MYKOLO ROMERIO UNIVERSITETAS

VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

AURELIJUS VRUBLIAUSKAS

KIBERNETINIŲ PAJĖGŲ MODELIAVIMO YPATUMAI: NATO VALSTYBIŲ PATIRTIS IR LIETUVOS PERSPEKTYVA

Magistro baigiamasis darbas

Vadovas:

Prof. Dr. Tadas Limba

VILNIUS, 2022

MYKOLO ROMERIO UNIVERSITETAS

VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

KIBERNETINIŲ PAJĖGŲ MODELIAVIMO YPATUMAI: NATO VALSTYBIŲ PATIRTIS IR LIETUVOS PERSPEKTYVA

Kibernetinio saugumo valdymo magistro baigiamasis darbas

Studijų programa: kibernetinio saugumo valdymas (nuo 2017)

Vadovas:

_____Prof. Dr. Tadas Limba

2022 05

Recenzentas

_____

2022 05

Atliko:

_____ KSVvmis20–1 gr.stud. A.Vrubliauskas

2022 05

VILNIUS, 2022

TURINYS

LENTELĖS 4
PAVEIKSLAI 5
SANTRUMPOS IR TERMINAI 6
ĮVADAS 7
1. KIBERNETINĖS GYNYBOS TEORINIAI ASPEKTAI 9
1.1. Kibernetinė gynyba nacionalinio saugumo ir kibernetinio saugumo strategijose 9
1.1.1 Kibernetinė gynyba nacionalinio saugumo strategijoje 9
1.1.2 Kibernetinė gynyba kibernetinio saugumo strategijoje 13
1.2. Kibernetinio saugumo valdymas ir atsakomybės 17
2. KIBERNETINIŲ PAJĖGUMŲ VERTINIMO MODELIAI 24
2.1. Šalies kibernetinių pajėgumų vertinimo modelių apžvalga 24
2.2. Karinių kibernetinių pajėgumų vertinimo modelių apžvalga 28
3. NATO KARINIŲ KIBERNETINIŲ PAJĖGUMŲ VYSTYMASIS IR TENDENCIJOS 32
3.1. NATO reikalavimai karinių kibernetinės gynybos pajėgų vystymui. 32
3.2 Estijos kariniai kibernetiniai pajėgumai 36
3.3 JAV kariniai kibernetiniai pajėgumai 40
4. LIETUVOS KARIUOMENĖS KIBERNETINIŲ GYNYBOS PAJĖGŲ BRANDOS TYRIMAS 45
4.1. Tyrimo metodologija 45
4.2. Tyrimo rezultatų analizė ir interpretavimas 48
3. Nacionalinės Ypatingos Svarbos Informacinės Infrastruktūros strategijos egzistavimas 51
IŠVADOS IR SIŪLYMAI 62
LITERATŪRA 64
ANOTACIJA 68
ANNOTATION 69
SANTRAUKA 70
SUMMARY 71
PRIEDAI 72

LENTELĖS

1 lentelė. NKSS įgyvendinimo tarpinstitucinio veiklos plano 2019–2021 m. tikslai, uždaviniai, priemonės, asignavimai ir dalyvaujančios institucijos

2 lentelė. Tyrimo ekspertai

3 lentelė. Doktrinos pajėgumų srities atsakymų suvestinė

4 lentelė. Organizacijos pajėgumų srities atsakymų suvestinė

5 lentelė. Rengimo pajėgumų srities atsakymų suvestinė

6 lentelė. Sistemos ir aprūpinimo pajėgumų srities atsakymų suvestinė

7 lentelė. Personalo pajėgumų srities atsakymų suvestinė

8 lentelė. Lyderystės pajėgumų srities atsakymų suvestinė

9 lentelė. Infrastruktūros pajėgumų srities atsakymų suvestinė

10 lentelė. Sąveikumo pajėgumų srities atsakymų suvestinė

PAVEIKSLAI

1 pav. Magistro baigiamojo darbo struktūros loginė schema

2 pav. Kibernetinį saugumą užtikrinančios institucijos ir valdymo organizacija

3 pav. Kibernetinio saugumo pajėgumų modelio struktūra

4 pav. Pajėgumų sričių brandos lygių suvestinė

SANTRUMPOS IR TERMINAI

Kibernetinis saugumas – LR Kibernetinio saugumo įstatyme apibrėžiamas kaip „visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, skirtų kibernetiniams incidentams išvengti, aptikti, analizuoti ir reaguoti į juos, taip pat įprastinei elektroninių ryšių tinklų, informacinių sistemų ar pramoninių procesų valdymo sistemų veiklai, įvykus šiems incidentams, atkurti“.

