



Влада на Република Северна Македонија

Стратегија за градење
отпорност и справување со
хибридни закани

PËRMBAJTJA

Parathënie nga kryetari i Qeverisë së Republikës së Maqedonisë së Veriut -----	2
Parathënie nga ministrja e Mbrojtjes e Republikës së Maqedonisë së Veriut -----	4
1. Hyrje-----	5
2. Kërcënimet hibride si koncept -----	8
2.1. Përkufizimi i kërcënimeve hibride-----	8
2.2. Metodatat dhe instrumentet hibride-----	8
2.3. Baza për ndërtimin e rezistencës dhe menaxhimit me kërcënimet hibride -----	11
3. Qëllimet dhe efektet që duhet të arrihen -----	13
3.1. Qëllimet e strategjisë -----	13
3.2. Fushat operative -----	13
3.3. Qëllimet e fushave operative -----	14
4. Mënyrat për arritjen e efekteve dhe realizimit të qëllimit -----	22
4.1. Detektimi i kërcënimit -----	22
4.2. Refuzimi i kërcënimit -----	22
4.3. Përgjigje ndaj kërcënimit -----	23
5. Instrumentet për realizimin e qëllimit -----	25
6. Përcaktimi i shkallës së zbatimit të strategjisë -----	26
6.1 Sfidat e realizimit -----	26

Aneksi 1- Plani i veprimit për zbatimin e Strategjisë për ndërtimin e rezistencës nacionale dhe menaxhimin me kërcënimet hibride

PARATHËNIE



Qytetarë të nderuar!

Shumëdimensionaliteti dhe natyra e shpejtë e zhvillimit të kërcënimeve është padyshim tipar kyç i sigurisë në shekullin 21. As shtetet, as qytetarët, as organizatat ndërkombëtare nuk mund të parashikojnë se prej ku dhe në çfarë forme do të shfaqen kërcënimet moderne të sigurisë. Për parandalimin e të njëjtës, është e nevojshme reagim gjithëpërfshirës shoqëror dhe i koordinuar i të gjithë faktorëve në vend. Është obligimi ynë si shtet që të ofrojmë mbrojtjen dhe sigurinë më të mirë për qytetarët tanë.

Në vitin 2020, por edhe në vitin 2021, po përballemi me kërcënim shumëdimensional dhe gjithëpërfshirës për shëndetin e qytetarëve të shkakuar nga virusi Corona. Përgjigja në përballjen me pandeminë kërkonte gjithëpërfshirje në angazhimin e burimeve nacionale, duke përfshirë reagim të sinkronizuar të disa institucioneve shtetërore, por edhe të subjekteve të tjera në shtet. Përvoja e veprimit në gjendje të jashtëzakonshme na tregoi të gjitha dobësitë tona, por na bëri edhe më të fortë. Mësimet e nxjerra kanë treguar se ne duhet të investojmë më shumë në mekanizmat për ndërtimin e qëndrueshmërisë së shoqërisë në përballjen me kërcënimet, të cilat shpesh kanë karakter hibrid.

Hapi i parë në këtë drejtim është ndërtimi i qasjes gjithëpërfshirëse të shoqërisë në përballjen me kërcënimet hibride. Strategjia për përballimin e kërcënimeve hibride duhet t'i nxisë jo vetëm institucionet, por edhe gjithë shoqërinë për të ndërmarrë hapa konkretë për të ndërtuar rezistencë nacionale në përballjen me kërcënimet. Në të njëjtën kohë, është obligimi ynë, si vend-anëtar i Aleancës, të investojmë në ndërtimin e rezistencës nacionale, duke qenë se Aleanca ka njohur kërcënimet hibride si tregues të mundshëm për aktivizimin e nenit 5 të Marrëveshjes së Uashingtonit. Është përgjegjësia jonë nacionale të ndërtojmë sistem të sinkronizuar dhe të koordinuar të reagimit ndaj kërcënimeve. Pjesë përbërëse e kësaj politike është zbatimi i rekomandimeve të BE-së në fushën e ndërtimit të rezistencës ndaj kërcënimeve hibride, në pajtim me Kornizën e përbashkët të Bashkimit për ballafaqimin me kërcënimet hibride.

Qeveria e Republikës së Maqedonisë së Veriut është përgjegjëse ndaj qytetarëve të saj dhe ndaj aleatëve tanë dhe ka për obligim të ndërtojë shoqëri rezistuese. Ne kemi treguar se në situata krize, përfshirë edhe gjendjen e jashtëzakonshme, mund të përgjigjemi me vendosmëri dhe arritëm të mbrojmë shëndetin e qytetarëve. Në periudhën e ardhshme, Qeveria dhe të gjithë ne kemi përpara punë shumë serioze në këtë fushë. Obligimi i Qeverisë është të përgatisë plan gjithëpërfshirës dhe të koordinuar për funksionimin e shoqërisë në situata krize dhe emergjente, duke përfshirë sistem të masave për paralajmërim të hershëm, njoftim, reagim dhe rikuperim të shpejtë, me pjesëmarrjen e të gjithë faktorëve përkatës, në të gjitha situatat.

Ballafaqimi me pandeminë ka treguar se është e mundur vetëm me institucione funksionale shtetërore dhe bashkëpunim dhe koordinim të ndërsjellë me të gjithë faktorët në shoqëri. Prandaj, institucionet duhet të përgatiten për funksionimin e duhur në kushte të ndryshme, përfshirë në situata krize dhe emergjente. Është përgjegjësia jonë t'u lëmë brezave tanë bazë të mirë për të përmirësuar aftësinë për t'u përshtatur me realitetin dhe të ardhmen e paparashikueshme të sigurisë.

Kryetari i Qeverisë së Republikës së Maqedonisë së Veriut

Zoran Zaev

PARATHËNIE



Të nderuar!

Sot nuk ka kufi të qartë midis gjendjes së paqes, krizës dhe konfliktit, kjo e bën mjedisin e sigurisë të paparashikueshëm dhe kompleks. Faktorët shtetërorë dhe joshtetërorë përdorin metoda dhe mjete të ndryshme veprimi joushtarake për të destabilizuar, diskredituar apo krijuar destabilitet. Kërcënimet hibride, duke përfshirë përhapjen e lajmeve të rreme dhe dezinformatave, mund të shkaktojnë dëm të madh në shoqëri, pa përdorimin e as një ushtari ose mjete ushtarake. Efektet e zbatimit të këtyre metodave janë negative për çdo segment të shoqërisë. Kohët e fundit, ato kanë marrë intensitet të ri, dimension dhe shpejtësi të re, si rezultat i zhvillimit të shpejtë të teknologjisë dhe globalizimit.

Diskutimi për konceptin e kërcënimeve hibride, në mbarë botën, ende karakterizohet nga perceptime të ndryshme. Megjithatë, vitet e fundit kërcënimet hibride janë bërë pjesë e çdo ngjarje, bisede apo strategjie që lidhet me sigurinë dhe mbrojtjen. Ato gjithashtu gjenden lartë në agjendën e NATO-s dhe BE-së. Prandaj, të gjithë pajtohemi që, sot, një shoqëri rezistente është vija e parë e mbrojtjes nacionale.

Qasja e këtillë kërkon zgjerim të qasjes sonë ndaj sigurisë. Në planet tona për ndërtimin e rezistencës së shoqërisë, duhet ta përfshijmë infrastrukturën, sistemin e energjetikës dhe komunikimit, sistemet e furnizimit me ushqim dhe ujë, ndryshimet klimatike dhe me kujdes ta ndjekim zhvillimin teknologjik. Çdo shoqëri duhet të ndërtojë kapacitete për t'u përballur me sfidat e reja, në të njëjtën mënyrë dhe përkushtim siç ndërtohen kapacitetet për t'u përballur me kërcënim konvencional. Kështu, në të gjithë, si faktorë individual, duhet ta kuptojmë rolin, përgjegjësinë dhe obligimet tona në këtë sistem kompleks.

