të | PSH | C.5.1 Hartimi i udhrit për ngritjen e grupit të punës | - | - | - | - | | | - | | | - |
| | | PSH | C.5.2 Hartimi i metodologjisë së bashkëpunimit të grupit të punës | - | - | - | - | | | - | | | - |
| | | | **Subtotal C.5.** | - | - | - | - | - | - | - | - | - | - |
| | **Subtotal C.** | | | **3,683,600** | **1,416,400** | **1,307,200** | **960,000** | - | - | **3,683,600** | - | - | - |
| Objektivi Specifik D - Rritja e ndërgjegjësimit dhe edukimi tek të gjitha segmentet e shoqërisë për përdorimin e sigurtë të Internetit nga fëmijët | D.1 Fushata ndërgjegjësimi me prindërit dhe edukatorët në lidhje me rreziqet dhe problemet me të cilat përballen fëmijët në Internet | AKCESK | D.1.1 Hartimi i kurrikulave të trajnimit | 124,800 | 62,400 | 62,400 | - | | | 124,800 | | | - |
| | | AKCESK | D.1.2 Organizimi i fushatave të ndërgjegjësimit | 1,600,000 | 560,000 | 560,000 | 480,000 | | | 1,600,000 | | | - |
| | | | **Subtotal D.1** | **1,724,800** | **622,400** | **622,400** | **480,000** | - | - | **1,724,800** | - | - | - |
| | D.2 Zhvillimi i programeve të trajnimit me mësuesit e TIK në lidhje me çështjet e Internetit të sigurtë | AKCESK | D.2.1. Hartimi i kurrikulave të trajnimit | 124,800 | 62,400 | 62,400 | - | | | 124,800 | | | - |
| | | AKCESK | D.2.2 Organizimi i programeve të trajnimit | 1,600,000 | 560,000 | 560,000 | 480,000 | | | 1,600,000 | | | - |
| | | | **Subtotal D.2.** | **1,724,800** | **622,400** | **622,400** | **480,000** | - | - | **1,724,800** | - | - | - |
| | D.3 Zhvillimi i programeve të trajnimit për Punonjësit e Mbrojtjes së Fëmijës lidhur me trajtimin e rasteve të fëmijëve në nevojë për mbrojtje ku rreziku i dhunës, abuzimit, | AKCESK | D.3.1 Hartimi i kurrikulave të programeve të trajnimit | 124,800 | 62,400 | 62,400 | - | | | 124,800 | | | - |
| | | AKCESK | D.3.2 Organizimi i fushatave të trajnimit | 1,600,000 | 560,000 | 560,000 | 480,000 | | | 1,600,000 | | | - |
| | | | **Subtotal D.3.** | **1,724,800** | **622,400** | **622,400** | **480,000** | - | - | **1,724,800** | - | - | - |
| | **Subtotal D.** | | | **5,174,400** | **1,867,200** | **1,867,200** | **1,440,000** | - | - | **5,174,400** | - | - | - |
| Objektivi Specifik E - Forcimi i bashkëpunimit ndërsektorial për mbrojtjen e fëmijëve në Internet. | E.1. Promovimi nëpërmjet bashkëpunimit me të gjitha ISP-të i mekanizmave ekzistues të aplikuar në platformat e tyre per sigurinë e fëmijëve në Internet. | AKCESK | E.1.1. Organizimi i aktiviteteve për promovimin e mekanizmave të mbrojtjes së fëmijëve në | 200,000 | 200,000 | - | - | | | 200,000 | | | - |
| | | AKCESK | E.1.2 Hartimi i fletëpalosjeve / materiale informuese me mekanizmat ekzistues për mbrojtjen e fëmijëve në Internet | 31,200 | 31,200 | - | - | | | 31,200 | | | - |
| | | | **Subtotal E.1.** | 231,200 | 231,200 | - | - | - | - | 231,200 | - | - | - |