Kibernetinė gynyba – veiksmai apsaugotoje kibernetinėje erdvėje skirti apginti erdvę nuo įvykusių arba gręsiančių įvykti kibernetinėje erdvėje pažeidimų, apimantys grėsmių aptikimą, klasifikavimą, užkardymą ir įvykimo tikimybės mažinimą bei veiksmai atstatantys saugų informacinių sistemų veikimą (US Joint publication 3-12, Cyberspace Operations).

Kibernetinė erdvė – LR Kibernetinio saugumo įstatyme apibrėžiamas kaip „aplinka, kurioje pavieniuose kompiuteriuose ar kitoje informacinėje ir ryšių technologijų įrangoje sukuriama elektroninė informacija ir (arba) perduodama per elektroninių ryšių tinklu sujungtus kompiuterius ar kitą informacinių ir ryšių technologijų įrangą“.

Ypatingos svarbos informacinė infrastruktūra – LR Kibernetinio saugumo įstatyme apibrėžiamas kaip „elektroninių ryšių tinklas ar jo dalis, informacinė sistema ar jos dalis, informacinių sistemų grupė ar pramoninių procesų valdymo sistema ar jos dalis, nepaisant to, ar jos valdytojas yra privatus ar viešojo administravimo subjektas, kuriuose įvykęs kibernetinis incidentas gali padaryti didelę žalą nacionaliniam saugumui, šalies ūkiui, valstybės ir visuomenės interesams“.

Ypatingos svarbos infrastruktūros objektas – LR Kibernetinio saugumo įstatyme apibrėžiamas kaip „infrastruktūros objektas, teikiantis ypatingos svarbos paslaugą. Ypatingos svarbos paslauga – paslauga, kurios neveikimas ar veikimo sutrikimas padarytų didelį neigiamą poveikį nacionaliniam saugumui, šalies ūkiui, valstybės ar visuomenės interesams“.

ĮVADAS

Temos aktualumas. Po to, kai 2016 m. NATO pripažino kibernetinę erdvę atskira operacijų sritimi (kaip ir sausumos, oro bei jūrų) bei susitarė dėl Kibernetinės Gynybos Įsipareigojimų (anglų k. *Cyber Defence Pledge*) kibernetinės gynybos stiprinimui, buvo pasiektas vienas iš svarbių tikslų – nutarta stiprinti NATO kibernetinės gynybos pajėgumus. Siekiant sustiprinti NATO vadovavimo struktūrą (anglų k. *NATO Command Structure*) 2018 m. pradėtas kurti NATO Kibernetinės erdvės operacijų centras (anglų k. *Cyberspace Operations Centre*). Kartu su šiuo kritiniu organizaciniu pakitimu, Aljansas Briuselyje vykusiame aukščiausiojo lygio suvažiavime taip pat sutarė, kaip į NATO vadovaujamas operacijas ir misijas integruoti suverenius kibernetinius pajėgumus, kuriuos savanoriškai teiks sąjungininkai.

NATO šalys partnerės vieningai sutaria, kad kibernetinės atakos padaryta žala gali būti prilyginta konvencinės atakos padarytiems nuostoliams. Dėl to kibernetinė gynyba tapo viena iš NATO kolektyvinės gynybos pagrindinių užduočių (anglų k. *Core task*), kur kibernetinė ataka gali paskatinti Vašingtono sutarties 5 straipsnio inicijavimą. Kaip ir kitose operacijų srityse, NATO veiksmai kibernetinėje gynyboje yra orientuoti į gynybą, proporcionalūs ir atitinka tarptautinės teisės reikalavimus. Siekdama užtikrinti tinkamą savo valstybių narių gynybą, NATO priėmė politiką ir veiksmų planus, įsteigė komitetus, agentūras ir operacinius centrus, siekiant integruoti kibernetinę gynybą į sąjungininkų operacijas ir pajėgumų plėtrą. Nepaisant to, neseniai pripažintas kibernetinis domenas kol kas neleidžia taikyti vieningo požiūrio į kibernetinę gynybą pagrindinėse NATO šalyse ir tai galima suskirstyti į dvi kategorijas: šalys, kurios siekia aktyvios gynybos, ir šalys, kurioms labiau patinka tik gynybinis požiūris.

Teorinis reikšmingumas. Kibernetinės gynybos stiprinimas siekiant apsisaugoti nuo besivystančių karinių kibernetinių grėsmių ir efektyvus kibernetinių incidentų valdymas yra viena iš būtinų sąlygų užtikrinant gyvybinius ir pirmaeilius valstybės nacionalinio saugumo interesus. Įgyvendinant Lietuvos kariuomenei (toliau – LK) keliamus uždavinius, bus plėtojami nacionaliniai kibernetinės gynybos pajėgumai, užtikrinantys LK sąveiką su valstybės civiliniais pajėgumais, taip pat LK gebėjimai užtikrinti patikimą agresoriaus atgrasymą kibernetinėje erdvėje, o nepavykus atgrasyti – savarankiškai ir kartu su sąjungininkais ginti Lietuvos Respubliką karinėmis kibernetinio saugumo priemonėmis.