Siguria jonë është e pandashme nga siguria euroatlantike. Kjo është arsyeja pse kjo Strategji bazohet në dokumentet themelore strategjike të NATO-s dhe BE-së. NATO-ja pasqyron rëndësinë e rezistencës në "shtatë kërkesat themelore për rezistencë", të cilat janë pjesë e kësaj Strategjie dhe Planit të veprimit. Megjithatë, NATO-ja dhe BE-ja e shohin ndërtimin e rezistencës si përgjegjësi kryesisht nacionale, me implikime për qëndrueshmërinë rajonale dhe kolektive. Se si do ta organizojmë sistemin tonë dhe sa seriozisht i qasemi kësaj

sfide, varet nga ne.

Strategjia, së bashku me Planin e veprimit, është hapi i parë drejt arritjes së tërësisë. Ky është proces që kërkon përgjigje të qëndrueshme në të gjitha fushat funksionale. Gjithashtu, ky proces kërkon bashkëpunim të ngushtë ndërmjet të gjithë sektorëve në nivel nacional dhe me partnerët ndërkombëtarë, shkëmbim të informacioneve dhe përvojave dhe sigurisht, qasje dhe përkushtim serioz. Përfitimi nga sistemi i ndërtuar mirë do të thotë shoqëri rezistuese ndaj sfidave të reja të sigurisë, institucione të sigurta, vetëdije shoqërore dhe gatishmëri për mbrojtjen dhe sigurinë e qytetarëve dhe të mirave sociale.

Për këtë arsye, është e nevojshme që të gjithë të kontribuojmë dhe së bashku të ndërtojmë shoqëri më të sigurt dhe më rezistuese për qytetarët tanë, për të gjithë ne.

Ministrja e Mbrojtjes e Republikës së Maqedonisë së Veriut

Radmilla Shekerinska

DRAFT

1. Hyrje

Pamja moderne e sigurisë karakterizohet nga kërcënime komplekse, të cilat në thelb kanë ndryshuar që nga periudha e dy dekadave më parë. Kërcënimet për sulm me armë konvencionale janë pak të mundshme, por paralelisht rreziku i sulmeve me mjete jokonvencionale është rritur. Për këtë arsye, është e nevojshme të zgjerohet kuptimi dhe vizioni i mbrojtjes së shoqërisë duke njohur spektrin modern të kërcënimeve. Çdo shoqëri moderne duhet të ndërtojë koncept efektiv për t'u përballur me sfidat e shumtë si terrorizmi, ekstremizmi i dhunshëm dhe radikalizmi, proliferimi i armëve, ndërprerja e furnizimit me energji si dhe mbrojtja kundër

kërcënimeve kibernetike dhe hibride. Prandaj, çdo vend duhet të jetë në gjendje të përshtatet me realitetin e paparashikueshëm, kompleks dhe të ndryshueshëm të sigurisë.

Kërcënimet vijnë nga faktorë shtetërorë dhe joshtetërorë që përdorin gjithnjë e më shumë mekanizmat e fuqisë së "butë" (politike, ekonomike, informative) për të dobësuar institucionet, ekonomitë dhe shoqëritë dhe për të kërcënuar sigurinë e tyre. Duke marrë parasysh faktin se kërcënimet moderne kanë përmbajtje komplekse, imponohet edhe nevoja për t'iu përgjigjur gjithë shoqëria. Kjo nënkupton nevojën për të ndërtuar kapacitete nacionale për të përmirësuar rezistencën ndaj këtyre kërcënimeve përmes një qasje më të gjerë, më të integruar dhe më të koordinuar në nivel nacional.

Si anëtare e NATO-s, Republika e Maqedonisë së Veriut ka për obligim ta rrisë rezistencën nacionale ndaj gjithë spektrit të kërcënimeve dhe të zbatojë të ashtuquajturat shtatë nevojat/kërkesat bazë për rezistencë nacionale. Këto nevoja janë vendosur për të mbështetur tre funksionet thelbësore të gatishmërisë civile:

- vazhdimësia e pushtetit,
- vazhdimësia e shërbimeve themelore për popullatën,
- mbështetja civile e Armatës.

Krahas obligimit për mbrojtje kolektive, Republika e Maqedonisë së Veriut, si anëtare e NATO-s, ka obligim të ndërtojë dhe ruajë gatishmërinë dhe rezistencën përkatëse civile. Ndërtimi i rezistencës është në pajtim me nenin 3 të Marrëveshjes Veri-atlantike përkatësisht me obligimin për zhvillim kolektiv dhe individual të kapacitetet për t'iu përgjigjur çdo forme kërcënimi ose krize.

Strategjia për ndërtimin e rezistencës dhe përballimin e kërcënimeve hibride është dokument që duhet të rezultojë në krijimin e një aftësie nacionale për t'i përballuar me sukses kërcënimet apo krizat e shumëanshme, të cilat synojnë të kërcënojnë shoqërinë dhe vlerat tona demokratike si dhe të destabilizojnë funksionimin e institucioneve shtetërore. Qëllimi i kësaj strategjie është të krijojë vetëdije të përbashkët për natyrën e kërcënimeve hibride, hartimin e obligimeve dhe bartësve, identifikimin e mënyrave të veprimit si dhe krijimin e burimeve për ndërtimin e rezistencës nacionale duke angazhuar gjithë shoqërinë (whole- of- society approach). Kjo gjithashtu nënkupton ndërtimin e një shoqërie të përgatitur për zbulimin e hershëm, reagimin dhe rimëkëmbjen e shpejtë, me pjesëmarrjen e të gjithë faktorëve përkatës.

Gjithashtu, Republika e Maqedonisë së Veriut duhet të krijojë vlerësim të trendeve strategjike globale, në të cilin do të përcaktojë rolin e shtetit në botë, do të përcaktojë saktësisht dhe sipas prioritetit kërcënimet ndaj sigurisë nacionale, duke marrë parasysh efektet e ndryshimeve klimatike si dhe zhvillimi i teknologjive të reja, urbanizimi, ndryshimet gjeopolitike, ndotja e mjedisit, ndryshimet demografike dhe faktorë të tjerë.

2. Kërcënimet hibride si koncept

2.1. Përkufizimi i kërcënimeve hibride

Hapi i parë në ndërtimin e rezistencës dhe trajtimin e kërcënimeve hibride është përcaktimi teorik i këtij kërcënimi të sigurisë. Termi "kërcënim hibrid" do të thotë kombinim i aktiviteteve keqdashëse dhe subversive, metodave konvencionale dhe jokonvencionale (diplomatike, ushtarake, ekonomike, teknologjike), që përdoren në mënyrë të koordinuar nga subjektet shtetërore ose joushtetërore për të arritur qëllime të caktuara. Këto veprime janë të koordinuara, të sinkronizuara dhe kanë për qëllim dobësitë e qëllimit të caktuar. Ato mund të synojnë çdo fushë të shoqërisë, politike, ekonomike, ushtarake, civile apo informative. Gjithashtu, përdoret shumëllojshmëri të mjeteve, të dizajnuara për të mbetur të pazbuluar.

Kërcënimet hibride paraqesin kombinim të mjeteve ushtarake dhe joushtarake, duke përfshirë dezinformimin, sulmet kibernetike, presionin ekonomik, përdorimin dhe vendosjen e grupeve të armatosura të parregullta si dhe përdorimin e forcave të rregullta ushtarake. Intensiteti i kërcënimeve hibride ndryshon vazhdimisht, ashtu si edhe shkalla dhe shpejtësia e tyre. Prandaj, përkufizimi i kërcënimeve hibride duhet të shihet gjerësisht dhe në mënyrë fleksibile për t'iu përgjigjur natyrës së tyre në zhvillim.