| | E.2 Integrimi nga të gjitha ISP-të në platformat e tyre të Listës IWF (Internet Watch Foundation Hash List) që ndalon çdo individ të hedhë, shkarkojë apo shikojë imazhe apo | Propozim i shoqërisë civile (UNICEF) | E.2.1. Hartimi i udhëzimit për integrimin e listës IWF në platformat e ISP-ve | - | - | - | - | | | - | | | - |
| | | Propozim i shoqërisë civile | E.2.2 Monitorimi i zbatueshmërisë së udhëzimit të hartuar | - | - | - | - | | | - | | | - |
| | | | **Subtotal E.2.** | - | - | - | - | - | - | - | - | - | - |
| | E.3 Ngritja e një Komiteti Teknik Këshillues për Sigurinë e Fëmijëve në Internet, pranë Këshillit Kombëtar për të Drejtat dhe Mbrojtjen e Fëmijëve | MSH | E.3.1 Takime të komiteteve teknike këshilluese, për çështjet e të drejtave dhe mbrojtjes të fëmijëve. | - | - | - | - | | | - | | | - |
| | | MSH | E.3.2 Percaktim i rregulloreve mbi të drejtat dhe mbrojtjen e fëmijëve | - | - | - | - | | | - | | | - |
| | | | **Subtotal E.3** | - | - | - | - | - | - | - | - | - | - |
| | **Subtotal E.** | | | 231,200 | 231,200 | - | - | - | - | 231,200 | - | - | - |
| **Total 3** | | | | **9,770,400** | **3,858,000** | **3,486,400** | **2,426,000** | - | - | **9,770,400** | - | - | - |

| | Specific objective | Sub- Objective | Institucioni përgjegjës | Results | Kosto totale | Kostot në Lek | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Viti 2021 | Viti 2022 | Viti 2023 | Viti 2024 | Viti 2025 | PBA | Donatore | Te tjere | Hendeku |
| Q | | A.1. Rritja e bashkëpunimit dhe koordinimit ndërmjet institucioneve shtetërore për të garantuar sigurinë në nivel kombëtar në hapësirën kibernetike | AKCESK | A.1.1. Hartimi dhe nënshkrimi i marrëveshjeve ndërinstitucionale | 140,400 | 46,800 | 46,800 | 46,800 | | | 140,400 | | | - |
| | | | AKCESK | A.1.2 Krijimi i njetat të pikave të kontaktit dhe hartimi i metodologjisë së punës së njetit | 140,400 | 46,800 | 46,800 | 46,800 | | | 140,400 | | | - |
| | | | AKCESK | besimit me ekspet e tjera publike dhe private të CERT dhe CSIRT, dhe komunitetet akademike. | 140,400 | 46,800 | 46,800 | 46,800 | | | 140,400 | | | - |
| | | | | **Subtotal A.1.** | 421,200 | 140,400 | 140,400 | 140,400 | - | - | 421,200 | - | - | - |
| E | Objektivi Specifik A - Forcimi i bashkëpunimit institucional në nivel kombëtar | A.2. Krijimi i një instrumenti për shkëmbimin e informacionit përmes | AKCESK | platforme/sistemi kombëtar për shkëmbimin e informacionit në lidhje me ligjet, incidentet dhe | 140,400 | 46,800 | 46,800 | 46,800 | | | 140,400 | | | - |
| | | | AKCESK | njoftuese dhe përvojes midis sektorit publik dhe atij të mbrojtjes dhe sigurisë në fushën e | 140,400 | 46,800 | 46,800 | 46,800 | | | 140,400 | | | - |
| | | | AKCESK | informacioni me sektorët privatë dhe civil | 140,400 | 46,800 | 46,800 | 46,800 | | | 140,400 | | | - |
| | | | AKCESK | normave të sigurisë, standardizimin e bashkëpunimit, si dhe përcaktimin dhe vendosjen e | 140,400 | 46,800 | 46,800 | 46,800 | | | 140,400 | | | - |