Darbo tyrimo rezultatai gali būti pritaikyti siekiant vystyti LK kibernetinės gynybos pajėgumus.

Darbo problema. Kiekviena NATO šalis kibernetinės erdvės saugumą užtikrina skirtingais kariniais pajėgumais ir nėra vieningo nusistovėjusio organizacinio modelio, kuris tiktų visoms šalims narėms. Atsižvelgiant į tai, būtina išanalizuoti LK kibernetinės gynybos pajėgumus formuluojant mokslinę

problemą: *Ar LK kibernetinės gynybos pajėgumai pakankami siekiant užtikrinti efektyvią LK kibernetinės erdvės gynybą?*

Darbo objektas: LK kibernetinės gynybos pajėgumai.

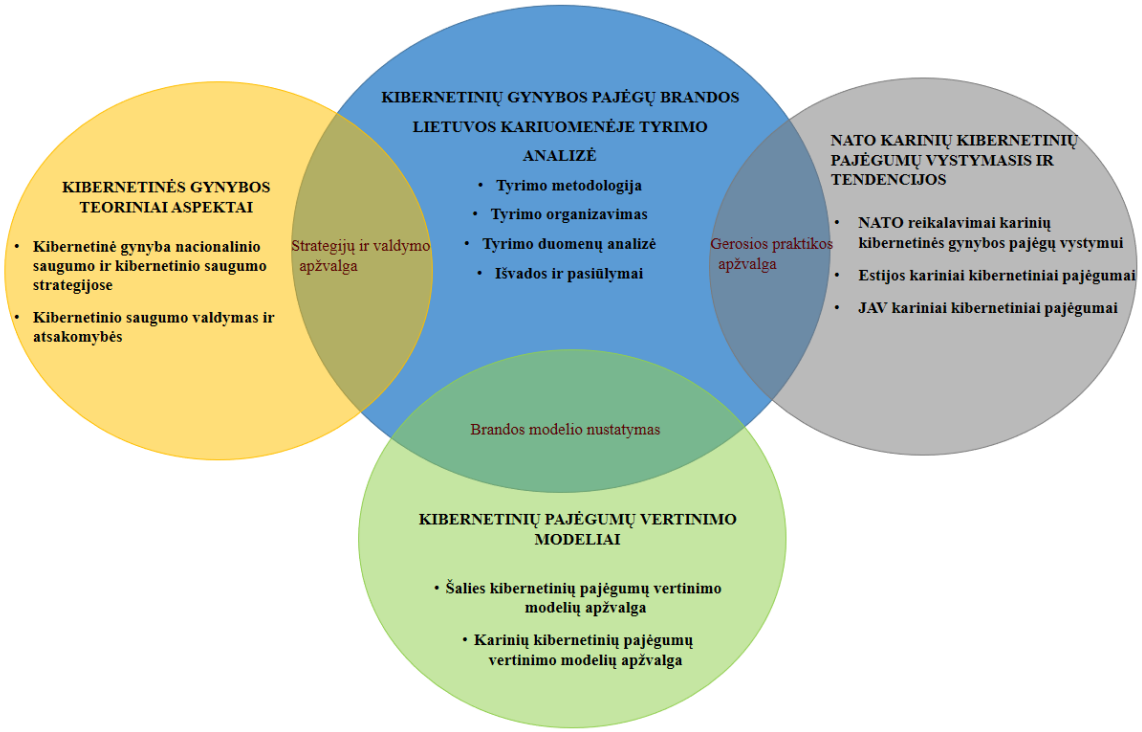
Darbo tikslas: nustatyti LK kibernetinės gynybos pajėgumų brandos lygį ir pateikti su šia sritimi susijusius pasiūlymus.

Darbo uždaviniai:

1. Ištirti kibernetinio saugumo valdymo struktūrą ir atsakomybes.
2. Ištirti kibernetinių pajėgumų vertinimo modelius.
3. Išanalizuoti NATO reikalavimus kibernetiniams pajėgumams.
4. Nustatyti LK kibernetinės gynybos pajėgumų vystymo sričių privalumus ir trūkumus.
5. Pateikti rekomendacijas LK kibernetinės gynybos pajėgumų vystymui.

Duomenų rinkimo metodai: Mokslinės literatūros sisteminimas, analizė, palyginimas, dokumentų analizė, ekspertų apklausa (kiekybinio tyrimo strategija).

Duomenų analizės metodai: kokybinė turinio (anglų k. *Content*) analizė, kiekybinė analizė ir interpretavimas bei lyginamoji gautų duomenų analizė.