2.2. Metodatat dhe instrumentet hibride

Kërcënimi hibrid nuk është koncept i ri strategjik, por më tepër risi e bazuar në përdorimin e teknologjive të reja dhe koncepteve të modifikuara. Metodatat që janë përdorur në të kaluarën, si sabotimi, propaganda apo taktika të tjera joushtarake, marrin kuptim të ri si rezultat i zhvillimit të teknologjisë. Epoka digjitale dhe globalizimi kanë rritur fuqinë e këtyre metodave, duke rritur shpejtësinë, intensitetin dhe shtrirjen e veprimit të tyre.

Lufta hibride nuk është metodë e pranuar zyrtarisht për arritjen e qëllimeve, por mënyrë për të shmangur luftën konvencionale dhe për të arritur qëllimin duke përdorur metoda jokonvencionale që do të ndikojnë negativisht në financat, politikën, ekonominë, sigurinë dhe strukturën sociale të një shoqërie. Përdorimi i forcës ushtarake në luftën hibride është mjeti i fundit dhe duhet të shmanget nëse është e mundur. Nëse përdoret forca ushtarake, vendi agresor mund të përdorë përfaqësues përkatësisht forca të parregullta, gjë që mundëson mohimin e përfshirjes së drejtpërdrejtë në dhunë nga shteti agresor.

Çelësi i kërcënimeve hibride janë instrumentet civile të pushtetit. Kërcënimi hibrid thekson fushë abstrakte të betejës ku sulmuesi kërkon të gërryjë kohezionin sociokulturor të qëllimit të targetuar. Dobësitë e shkaktuara nga ndryshimet socio-kulturale shfrytëzohen brenda këtyre kornizave kurse ndikimi i sektorit civil shpesh përdoret për të arritur ndikim. Rrjedhimisht, Republika e Maqedonisë së Veriut duhet ta mbrojë kohezionin socio-kulturor të qytetarëve të vendit dhe ta menaxhojë ndikimin e organizatave të huaja qeveritare dhe joqeveritare, veçanërisht ato me origjinë nga vendet që nuk janë anëtare të BE-së dhe NATO-s.

Metodë domethënëse e përdorur në kërcënimin hibrid, nëpërmjet përdorimit të instrumenteve civile të pushtetit, është përhapja e ideologjive dhe keqpërdlrimi me kulturën për të arritur ndikimin e dëshiruar. Ideologjitë dhe përdorimi i vlerave kulturore përdoren për të imponuar ndërjegjësimin e individëve, për të ndryshuar qëndrimet e tyre politiko-ideologjike dhe kulturore dhe për të shkaktuar përhapjen e mëtejshme të një ndikimi të tillë në shoqërinë e targetuar. I tillë është rasti me Federatën Ruse, e cila ka zhvilluar mjete për të ndikuar në shoqërinë

civile nëpërmjet organizatave të sponsorizuara nga shteti që synojnë t'i promovojnë idetë dhe kulturën ruse. Ndikime të tilla synojnë të krijojnë grup kritik të njerëzve që mund të përdoren për t'i rezistuar vlerave të vendosura demokratike dhe për të demonstruar kundër qeverisë, në moment të caktuar. Prandaj, aftësia e Republikës së Maqedonisë së Veriut për të identifikuar, parandaluar dhe neutralizuar ideologji të tilla të imponuara nga palët e treta duhet të jetë aftësi kyçe në trajtimin e kërcënimeve hibride.

Një element i rëndësishëm i kërcënimit hibrid është përdorimi i instrumenteve ekonomike të pushtetit. Instrumentet ekonomike përfshijnë investimet e huaja të drejtpërdrejta, kreditë me interes të ulët, financimin e ngjarjeve kulturore, financimin e partive politike si dhe financimin e stacioneve radiotelevizive dhe rrjeteve energjetike. Korrupsioni është gjithashtu instrument ekonomik i kërcënimit hibrid. Korrupsioni lejon qasje të drejtpërdrejtë në informacione të ndjeshme për të gjeneruar materiale komprometuese dhe për të minuar autoritetin e udhëheqjes politike si dhe për të frikësuar kritikët e sulmuesit. Në të njëjtën kohë, korrupsioni mundëson financimin e partive politike dhe grupeve të pakënaqura që mund të përdoren për të arritur qëllimet e sulmuesit. Kjo tregon se Republika e Maqedonisë së Veriut duhet të ketë mekanizma për kontrollin e financimit të partive politike dhe mediave, kontrollin e investimeve të huaja të drejtpërdrejta si dhe luftë efektive kundër korrupsionit, të mbështetur me rregullore përkatëse. Posedimi i këtyre mekanizmave do të zvogëlojë rrezikun nga kërcënimet hibride, veçanërisht në sektorin ekonomik.

Një nga metodat që mund të përdoret për të ndikuar në ekonomi, sektorin informativ si dhe në sektorë të tjerë kyç të një shteti, është keqpërdorimi i hapësirës kibernetike nga faktorë joshtetërorë dhe mbi të gjitha shtetërorë. Sulmet kibernetike kundër sektorëve bankarë, të energjisë dhe të transportit të Ukrainës në vitin 2017 treguan se siguria kibernetike është kritike për stabilitetin e vendit. Prandaj, rritja e sigurisë kibernetike të institucioneve shtetërore dhe mbrojtja e infrastrukturës kritike janë synimet kryesore të Republikës së Maqedonisë së Veriut.

Kërcënimi hibrid ka mundësi të mëdha për veprim, mbi të gjitha në sektorin informativ. Ndoshta metoda më e dukshme e kërcënimit hibrid është përdorimi i instrumenteve në sektorin informativ. Operacionet informative mund të përdoren për të sulmuar drejtpërdrejt qeverinë, për të formuar opinion publik dhe për të ndikuar në vullnetin për të rezistuar. Këto operacione janë të fokusuara në mënyrë specifike në elitën politike dhe sektorin civil dhe janë të sinkronizuara me aktivitetet politike, ekonomike, ushtarake dhe diplomatike të subjektit që krijon kërcënimin hibrid. Operacionet informative përfshijnë përdorimin e mediave, "bot" dhe "troll" në rrjetet sociale, por edhe metoda duke përhapur teori të rreme shkencore, paradigma, koncepte dhe strategji që ndikojnë në administratën shtetërore, në drejtim të reduktimit të potencialit për mbrojtje nacionale. Lajmet e rreme përkatësisht neglizhenca e vetëdijshme e fakteve apo "rrotullimi" i tyre, përzierja e së vërtetës me gënjeshtër, krijojnë situatë të përshtatshme për veprimtari informative armiqësore. Ballafaqimi me operacione të tilla informative kërkon ndërgjegjësim të lartë qytetar dhe aftësi për të krijuar opinion kritik, i cili do ta rriste rezistencën ndaj instrumenteve informative të operacioneve hibride. Për menaxhimin me operacionet informative, Republika e Maqedonisë së Veriut duhet të ketë potencialin dhe kapacitetet për të zbuluar burimet armiqësore të propagandës, dezinformimit dhe lajmeve të rreme, në mënyrë që t'i neutralizojë efektet e tyre negative.

Duke kuptuar ndërlíkueshmërinë e kërcënimeve hibride si dhe nevojën për përshtatje dhe uljen e shkallës së rrezikut, Republika e Maqedonisë së Veriut duhet të rrisë aftësinë dhe kapacitetet për t'iu përgjigjur të njëjtave.

2.3. Baza për ndërtimin e rezistencës dhe menaxhimit me kërcënimet hibride në Republikën e Maqedonisë së Veriut

Në vitin 2019, në bashkëpunim me Shërbimin europian të veprimit të jashtëm (EEAS ¹), filloi proces për të hetuar rrezikun e Republikës së Maqedonisë së Veriut ndaj kërcënimeve hibride, në pajtim me Kornizën e përbashkët të BE-së për ballafaqimin me kërcënimet hibride nga viti 2016.² Qeveria e Republikës së Maqedonisë së Veriut krijoi grup pune për ndërtimin e rezistencës nga kërcënimet dhe rreziqet hibride, i cili kreu hulumtime për të përcaktuar aftësinë dhe kapacitetet në nivel nacional për zbulimin e kërcënimeve hibride, rezistencën ndaj tyre dhe aftësinë për t'u përballur me pasojat. Sipas rezultateve të hulumtimit nacional, BE-ja ka dorëzuar rekomandime për përmirësimin e rezistencës ndaj kërcënimeve hibride në Republikën e Maqedonisë së Veriut, të cilat janë pranuar nga Qeveria e Republikës së Maqedonisë së Veriut. Hapi i parë për zbatimin e tyre është zhvillimi i një strategjie për ndërtimin e rezistencës nacionale dhe menaxhimit të kërcënimeve hibride.