| | | | AKCESK | të eilat do të shfaqen në pikat e aksjtjes | 62,400 | 62,400 | | | | | 62,400 | | | - |
| | | | | **Subtotal A.2.** | 624,000 | 249,600 | 187,200 | 187,200 | - | - | 624,000 | - | - | - |
| | | A.3. Ngritja e një strukture fleksibël me ekspertët më të mirë të sigurisë kibernetike në vend, me qëllim | AKCESK | A.3.1 Krijimi i instrumentit për ngritjen e strukturës | 124,800 | 62,400 | 62,400 | - | | | 124,800 | | | - |
| | | | AKCESK | A.3.2 Hartimi i metodologjisë së bashkëpunimit | 124,800 | 62,400 | 62,400 | - | | | 124,800 | | | - |
| | | | | **Subtotal A.3.** | 249,600 | 124,800 | 124,800 | - | - | - | 249,600 | - | - | - |
| | | | | **Subtotal A.** | 1,294,800 | 514,800 | 452,400 | 327,600 | - | - | 1,294,800 | - | - | - |
| | Objektivi Specifik B -Forcimi i bashkëpunimit ndërkombëtar në fushën e sigurisë dhe mbrojtjes kibernetike dhe luftës kundër ekstremizmit të dhunshëm dhe | B.1. Zhvillimi i mekanizmave dhe proceduarve efikase, për bashkëpunim ndërkombëtar, në rast | AKCESK | me zhvillimet më të fundit të fushës së sigurisë kibernetike. | 140,400 | 46,800 | 46,800 | 46,800 | | | 140,400 | | | - |
| | | | AKCESK | ndërinstitucionale për marrjen dhe shpërndarjen e informacionit | 140,400 | 46,800 | 46,800 | 46,800 | | | 140,400 | | | - |
| | | | | **Subtotal B.1.** | 280,800 | 93,600 | 93,600 | 93,600 | - | - | 280,800 | - | - | - |
| | | B.2. Forcimi i bashkëpunimit dhe shkëmbimi i informacionit me NATO / OSBE dhe organizata / forume të tjerë ndërkombëtarë | AKCESK | ndërkombëtare në kuadër të sigurisë kibernetike | 2,700,000 | 900,000 | 900,000 | 900,000 | | | 2,700,000 | | | - |
| | | | AKCESK | kibernetike dhe aktivitetet e ndërtimit të besimit. | 2,700,000 | 900,000 | 900,000 | 900,000 | | | 2,700,000 | | | - |
| | | | AKCESK | B.2.3 Anëtarësimi dhe pjesëmarrja në aktivitete dhe inicativa të ndryshme ndërkombëtare në fushën e sigurisë kibernetike (First, Trust Introducer) | - | - | - | - | | | - | | | - |
| | | | | **Subtotal B.2.** | 5,400,000 | 1,800,000 | 1,800,000 | 1,800,000 | - | - | 5,400,000 | - | - | - |
| | | **Subtotal B.** | | | 5,680,800 | 1,893,600 | 1,893,600 | 1,893,600 | - | - | 5,680,800 | - | - | - |
| l | **Total 4** | | | | 6,975,600 | 2,408,400 | 2,346,000 | 2,221,200 | - | - | 6,975,600 | - | - | - |
| i | | | | | | | | | | | | | | |
| p | | | | | | | | | | | | | | |
| o | | | | | | | | | | | | | | |
| l | | | | | | | | | | | | | | |
| i | | | | | | | | | | | | | | |
| t | | | | | | | | | | | | | | |
| i | | | | | | | | | | | | | | |
| k | | | | | | | | | | | | | | |
| e | | | | | | | | | | | | | | |
| s | | | | | | | | | | | | | | |
| 4 | | | | | | | | | | | | | | |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| KOSTO TOTALE E STRATEGJISE | 522,795,524 | 325,604,908 | 137,127,583 | 56,616,708 | - | - | 236,698,724 | - | - | 374,400 |