1 pav. Magistro baigiamojo darbo struktūros loginė schema

1. KIBERNETINĖS GYNYBOS TEORINIAI ASPEKTAI

1.1. Kibernetinė gynyba nacionalinio saugumo ir kibernetinio saugumo strategijose

1.1.1 Kibernetinė gynyba nacionalinio saugumo strategijoje

Kodėl yra svarbu suprasti kibernetinės gynybos svarbą nacionalinio saugumo kontekste? 2014 ir 2022 metų įvykiai Ukrainoje visam pasauliui įrodė, kad net XXI amžiuje vakarietiškame pasaulyje įmanomi įvykiai, kada dalis suverenios valstybės yra žaibiškai užimta agresoriaus. Nacionalinio saugumo strategijoje aiškiai įvardijamas grėsmių kompleksiškumas, kuris „pasižymi nykstančiomis skirtimis tarp karo ir taikos, išorinių ir vidinių, karinių ir nekarinių grėsmių, valstybinių ir nevalstybinių grėsmių šaltinių“. Visa tai lemia didėjantį hibridinių grėsmių iššūkį ne tik Lietuvos Respublikai, bet ir visai euroatlantinei bendruomenei.

Lietuvos nacionalinio saugumo samprata apima nacionalinį saugumo lygmenį, orientuodamasi į tas mūsų šalies problemas, kurios yra suvokiamos kaip grėsmės tautos ir valstybės egzistencijai ir jos saugumui, t. y. šalies gynyba, ekonomika, kultūra, gamtosauga, demografija, viešoji tvarka ir t.t. (Petrauskaitė, Kazlauskaitė-Markelienė, Gedminienė, 2016).

Grėsmių, ypatingai hibridinių, sąrašą papildo ir virsmo technologijų (anglų k. *Disruptive technologies*)[1] plėtra, kurios vis dažniau pritaikomos „greitesniems, pavojingesniems ar sunkiau atpažįstamiems ir atsekamiems veiksmams prieš kitas valstybes vykdyti“. Rusijos Federacija ir Kinijos Liaudies Respublika šias technologijas pasitelkia savo galiai didinti. Skaitmeninės erdvės svarbą šių laikų saugumo aplinkos sampratoje lemia „auganti takoskyra tarp laisvos rinkos principais paremto demokratinių ir valstybės kontrole grįsto autoritarinių valstybių skaitmeninio suvereniteto“. Autoritarinės valstybės vis labiau stengiasi kontroliuoti duomenų valdymą bei asmens privatumą.

Nacionalinio saugumo kontekste išskiriama sekanti Lietuvos Respublikos teisės aktų hierarchija, reglamentuojanti kibernetinį saugumą:

a) Lietuvos Respublikos Konstitucija;

b) Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas;

c) Nacionalinio saugumo strategija;

d) Lietuvos Respublikos kibernetinio saugumo įstatymas;

e) Nacionalinė kibernetinio saugumo strategija.

Darbe nagrinėjamos kiekviename dokumente įtvirtintos kibernetinio saugumo nuostatos.

[1] Virsmo technologijos – dirbtinis intelektas, didieji duomenys, autonominės, kvantinės ir kitos technologijos.

Lietuvos Respublikos Konstitucijos 135 straipsnis nustato, kad „Lietuvos Respublika, įgyvendindama užsienio politiką, vadovaujasi visuotinai pripažintais tarptautinės teisės principais ir normomis, siekia užtikrinti šalies saugumą ir nepriklausomybę, piliečių gerovę ir pagrindines jų teises bei laisves, prisideda prie teise ir teisingumu pagrįstos tarptautinės tvarkos kūrimo. Konstitucija reglamentuoja pamatinius Lietuvos valstybės ir visuomenės gyvenimo aspektus, esminius nacionalinio saugumo klausimus – teisę priešintis ir ginti valstybę, viešąją tvarką, vadovautis visuotinai pripažintais tarptautinės teisės principais ir normomis“.

Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymo (toliau – LR nacionalinio saugumo pagrindų įstatymas) nuostatos leidžia teigti, kad Lietuvos nacionalinio saugumo samprata apima ir individualaus saugumo, ir tarptautinio saugumo lygmenis (Petrauskaitė, Kazlauskaitė-Markelienė, Gedminienė, 2016). Įstatyme yra pažymėta, kad „vienas iš pagrindinių nacionalinio saugumo objektų, yra žmogaus ir piliečio teisės, laisvės bei asmens saugumas, t. y. individualus saugumas nurodytas kaip nacionalinio saugumo prioritetas. Tarptautinis nacionalinio saugumo politikos lygmuo yra apibrėžtas Lietuvos užsienio politikos nuostatose, užtikrinančiose nacionalinį saugumą, t. y. užtikrinant šalies saugumą, tinkamai vykdant Šiaurės Atlanto sutarties organizacijos ir Europos Sąjungos narystės įsipareigojimus, aktyviai prisidedant prie tarptautinės tvarkos kūrimo ir tarptautinės bendrijos pastangų įtvirtinti demokratiją, užkertant kelią terorizmui, konfliktams, įvedant, atkuriant ir palaikant taiką krizių paveiktuose regionuose“.