Në vitin 2020, BE-ja miratoi strategji të re për siguri të Bashkimit (EU Security Union Strategy) për periudhën nga 2020 deri në 2025, e cila ofron udhëzime për përforsimin e sigurisë duke parandaluar dhe zbuluar kërcënimet hibride. Në të njëjtën kohë, Strategjia e BE-së përshkruan mjetet dhe masat për arritjen e këtij qëllimi. Qasja gjithëpërfshirëse e BE-së për trajtimin e kërcënimeve hibride si dhe bashkëpunimi i krijuar BE-NATO në fushën e kërcënimeve hibride³, mbrojtjes kibernetike dhe ngritjes së kapaciteteve, janë marrë gjithashtu parasysh gjatë zhvillimit të kësaj strategjie nacionale.

Brenda NATO-s, në vitin 2016, u përcaktuan udhëzimet për ndërtimin e rezistencës si dhe kriteret e vlerësimit, për të mbështetur shtatë nevojat/kërkesat bazë për ndërtimin e rezistencës nacionale. Si rezultat i mësimet të nxjerra nga përballja me pandeminë COVID-19, në vitin 2020 ministrat e mbrojtjes të NATO-s miratuan dokument të rishikuar që i përfshinte të njëjtat. Në të njëjtën kohë, dokumenti i rishikuar merr parasysh ndikimin e mundshëm të teknologjive të reja, si 5G si dhe investimet e huaja të drejtpërdrejta. Kjo kornizë është bazë për zhvillimin e kësaj strategjie. Vërtetim se ballafaqimi me kërcënimet hibride është i lartë në agjendën e sigurisë së Aleancës është fakti se, në pajtim me Deklaratën e Samitit të Varshavës (2016), në rast të ndonjë kërcënimi hibrid ndaj një shteti anëtar, NATO mund të kërkojë aktivizimin e nenit 5 nga Marrëveshja e Uashingtonit. Prandaj, shtetet-anëtare të NATO-s duhet të ndërtojnë kapacitete për rezistencë ndaj kërcënimeve hibride si pjesë e angazhimit të tyre të mbrojtjes kolektive. Rezistenca është element themelor i konceptit të NATO-s për parandalim dhe mbrojtje.

Aktivitetet dhe mësimet e nxjerra të BE-së dhe NATO-s ofrojnë bazë për krijimin e një kornize për avancimin e rezistencës së kërcënimeve hibride në nivel nacional. Republika e Maqedonisë së Veriut është në pozitë t'i përdorë mësimet e nxjerra, të bashkëpunojë dhe të kontribuojë në të gjitha aktivitetet relevante të BE-së dhe NATO-s në lidhje me kërcënimet hibride, siç janë komunikimet strategjike, inteligjenca, siguria kibernetike, mbrojtja HBRN, mbrojtja e proceseve zgjedhore dhe kërkimet akademike, nëpërmjet bashkëpunimit me strukturat e sigurisë dhe mbrojtjes të të dyja organizatave. Përveç kësaj, Republika e Maqedonisë së Veriut do t'i përdorë edhe kapacitetet e trajnimit siç është Qendra e situatave të jashtëzakonshme e NATO-s për mbrojtje kibernetike⁴, Qendra e situatave të jashtëzakonshme e BE-së për kërcënimet hibride⁵, Qendra e situatave të jashtëzakonshme e NATO-s për komunikime strategjike⁶, kurse do të bashkëpunojë edhe me ekspertët të NATO-s për mbështetje në luftën kundër kërcënimeve hibride.

¹ European External Action Service

² Joint Framework on countering hybrid threats

³ EU-NATO Joint Declaration (2016 and 2018)

⁴ NATO Cooperative Cyber Defence Centre of Excellence

⁵ European Centre of Excellence for Countering Hybrid Threats

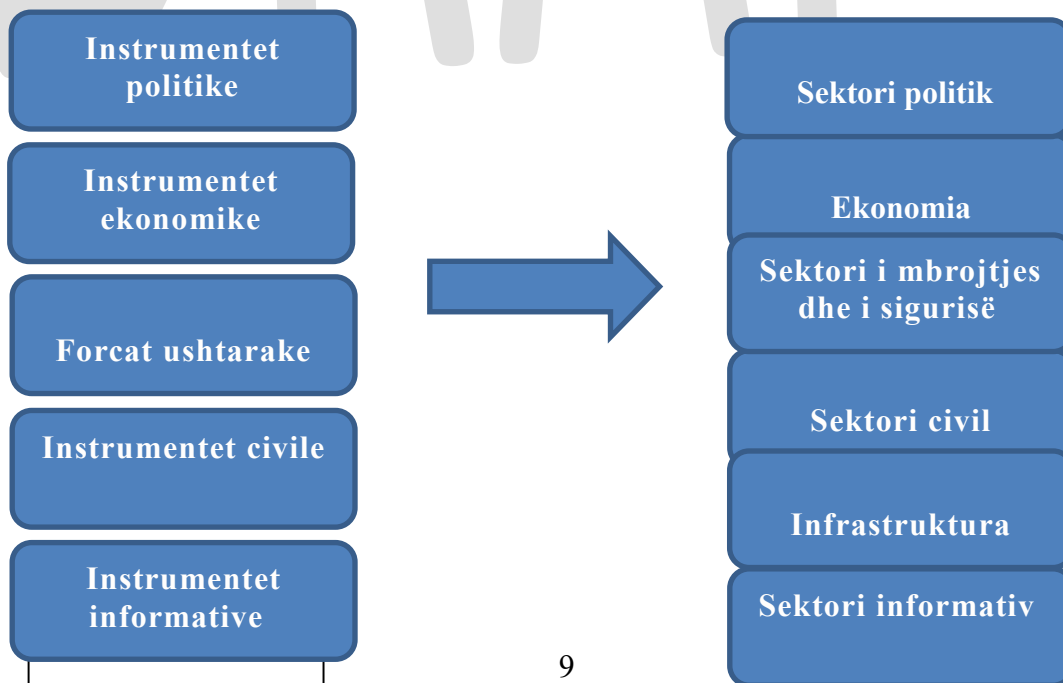
⁶ NATO STRATCOM Centre of Excellence

3. Qëllimet dhe efektet që duhet të arrihen

3.1. Qëllimet e strategjisë

Qëllimi i kësaj strategjie është krijimi i rezistencës nacionale si dhe përballja në mënyrë efikase dhe efektive me kërcënimet hibride. Për të arritur këtë qëllim, Strategjia synon të krijojë aftësi për të zbuluar dhe reduktuar rrezikun nga kërcënimet hibride, ndërkohë që duhet ta rrisë aftësinë për t'u përgjigjur, në pajtim me kornizën e vendosur nga NATO-ja dhe BE-ja. Aktivitetet e shtetit do të ndahen në gjashtë fusha të aktiviteteve operative.

3.2 Fushat operative



3.3 Qëllimet e fushave operative

Fusha e parë e veprimtarisë operative është në sferën e politikës. Një efekt kyç që duhet të arrihet në këtë fushë është vazhdimësia e pushtetit. Për këtë qëllim do të ndërtohet sistem për paralajmërimin dhe njoftimin e hershëm të kërcënimeve të mundshme si dhe identifikimin dhe përgatitjen e personelit kyç. Gjithashtu, do të sigurohet sistem efikas i menaxhimit të krizave në mbështetje të aktiviteteve të qeverisë në kohë krize, me kapacitete rezervë për funksionim të pavarur për një periudhë njëmuajore si dhe lidhje të sigurta komunikimi.