LR nacionalinio saugumo pagrindų įstatyme išskiriami strategiškai svarbūs ūkio sektoriai nacionaliniam saugumui, t.y. „energetikos, transporto, informacinių technologijų ir telekomunikacijų, kitų aukštųjų technologijų, finansų ir kredito bei karinės įrangos. Siekdama užtikrinti nacionalinio saugumo interesų apsaugą, Vyriausybė teikia Seimui įstatymu tvirtinti, kurie nacionaliniam saugumui strategiškai svarbūs objektai privalo būti valstybės nuosavybė, o kuriuose ir kokiomis sąlygomis kapitalo dalį gali sudaryti privatus nacionalinis bei užsienio kapitalas, atitinkantis europinės ir transatlantinės integracijos kriterijus, paliekant sprendžiamąją galią valstybei, taip pat teikia tvirtinti kitus nacionalinio saugumo užtikrinimui svarbius objektus“. Vertinant valstybės svarbius objektus užtikrinančius nacionalinį saugumą kibernetinio saugumo kontekste, verta pažymėti, kad Lietuvos Respublikos kibernetinio saugumo įstatyme išskirta ypatingos svarbos informacinė infrastruktūra (sutr. YSII), kurios pažeidimas darytų neigiamą įtaką šalies nacionaliniam saugumui. Pagal patvirtintą YSII identifikavimo metodiką, skiriami šie ypatingos svarbos sektoriai: energetikos, transporto ir pašto, finansų, sveikatos priežiūros, geriamojo vandens tiekimo, paskirstymo ir tvarkymo, informacinių technologijų ir elektroninių ryšių, aplinkos, civilinė saugos, krašto apsaugos, maisto produktų, pramonės, užsienio reikalų ir saugumo politikos, valstybės valdymo, viešojo saugumo ir teisinės tvarkos. Šių ypatingos svarbos infrastruktūros objektų (sutr. YSIO) valdytojai privalo

skirti ypatingą dėmesį jų valdomų ryšių ir informacinių sistemų kibernetiniam saugumui, taip pat užtikrinti jų atitiktį organizaciniams ir techniniams kibernetinio saugumo reikalavimams. 2021 m. duomenimis, informacinės infrastruktūros ir jos valdytojų sąrašą sudarė 161 subjektas.

Nacionalinės saugumo strategijos naujoje (2021 m.) redakcijoje išskiriami trys nacionalinio saugumo prioritetai ir uždaviniai: valstybės gynyba, valstybės ir visuomenės atsparumas ir Lietuvos Respublikos interesus atitinkanti tarptautinė saugumo sistema. Pagrindinis valstybės ramstis gynybai užtikrinti yra kariuomenė. Strategijoje nurodyti nacionalinių karinių pajėgumų stiprinimo uždaviniai susiję su kibernetiniu saugumu:

a) plėtoti augančią kibernetinės operacinės erdvės svarbą atitinkančius kibernetinio saugumo ir gynybos pajėgumus, užtikrinti nacionalinius gebėjimus vykdyti karines operacijas kibernetinėje erdvėje;
b) įtraukti virsmo technologijų pajėgumų siekius į nacionalinį gynybos planavimą, atsižvelgiant į NATO gynybos planavimo proceso keliamus reikalavimus.

Siekiant įgyvendinti valstybės institucijų ir piliečių pasirengimo remti ginkluotos gynybos užduočių įgyvendinimą, būtina užtikrinti, kad civilinių sektorių, ypač transporto, energetikos, finansų ir kredito, informacinių technologijų ir telekomunikacijų, žemės ir maisto ūkio plėtra atitiktų pasirengimo valstybės ginkluotai gynybai poreikius, didintų ypatingos svarbos infrastruktūros atsparumą ir saugumą, garantuotų pakankamą strateginį rezervą ar reikalingus gamybos pajėgumus.

Kalbant apie valstybės ir visuomenės atsparumą kaip apie vieną iš nacionalinio saugumo prioritetų, strategijoje detalizuoti sekantys kibernetinio ir informacinio saugumo bei atsparumo stiprinimo uždaviniai:

a) plėtoti kibernetinio saugumo ir gynybos pajėgumus, siekiant užtikrinti nuolatinę nacionalinės kibernetinio saugumo ir gynybos sistemos plėtrą, efektyvų kibernetinių incidentų atpažinimą, prevenciją, užkardymą ir valdymą, vystyti veiksmingą viešojo ir privataus sektorių bendradarbiavimą šioje srityje;
b) užtikrinti, kad valstybės skaitmenizavimas, vykdant duomenų atvėrimo, skaitmeninės infrastruktūros, elektroninių paslaugų, skaitmeninio turinio ar duomenų kūrimo, plėtros ir kitas skaitmenizavimo iniciatyvas, atitiktų nacionalinio saugumo interesus;
c) sudaryti sąlygas valstybei ir visuomenei saugiai naudotis naujųjų technologijų teikiamomis galimybėmis ir užtikrinti, kad YSII bei valstybės informaciniuose ištekliuose būtų naudojama tik patikimų gamintojų įranga, o naujųjų technologijų, tokių kaip dirbtinio intelekto, daiktų interneto, 5G ir kitų, diegimas ir valstybės skaitmenizavimas būtų vykdomas laikantis aukščiausių kibernetinės saugos ir atsparumo standartų, užtikrinti nepertraukiamą YSII veikimą krizių atveju;

d) skatinti kibernetinio saugumo kultūrą per viešojo, privataus, nevyriausybinio ir mokslo sektorių bendradarbiavimą, mokslinių tyrimų ir inovacijų plėtrą, tarptautinį bendradarbiavimą bei visuomenės švietimą, kibernetinio saugumo raštingumą;
e) plėtoti valstybės institucijų gebėjimus vykdyti kryptingą kovą su dezinformacija, siekiant užtikrinti koordinuotą informacinės aplinkos stebėjimą, analizę, vertinimą ir operatyvų perspėjimą bei savalaikį reagavimą į informacinius incidentus;
f) stiprinti visuomenės atsparumą dezinformacijai ir kitoms informacinėms grėsmėms, tobulinant švietimo sistemą, plėtojant kultūros paslaugas, ugdant kritinį mąstymą ir vykdant koordinuotas žiniasklaidos, medijų ir informacinio raštingumo programas bei strateginės komunikacijos kampanijas, stiprinti viešojo, privataus ir nevyriausybinio sektorių bendradarbiavimą;
g) užtikrinti sąlygas žiniasklaidos veiklos gyvybingumui, nepriklausomumui, skaidrumui ir pliuralizmui, vykdant subalansuotą ir nuoseklią valstybės paramos bei mokesčių politiką;
h) plėtoti bendradarbiavimą NATO, ES ir daugiašaliais formatais kibernetinio saugumo ir kovos su dezinformacija srityje, siekiant ne tik stiprinti Lietuvos Respublikos ekspertizę šioje srityje, bet ir panaudoti turimas žinias bei kompetencijas kolektyvinio euroatlantinės bendruomenės saugumo labui.

Trečio nacionalinio saugumo prioriteto – Lietuvos Respublikos nacionalinių saugumo interesų užtikrinimas labai priklauso nuo tarptautinių politinių procesų. Šio prioriteto įgyvendinimui išskiriamas vienas iš Euroatlantinių saugumo struktūrų ir Europos saugumo architektūros stiprinimo uždavinių – plėtoti transatlantinį bendradarbiavimą vykdant technologijų plėtrą, kuriant ir vykdant jų normas, standartus ir teisinį reguliavimą, užkardyti nepatikimų technologijų tiekėjų, galinčių kelti grėsmę nacionalinio saugumo požiūriu svarbiuose sektoriuose, veiklą, stiprinti bendradarbiavimą atliekant virsmo technologijų tyrimus ir jas tobulinant.

Specifinė nacionalinės saugumo strategijos vieta strateginių dokumentų hierarchijoje lemia tai, jog Strategija yra įgyvendinama per planavimo dokumentus: Nacionalinį pažangos planą, ilgalaikes valstybines saugumo stiprinimo programas, plėtros programas ir nacionalines darbotvarkes.

Atskaitomybė užtikrinama LR Vyriausybei informuojant Seimą apie Strategijos nuostatų įgyvendinimą: teikiama nacionalinio saugumo būklės ir plėtros ataskaita, kuri yra sudedamoji Lietuvos Respublikos Vyriausybės (toliau – LRV) metinės veiklos ataskaitos dalis.

1.1.2 Kibernetinė gynyba kibernetinio saugumo strategijoje

Nacionalinė kibernetinio saugumo strategija (toliau – NKSS) nustato „svarbiausias nacionalinės kibernetinio saugumo politikos viešajame ir privačiame sektoriuose kryptis. Įgyvendinant NKSS siekiama stiprinti valstybės kibernetinį saugumą ir kibernetinių gynybos pajėgumų plėtrą, užtikrinti nusikalstamų veikų, kurias vykdant naudojami kibernetinę erdvę sudarantys objektai, prevenciją, užkardymą ir tyrimą, skatinti kibernetinio saugumo kultūrą ir inovacijų plėtrą, stiprinti glaudų viešojo ir privataus sektorių, tarptautinį bendradarbiavimą ir užtikrinti tarptautinių įsipareigojimų kibernetinio saugumo srityje vykdymą valstybėje iki 2023 m.“.