Gjithashtu, brenda kësaj zone, procesi zgjedhor do të mbrohet nga kërcënimet hibride, aktivitetet armiqësore kibernetike, operacionet informative të kryera nga subjekte të tjera shtetërore dhe joshtetërore si dhe financimi i partive politike, politikanëve dhe organizatave joqeveritare nga faktorë të jashtëm armiqësor. Për ta arritur këtë qëllim, bartësit nacional do t'i përdorin mësimet e nxjerra dhe ekspertizën nga NATO-ja dhe BE-ja.

Fusha e dytë e aktiviteteve operative është zhvillimi i ekonomisë dhe klima e favorshme e biznesit. Efekti që duhet të arrihet në këtë fushë është krijimi i një mekanizmi funksional për përballimin e rreziqeve që lidhen me investimet e huaja të drejtpërdrejta. Krijimi i kushteve për zhvillimin e ekonomisë vendore duhet gjithashtu të arrijë pavarësi të konsiderueshme tregtare dhe energjetike. Krijimi i kushteve për ekonomi digjitale do të mundësojë konkurrencën e kompanive vendore në tregjet botërore, veçanërisht në tregun e BE-së si dhe krijimin e vendeve të reja të punës dhe transformimin e tyre të shpejtë në ndryshimet e tregut. Aktiviteti thelbësor në këtë fushë është lufta kundër korrupsionit.

Fusha e tretë e aktiviteteve operative janë forcat dhe institucionet ushtarake dhe të sigurisë përkatësisht sektori i mbrojtjes dhe sigurisë. Në këtë fushë është thelbësore krijimi i aftësive të forcave ushtarake dhe të sigurisë dhe kapaciteteve për menaxhim dhe mbështetje në kushte krize, me synim rritjen e rezistencës së shoqërisë për t'u përballur me kërcënimet hibride. Fakti që përdorimi i forcave të armatosura konvencionale minimizohet gjatë kërcënimit hibrid, tregon nevojën për përmirësim të vazhdueshëm të mekanizmave të mbrojtjes dhe sigurisë. Në këtë drejtim, është e nevojshme të arrihet aftësi e lartë për t'u përballur me sulme të shumta të njëkohshme ndaj qëllimeve civile dhe ushtarake, aftësia për të krijuar mekanizëm efikas për sigurinë e burimeve të ushqimit dhe të ujit, për t'u përballur me lëvizjen e pakontrolluar të një numri të konsiderueshëm të njerëzve dhe për t'u përballur me incidente që kanë rezultuar me numër të madh të viktimave. Gjithashtu, subjektet e inteligjencës në Republikën e Maqedonisë së Veriut duhet të kenë bashkëpunim dhe koordinim të vazhdueshëm të ndërsjellë me institucionet e inteligjencës të BE-së dhe NATO-s, përgjegjëse për vlerësimin e kërcënimeve hibride.

Siguria gjatë kërcënimeve hibride përfshin gjithashtu sigurinë e shëndetit publik, e cila mund të kërcënohet nëpërmjet sëmundjeve ngjitëse ose kontaminimit të ushqimit, tokës, ajrit dhe ujit me agjentë kimikë, biologjikë, radiologjikë dhe bërthamorë. Përhapja e qëllimshme e sëmundjeve epidemiologjike mund të kërcënojë në mënyrë të konsiderueshme sigurinë e ushqimit dhe të ketë efekte negative të gjera ekonomike. Për t'u përballur me kërcënime të tilla, anëtarët e BE-së janë të lidhur nëpërmjet sistemit të paralajmërimit dhe reagimit të hershëm⁷. Për më tepër, në fushën e sigurisë së ushqimit, anëtarët e BE-së shkëmbejnë informacione dhe analiza nëpërmjet sistemit të lajmërimit të emergjencave për ushqimin dhe ushqimin e kafshëve⁸ dhe sistemin e përbashkët të menaxhimit të rrezikut të doganave⁹. Rrjedhimisht, Republika e Maqedonisë së Veriut do t'i

⁷ Early Warning and Response System

⁸ Rapid Alert System for Food and Feed

⁹ Common Risk Management System for customs

zhvillojë aftësitë nacionale për të mbrojtur shëndetin publik nga kërcënimet hibride dhe do të krijojë bashkëpunim efektiv me institucionet e BE-së në këtë fushë.

Fusha e katërt e aktiviteteve operative është shoqëria civile. Në fakt, lufta hibride është krijuar për të arritur ndarje sociale dhe për të shkaktuar trazira për të përmbysur qeverinë, kryesisht nëpërmjet dezinformimit dhe operacioneve psikologjike. Prandaj, është e nevojshme të krijohet aftësia për vetëdije kritike dhe njohuri mediatike tek qytetarët e Republikës së Maqedonisë së Veriut. Një kusht tjetër që duhet të arrihet në sektorin civil është arritja e nivelit të lartë të tolerancës ndëretnike dhe ndërftare.

Fusha e pestë e aktiviteteve operative është sektori informativ. Efekt kyç i nevojshëm për t'i përballuar kërcënimet hibride në këtë sektor është krijimi i aftësisë për ta zbuluar dezinformimin dhe operacionet psikologjike si dhe aftësia për t'u përballur me "troll-et" e internetit dhe përdorimin e inteligjencës artificiale në procesin e përhapjes së lajmeve të rreme dhe dezinformative. Një nga efektet që duhet të arrihet është krijimi i një sistemi të përhershëm dhe efektiv për komunikim strategjik, i menaxhuar drejtpërdrejt nga Qeveria e Republikës së Maqedonisë së Veriut, në bashkëpunim me institucionet tjera relevante shtetërore. Gjithashtu, duhet të arrihet gjendje në të cilën shërbimi i radio-difuzionit publik do të zbatojë aktivitete planifikuese për t'u ballafaquar me lajmet e rreme dhe dezinformatat. Në të njëjtën kohë, shteti do t'i mbështesë shoqatat e qytetarëve që janë aktive në trajtimin e dezinformative.

Fusha e gjashtë e aktiviteteve operative është mbrojtja e infrastrukturës kritike të Republikës së Maqedonisë së Veriut. Efekti i parë që duhet të arrihet është miratimi i zgjidhjes ligjore që do ta përcaktojë infrastrukturën kritike si dhe miratimi i rregulloreve për mbrojtjen e saj. Në këtë kontekst, rregulloret e BE-së dhe NATO-s do të jenë kornizë për aktivitetet e ardhshme të Republikës së Maqedonisë së Veriut në përcaktimin dhe sigurimin e infrastrukturës kritike.

Një tjetër element thelbësor për trajtimin e kërcënimeve hibride, që lidhen me infrastrukturën kritike, është diversifikimi i burimeve të energjisë dhe furnizuesve. Për të arritur këtë, është e nevojshme të kemi infrastrukturë që do të mundësojë nivel të lartë të pavarësisë energjetike të Republikës së Maqedonisë së Veriut nga furnizuesit individualë të jashtëm të energjisë. I njëjti koncept i shmangies së varësisë duhet të përdoret në lidhje me infrastrukturën e bazuar në teknologjitë e reja si celulari, interneti dhe komunikimi satelitor. Republika e Maqedonisë së Veriut, në drejtim të përcaktimit të infrastrukturës kritike dhe planifikimit të sigurisë së saj, do ta ketë parasysh zhvillimin teknologjik dhe ndikimin e teknologjive të reja të larta.

Republika e Maqedonisë së Veriut duhet të krijojë infrastrukturë të sigurt të trafikut, burime të besueshme të energjisë dhe transport, rrjet telekomunikues, sistem të qëndrueshëm shëndetësor dhe social, media të pavarura dhe sistem ekonomik-financiar, si pjesë themelore e infrastrukturës kritike sepse ndërlikueshmëria e kërcënimeve hibride kërkon përfshirjen e plotë të gjithë faktorëve institucionalë në sistemin e sigurisë nacionale.