NKSS išskiriami šie tikslai:

a) stiprinti valstybės kibernetinį saugumą ir kibernetinių gynybos pajėgumų plėtrą;
b) užtikrinti nusikalstamų veikų kibernetinėje erdvėje prevenciją, užkardymą ir tyrimą;
c) skatinti kibernetinio saugumo kultūrą ir inovacijų plėtrą;
d) stiprinti glaudų viešojo ir privataus sektorių bendradarbiavimą;
e) stiprinti tarptautinį bendradarbiavimą ir užtikrinti tarptautinių įsipareigojimų kibernetinio saugumo srityje vykdymą.

Šio darbo kontekste nagrinėjami tik pirmojo tikslo įgyvendinimo uždaviniai:

Pirmasis tikslo uždavinys – kurti sisteminį požiūrį į kibernetinį saugumą ir prevencinę veiklą. Šis uždavinys bus įgyvendinamas tobulinant kibernetinio saugumo rizikos nustatymo, vertinimo ir prognozavimo būdus, formuojant kibernetinio saugumo atpažinties paveikslą ir rizikos žemėlapį, kuris atskleistų atskiriems sektoriams būdingas rizikas, kuriant regioninį kibernetinio saugumo centrą ir valstybės valdomą elektroninių ryšių tinklą su kompleksinėmis kibernetinio saugumo priemonėmis, jungiantį valstybines mobilizacines užduotis gyvybiškai svarbioms valstybės funkcijoms atlikti paskirtas vykdyti valstybės ir savivaldybių institucijas, įstaigas ir įmones, atliekant kibernetinio saugumo būsenos tyrimus, pažangos matavimus ar brandos vertinimus, užtikrinant visuomenės informavimą apie kibernetinio saugumo būklę, vykdant kitas kibernetinį saugumą ir prevencinę veiklą stiprinančias priemones ir veiksmus.

Antrasis tikslo uždavinys – didinti kibernetinio saugumo politikos formavimo ir įgyvendinimo efektyvumą, mažinant administracinę naštą kibernetinio saugumo subjektams. Šis uždavinys bus įgyvendinamas tobulinant kibernetinio saugumo teisinį reguliavimą, parengiant standartizuotus, bet diferencijuojamus kibernetinio saugumo reikalavimus, atliekant gerosios praktikos, standartų, taikomų užtikrinant kibernetinį saugumą, analizę, skatinant kibernetinio saugumo subjektus jais vadovautis, nustatant nacionalinį integruotą krizių valdymo mechanizmą, užtikrinant visų lygmenų struktūrų sklandų bendradarbiavimą, atnaujinant kibernetinio saugumo rizikos vertinimo sistemą, įvertinant metodines

galimybes vykdyti kibernetiniam saugumui reikalingų lėšų stebėseną ir kontrolę, nustatant jų skyrimo ir naudojimo pirmumą, vykdant kitas kibernetinio saugumo politikos formavimo ir įgyvendinimo plėtojimo priemones.

Trečiasis tikslo uždavinys – skatinti nacionalinių pratybų vykdymą ir dalyvavimą tarptautinėse pratybose. Šis uždavinys bus įgyvendinamas periodiškai rengiant kompleksines nacionalines kibernetinio saugumo pratybas, dalyvaujant Europos Sąjungos, NATO ir kitų šalių organizuojamose pratybose, integruojant nacionalinių ir tarptautinių pratybų patirtį atliekant situacijų valdymo, incidentų vertinimo, informacijos komunikavimo ar kitus veiksmus.

Ketvirtasis tikslo uždavinys – plėtoti valstybės kibernetinės gynybos pajėgumus. Šis uždavinys bus įgyvendinamas užtikrinant efektyvią Lietuvos kariuomenės sąveiką su valstybės civiliniais pajėgumais, plėtojant kibernetinės gynybos pajėgumus ir teikiant pagalbą kitoms valstybės ir savivaldybių institucijoms ir įstaigoms.

NKSS numatyta, kad siekiant įgyvendinti strategijoje numatytus tikslus ir uždavinius, „LR Vyriausybė tvirtina tarpinstitucinį veiklos planą, kuriame nustatomos strategijos įgyvendinimo priemonės ir lėšos joms įgyvendinti. Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstituciniame veiklos plane“ (toliau – planas) nustatytos priemonės ir asignavimai minėtų tikslų ir uždavinių įgyvendinimui 2019–2021 m. laikotarpiui. Valstybės kibernetinio saugumo ir kibernetinių gynybos pajėgumų plėtros tikslo stiprinimui, konkrečiau – kibernetinės gynybos pajėgumų plėtrai buvo numatyti asignavimai pateikti 1 lentelėje.