Qëllimi: Krijimi i rezistencës nacionale si dhe trajtimi efikas dhe efektiv i kërcënimeve hibride	
Fusha e veprimtarive operative	Qëllimet që duhet të arrihen
1. Politika	<p>1.1 Vazhdimësia e Qeverisë dhe shërbimeve kritike të saj</p> <p>Miratimi i plani të formalizuar për punë të vazhdueshme dhe të koordinuar të Qeverisë ku rregullohen :</p> <ul style="list-style-type: none"> - transferimi i autoritetit dhe procesi i qartë i vendimmarrjes në rast krize, - përzgjedhja dhe prioretizimi i agjencive kritike qeveritare, shërbimeve thelbësore dhe funksioneve të obligueshme në mbështetje të aktiviteteve ushtarake, si sigurimi dhe shpërndarja e ushqimit, ujit, karburantit, energjisë elektrike, ngrohjes, transportit, mjeteve dhe pajisjeve speciale për mbrojtje mjekësore/farmaceutike/personale, - përzgjedhja dhe trajnimi i personelit kryesor civil (nga qeveria dhe ofruesit e shërbimeve kritike) dhe personelit ushtarak përkatës, - testimi periodik i sistemeve për teknologjitë e komunikimit dhe informacionit, strehimoret dhe rezervat si dhe inspektimi i kontratave të furnizimit nga subjektet private.
	<p>1.2 Struktura nacionale për menaxhimin e krizave në mbështetje të aktiviteteve të qeverisë në kohë krize, me kapacitete të lira për funksionim të pavarur për periudhë një mujore, si gjeneratorë për energji elektrike, ushqim, ujë, komunikim, mbrojtje kolektive HBRN, etj.</p>
	1.3 Procesi i mbrojtur zgjedhor

2. Ekonomia ¹⁰	2.1 Kontrolli i investimeve të huaja të drejtpërdrejta në pajtim me mësimet e nxjerra dhe praktikat në BE
3. Forcat dhe kapacitetet ushtarake dhe të sigurisë	3.1 Aftësia për të luftuar kundër forcave të armatosura të parregullta
	3.2 Aftësia për mbrojtje kibernetike kundër sulmeve komplekse kibernetike
	3.3 Aftësia për të trajtuar njëkohësisht disa incidente që përfshijnë përdorimin e armëve bërthamore, kimike, biologjike dhe radiologjike (HBRN)
	3.4 Vendosja e bashkëpunimit me institucionet e BE-së dhe NATO-s, me qëllim përballimin e kërcënimeve hibride
	3.5 Ballafaqimi me lëvizjen e pakontrolluar të njerëzve <ul style="list-style-type: none"> - janë miratuar plane nacionale për trajtimin e lëvizjes së shpejtë dhe masive të njerëzve, që mbulon mbi 2% të popullsisë së vendit, - është miratuar plan dhe trajnim (nëpërmjet simulimit) për trajtimin e lëvizjes së civilëve përgjatë një rruge të transportit në të cilën lëvizin forcat ushtarake (nënkupton ekzistencën e një mekanizmi për prioritetizimin e lëvizjes dhe mbështetjen e civilëve).
	3.6 Aftësia për ballafaqimin me viktima masive <ul style="list-style-type: none"> - krijim të sistemit të integruar për paralajmërim dhe njoftim që do të marrë informacione përkatëse nga NATO-ja dhe BE-ja, me qëllim që të paralajmërojë popullatën dhe t'i alarmojë ofruesit e shërbimeve nacionale, operatorët e infrastrukturës kritike, - krijimin e bazës së të dhënave gjithëpërfshirëse të mjeteve mjekësore ushtarake dhe civile, kapacitetin e akomodimit të pacientëve, mjetet e mbrojtjes kolektive, mjetet e transportit të viktimave dhe aftësitë e evakuimit, - miratimin e planit civil-ushtarak për situata emergjente që përfshin shërbimet përkatëse të emergjencës, mekanizmat për rritje të aftësive si dhe për mbajtjen e rregullt të ushtrimeve; - plan nacional gjithëpërfshirës sigurie të kundërmasave mjekësore ku merren parasysh dobësitë dhe sfidat e zinxhirit të furnizimit.
	3.7 Rezistencë të burimeve të ushqimit dhe ujit <ul style="list-style-type: none"> - sistem i vendosur për monitorimin, zbulimin, testimin dhe raportimin e kontaminimit të burimeve dhe infrastrukturës kryesore për furnizimin me ushqim dhe ujë, - është miratuar plan gjithëpërfshirës që rregullon furnizimin nëpërmjet burimeve alternative për ushqim dhe ujë, - është miratuar plan gjithëpërfshirës që identifikon funksionet kryesore, fuqinë punëtore, ekspertët, materialet kryesore, kontratat, bashkëpunimin e kërkuar

¹⁰ Strategjia nënkupton përbushjen e Strategjisë nacionale për parandalimin e korrupsionit dhe konfliktit të interesit 2021-2025

	ndër-sektorial dhe merr parasysh investimet/pronësinë/kontrollin e huaj të drejtpërdrejtë të nyjave dhe burimeve kryesore, në mënyrë që të sigurohet furnizim i vazhdueshëm me ushqim dhe ujë.
4. Shoqëria civile	4.1 Arritje të nivelit të lartë të edukimit mediatik dhe aftësisë për mendim kritik në sektorin civil .
	4.2 Arritja e nivelit të lartë të tolerancës në baza fetare, sociale dhe etnike .
5. Sektori informativ	5.1 Krijim të sistemit për komunikim strategjik, i udhëhequr dhe i koordinuar nga Qeveria e Republikës së Maqedonisë së Veriut .
	5.2 OJQ e pavarur dhe shërbim të radio-difuzionit publik për luftë efektive kundër lajmeve të rreme dhe dezinformatave .
6. Infrastruktura	6.1 Sigurim të sistemit rezistues për transport civil <ul style="list-style-type: none"> - infrastruktura e transportit civil, rezistuese dhe e aftë për t'u përballur me dëmtimet dhe rreziqet nga kërcënimet natyrore, kërcënimet hibride, sulmet kibernetike, epidemitë/pandemitë, pasojat e pronësisë së huaj mbi të njëjtat si dhe nga rreziku që lidhet me teknologjitë e reja, - ndërtimi i infrastrukturës së trafikut, financiar dhe energjetik që mundëson vazhdimësinë e zinxhirit të furnizimit të mallrave, burimeve financiare dhe përçimit të energjisë si dhe komunikim dhe navigacion të vazhdueshëm.
	6.2 Miratohen rregulloret, politikat dhe mekanizmat ligjore për: <ul style="list-style-type: none"> - identifikimin, organizimin, prioritetimin dhe sigurimin e burimeve të transportit, infrastrukturës, shërbimeve dhe rrugëve të transportit për të mbështetur prioritetet nacionale gjatë krizës, - mundësimin e kalimit përtej kufirit shtetëror për të mbështetur lirinë e lëvizjes së forcave të NATO-s, nëpërmjet një pike të vetme nacionale të kontaktit, mbështetur nga ministrinë përkatëse, - rregullimin e sigurimit ushtarak ose metodave alternative për të mbështetur subjektet e transportit, brenda 48 orëve nga hyrja e forcave të NATO-s në zonën e operacioneve, për të rregulluar trafikun ajror në zonat ku sigurimi komercial nuk është i arritshëm.
	6.3 Sistemet e teknologjisë informative që janë rezistuese, të shkathta dhe të afta për t'i kryer funksionet kryesore me ndërprerje minimale që përfshijnë : <ul style="list-style-type: none"> - - pasqyrë të hollësishme të infrastrukturës kritike të transportit, me prioritet - - sistem rezervë, nëse ka pengesa në funksionimin e sistemit bazë, - - mekanizëm për njoftimin e NATO-s brenda dy orëve nga ndonjë sulm në sistemin e transportit dhe këshillim për ndikim në operacionet e NATO-s, - - komunikim të sigurt ndërmjet autoriteteve dhe vendimmarrësve në lidhje me operatorët e infrastrukturës kritike.
	6.4 Rezistencë në sistemin e furnizimit me energji : <ul style="list-style-type: none"> - qasje të vazhdueshme në burime/furnizues të besueshëm të energjisë në kohë krize si dhe pavarësi energjetike,

	<ul style="list-style-type: none"> - ndërtimi i opsioneve dhe kapaciteteve rezervë në rast të ndërprerjes së furnizimit me energji, - posedim të mjeteve për t'i identifikuar nyjat dhe ndërvarësitë e energjisë (ndërlidhës ndërkufitar, ndërsektorial dhe sektorial), duke përfshirë kontratat me operatorë privatë që ndërmjetësojnë në trajtimin e rreziqeve që lidhen me investimet/pronësinë/kontrollin e huaj të drejtpërdrejtë; - zbatim të procedurave për ndarjen e informacioneve dhe ndërgjegjësimin për informim në kohë dhe efektiv për të gjithë palët e interesuara që marrin pjesë në mbrojtjen kolektive.
	<p>6.5 Sistem rezistues i komunikimit civil:</p> <ul style="list-style-type: none"> - - qasje e siguruar e vazhdueshme në shërbime të sigurta dhe gjithëpërfshirëse të komunikimit në kohë paqe, krize dhe lufte, duke marrë parasysh rreziqet e mundshme që dalin nga individët, kërcënimet kibernetike, kërcënimet hibride dhe fatkeqësitë natyrore, dobësitë që dalin nga pronësia e huaj e sistemeve të komunikimit si dhe dobësitë që lidhen me teknologjitë e reja dhe të ardhshme, - - sigurohen mundësi të gjera alternative për vendosjen e komunikimeve në të gjitha kushtet, - - marrëveshje të siguruara ndërmjet autoriteteve nacionale dhe rrjeteve të komunikimit civil për qasje me prioritet në rast të situatave të krizës, duke përdorur teknologjitë ekzistuese dhe të reja, - - sistem për shkëmbimin efektiv dhe në kohë të informacioneve në nivel nacionale dhe ndërkombëtar, me qëllim të menaxhimit të rreziqeve në sistemin e komunikimit.



4. Mënyrat për arritjen e efekteve dhe realizimit të qëllimit

Qëllimi i Strategjisë do të arrihet duke përdorur tre metodat e mëposhtme: zbulim, refuzim dhe përgjigje. Qëllimi parësor i Republikës së Maqedonisë së Veriut është parandalimi i kërcënimeve.

4.1 Detektimi i kërcënimit

Një pikë kyçe në trajtimin e kërcënimeve hibride është zbulimi. Si mënyrë për menaxhimin me kërcënimet hibride, zbulimi përfshin aftësinë për të marrë informacione përkatëse dhe në kohë në lidhje me qëllimet e mundshme të sulmuesit nga të gjitha fushat dhe bartësit.

Për shkak të natyrës komplekse të kërcënimeve hibride, palët e interesuara në të gjitha fushat duhet të zhvillojnë metoda të zbulimit të hershëm. Në këtë kuptim, rëndësi të veçantë kanë subjektet e sigurisë dhe zbulimit, mbi të gjitha Këshilli koordinues nacional i komunitetit të inteligjencës dhe sigurisë. Metoda që do të përdoret për të zbuluar me sukses kërcënimet hibride përfshin identifikimin e dobësive kritike nacionale, lidhjen e dobësive me skenarët dhe supozimet e mundshme për qëllimet dhe aftësitë e sulmuesit dhe përcaktimin e treguesve për t'i lidhur dobësitë dhe masat që duhen marrë për t'i adresuar kërcënimet hibride. Institucionet që janë përgjegjëse kryesore për zbulimin e kërcënimeve hibride janë shërbimet e inteligjencës dhe sigurisë së Republikës së Maqedonisë së Veriut dhe ato janë të obliguara të zhvillojnë metodë efikase për mbledhjen e informacioneve përkatëse dhe në kohë dhe zbulimin e kërcënimeve hibride. Për të praktikuar këtë metodë është e nevojshme të përdoret ekspertizë dhe informacione nga të gjitha subjektet e Qeverisë, bartës të fushave individuale. Krijimi dhe zhvillimi i aftësisë së zbulimit është aktivitet me prioritet sepse pa zbulimin e kërcënimit nuk është e mundur të planifikohet përgjigje për ta luftuar atë në mënyrë efektive.

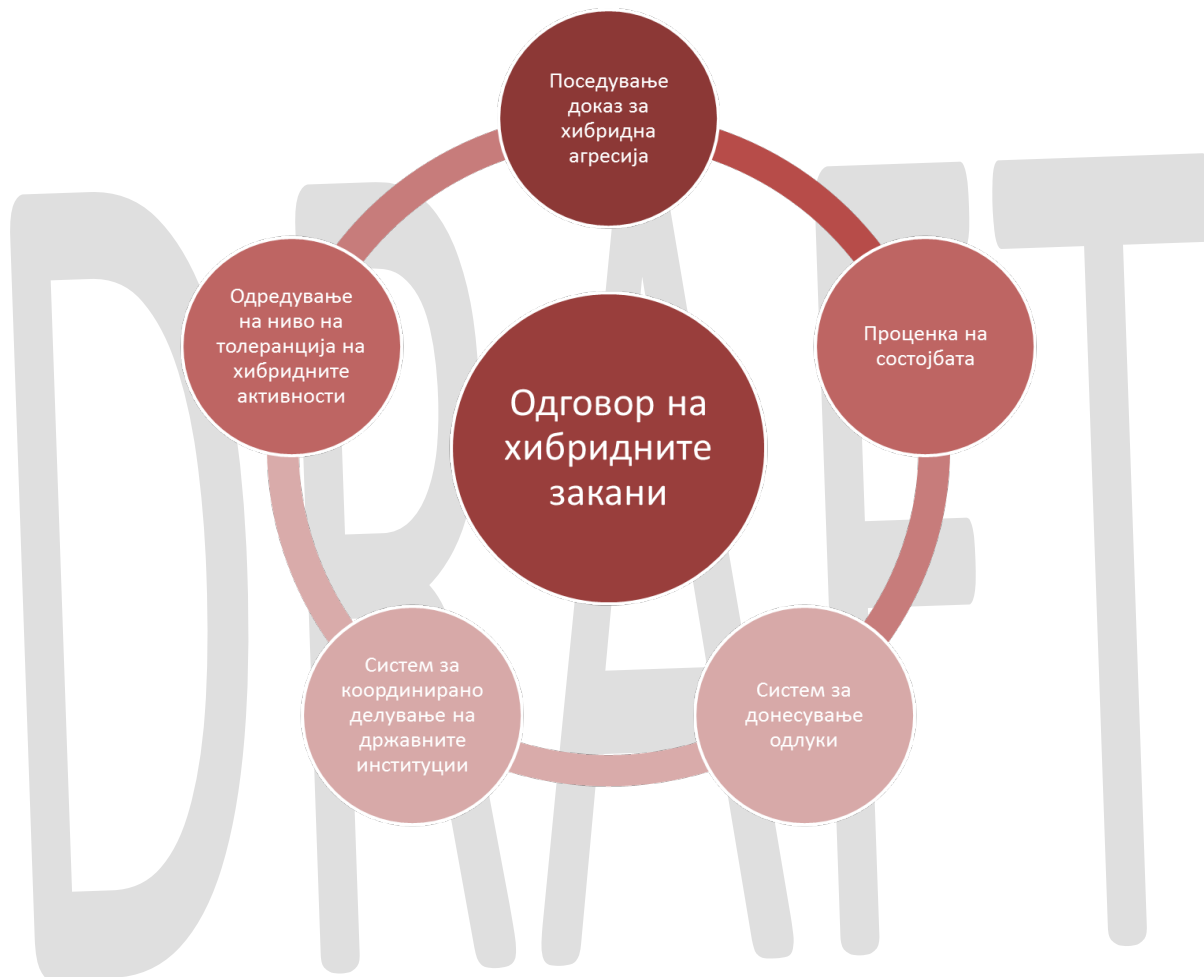
4.2 Refuzimi i kërcënimit

Aftësia e refuzimit të kërcënimit është metodë që synon ndërtimin e rezistencës, ndërtimin e kapaciteteve për ta përballuar stresin dhe aftësinë për ta tejkaluar dëmin e shkaktuar nga kërcënimet si dhe aftësinë për të luftuar kundër sulmuesit. Rezistenca nevojitet mbi të gjitha në fushat që synohen për sulmin hibrid, si politika, ekonomia, sektori i mbrojtjes dhe i sigurisë, sektori informativ, shoqëria civile dhe infrastruktura kritike. Aftësia për t'i neutralizuar sulmet nënkupton aftësi për t'i menaxhuar efektet e sulmit nga forcat ushtarake jokonvencionale, sulmet terroriste, sulmet në procesin zgjedhor, sulmet në sektorin financiar, sulmet kibernetike, sulmet me armë HBRN, operacionet informative, shkaktim të ekstremizmit të dhunshëm dhe radikalizimit si dhe përçarjet në shoqëri. Posedimi i këtyre aftësive do ta zvogëlojë efektin negativ të sulmeve të mundshme hibride. Faktori kryesor në refuzimin e kërcënimeve hibride është aftësia për të ndëshkuar sulmuesin. Kjo do të thotë krijim i instrumenteve për shkaktimin e dëmit ndaj subjektit që përdor metoda hibride, për t'i bërë aktivitetet e tij jofitimprurëse, sepse dëmi do ta tejkalonte fitimin. Posedimi i aftësisë së këtillë do ta pengonte sulmuesin e mundshëm nga përdorimi i veprimeve hibride kundër Republikës së Maqedonisë së Veriut, pasi ato do të ishin joefektive. Për të krijuar kapacitet për refuzim, Republika e Maqedonisë së Veriut do të planifikojë dhe zbatojë masa dhe aktivitete, duke përdorur qasje të plotë qeveritare.

4.3 Përgjigje ndaj kërcënimit

Përgjigja ndaj kërcënimeve hibride do të thotë të kesh proces vendimmarrës efektiv në nivel strategjik. Këshilli për koordinimin e komunitetit të inteligjencës dhe sigurisë është organi përgjegjës për dhënien e udhëzimeve, nxjerrjen e konkluzioneve dhe propozimin e masave për t'iu përgjigjur kërcënimeve hibride, si kërcënim për sigurinë nacionale. Faktor kyç në këtë proces është vlerësimi kredibil i situatës dhe përcaktimi i nivelit të tolerancës ndaj kërcënimit, tejkalimi i të cilit do të tregonte se vendi është subjekt i sulmit duke përdorur metoda hibride. Kjo kërkon komunikim dhe bashkëpunim efektiv ndërinstitucional, koordinim të shërbimeve të inteligjencës dhe proces të shpejtë dhe efikas për marrjen e vendimeve politike. Posedimi i informacioneve të besueshme dhe në kohë për kërcënimet hibride kundër Republikës së Maqedonisë së Veriut do të ndihmojë procesin e vendimmarrjes si dhe procesin e aktivizimit të mekanizmave ndihmës së BE-së dhe sistemit të mbrojtjes kolektive të NATO-s. Në përgjigje të ndonjë sulmi hibrid, mund të përdoren mekanizma të ndryshëm, si sanksionet ekonomike kundër shteteve, kompanive dhe individëve, dëbimi i diplomatëve, operacionet informative dhe aktivitete të tjera për të neutralizuar kërcënimet hibride. Megjithatë, është thelbësore që përgjigja të modelohet në mënyrë që nuk do ta përshkallëzojë kërcënimin, por do ta detyrojë sulmuesin t'i ndalojë aktivitetet hibride për shkak të joefektivitetit të tyre, pasi dëmi që do të pësojë nga aktivitete të tilla do të

jetë më i madh se përfitimi i mundshëm.



5. Instrumentet për realizimin e qëllimit

Bartës në procesin e arritjes së synimeve të dëshiruara të përcaktuara në këtë strategji do të jenë institucionet shtetërore, të cilat do të vendosin bashkëpunim efikas me faktorët relevantë.

Ndërtimi i rezistencës ndaj kërcënimeve hibride është përgjegjësi e gjithë shoqërisë. Të gjitha institucionet shtetërore kanë rol, obligime dhe detyra në përballjen me këto kërcënime, në suazat e kompetencave të tyre. Gjithashtu, ato janë të orientuara drejt bashkëpunimit me sektorin privat dhe civil. Subjekti kyç institucional për funksionimin e shtetit në rast të përballjes me kërcënimet hibride është Qeveria, e cila do të përgatitet për veprime të vazhdueshme dhe të koordinuara, nëse vendi përballlet me kërcënime hibride.

Roli, obligimet dhe detyrat e subjekteve shtetërore shpjegohen në mënyrë të hollësishme në Planin e veprimit, që është pjesë përbërëse e kësaj strategjie.

Realizimi i synimeve të kësaj strategjie do të mbështetet financiarisht nga buxhetet e institucioneve shtetërore. Subjektet shtetërore janë të orientuara drejt vendosjes së bashkëpunimit për shfrytëzimin e mbështetjes financiare, profesionale dhe institucionale nga BE-ja, NATO-ja dhe organizata të tjera ndërkombëtare.

6. Përcaktimi i shkallës së zbatimit të strategjisë

Qëllimi i përcaktimit të shkallës së realizimit është të përcaktohet se çfarë është arritur në zbatimin e strategjisë, por edhe të identifikohen sfidat dhe nevoja për ndryshime në strategji, plotësimi i saj si dhe nevoja për ndryshime në planin shoqëruar të veprimit.

Për realizimin me sukses të strategjisë dhe zbatimin e përpiktë të Planit të veprimit, Qeveria përcakton Këshillin për koordinimin e komunitetit të sigurisë dhe inteligjencës, i cili në nivel vjetor (tremujori i parë i vitit), do t'i paraqesë Qeverisë raport për shkallën e realizimit të strategjisë dhe Planit shoqëruar të veprimit. Bartësit e

fushave përkatëse, përfshirë Sekretariatit e përgjithshëm të Qeverisë dhe autoritetet përkatëse për komunikim strategjik, janë të obliguar t'i paraqesin Këshillit për koordinimin e komunitetit të sigurisë dhe inteligjencës informacione, të cilat i referohen rolit, qëllimeve dhe detyrave në pajtim me kriteret e vlerësimit të përfshira në planin e veprimit.

6.1. Sfidat e realizimit

- arritja e konsensusit nacional midis faktorëve politikë në vend në drejtim të vendimmarrjes efikase,
- nevoja për nivel të unifikuar dhe më të lartë ndërgjegjësimi dhe mirëkuptimi të institucioneve shtetërore lidhur me rolin e tyre në ndërtimin e rezistencës ndaj kërcënimeve hibride,
- koordinimin e subjekteve institucionale,
- krijimi i një mekanizmi efektiv për kontrollin e investimeve të huaja të drejtpërdrejta,
- zbatimi i teknologjive të reja në sistemin e mbrojtjes dhe sigurisë, sa i përket ekspertizës dhe burimeve,
- ngritja e nivelit të edukimit mediatik,
- ndërtimi i besimit ndërmjet sektorit publik dhe civil,
- përcaktimi dhe mbrojtja e infrastrukturës kritike.

DRAFT