1 lentelė. NKSS įgyvendinimo tarpinstitucinio veiklos plano 2019–2021 m. tikslai, uždaviniai, priemonės, asignavimai ir dalyvaujančios institucijos

Eil. Nr.	Tikslo, uždavinio, priemonės pavadinimas	2019 m.		2020 m.		2021 m.		Dalyvaujanti institucija
		Asignavimai, tūkst. eur	Panaudojimas	Asignavimai, tūkst. eurų	Panaudojimas	Asignavimai, tūkst. eurų	Panaudojimas	
1.	**Tikslas** – stiprinti valstybės kibernetinį saugumą ir kibernetinių gynybos pajėgumų plėtrą	1 545,9		2 069		2 695		
1.1.	**Uždavinys** – kurti sisteminį požiūrį į kibernetinį saugumą ir prevencinę veiklą	1 510,9		1 270		2 290		
1.1.1.	**Priemonė** – vystyti Lietuvos kariuomenės Specialiųjų operacijų pajėgų karinių bazių infrastruktūrą (įkurti Regioninį kibernetinio saugumo centrą)	10,9	10,9	140	0	1 240		Krašto apsaugos ministerija
1.4	**Uždavinys** – plėtoti valstybės kibernetinės gynybos pajėgumus	25		739		345		

1.4.1.	**Priemonė** – aprūpinti Ryšių ir informacinių sistemų batalioną kibernetinės gynybos priemonėmis	0	-	492	407,3	0		Krašto apsaugos ministerija
1.4.2.	**Priemonė** – palaikyti ir modernizuoti Ryšių ir informacinių sistemų bataliono kibernetinės gynybos priemones	0	-	197	193,4	295		Krašto apsaugos ministerija
1.4.3.	**Priemonė** – diegti ir atnaujinti priemones Kibernetinio saugumo informaciniame tinkle (toliau – tinklas), siekiant užtikrinti efektyvią Lietuvos kariuomenės kibernetinio saugumo pajėgumų sąveiką su valstybės kibernetiniais pajėgumais	25	23,6	50	48,8	50		Krašto apsaugos ministerija

Šaltinis: Lietuvos Respublikos vyriausybės 2019 m. gruodžio 30 d. nutarimas „Dėl Lietuvos Respublikos Vyriausybės 2019 m. liepos 3 d. nutarimo nr. 709 „Dėl nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinio veiklos plano patvirtinimo“ pakeitimo“.

2019 metų Nacionalinio kibernetinio saugumo centro prie KAM (sutr. NKSC) pateiktoje ataskaitoje apie nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinio veiklos plano įgyvendinimo rezultatus nurodyti šie reikšmingi valstybės kibernetinio saugumo ir kibernetinių gynybos pajėgumų plėtros pasiekimai:

a) *bendradarbiaujant su Sakartvelu, Ukraina bei JAV pradėti Regioninio kibernetinio saugumo centro, kaip praktinės tarptautinio bendradarbiavimo kibernetinio saugumo srityje platformos, steigimo darbai. Planuojama, kad išplėtojus Regioninio kibernetinio saugumo centro veiklą 2021 m. jame bus vykdomi bendri tyrimai, kibernetinio saugumo pratybos, bus kartu dirbama ir keičiamasi informacija apie naujausias kibernetines grėsmes;*
b) *toliau sėkmingai tęsiamas PESCO projektas „Kibernetinės greitojo reagavimo grupės ir savitarpio pagalba kibernetinio saugumo srityje“ (sutr. PESCO projektas), kurio vykdymas 2019 m. itin pasistūmėjo į priekį;*
c) *į NKSC infrastruktūrą įdiegta nauja įranga, kuri kiekvienam svetainės, registruotos Lietuvos zonoje (tik iš lietuviškų IP adresų), turėtojui suteikia galimybę savarankiškai pasitikrinti, ar jo svetainė yra saugi;*
d) *NKSC, vykdydamas Kibernetinio saugumo įstatymo numatytas funkcijas, 2019 m. toliau plėtojo Kibernetinio saugumo informacinį tinklą, į kurį iki 2019 m. pabaigos buvo įtraukta 70 proc. organizacijų, priskiriamų ypatingos svarbos informacinės infrastruktūros (toliau – YSII) ar valstybės informacinių išteklių valdytojams ir (arba) tvarkytojams;*

e) *NKSC 2019 m. spalio 22–24 d. surengė kasmetines nacionalines kibernetinio saugumo pratybas „Kibernetinis skydas 2019“. NKSC atstovai taip pat dalyvavo 4–iose ES, Šiaurės Atlanto sutarties organizacijos (toliau – NATO), kitų šalių organizuotose kibernetinio saugumo pratybose, kuriose stiprino kibernetinių incidentų valdymo įgūdžius;*

f) *Lietuvos kariuomenės (toliau – LK) Ryšių ir informacinių sistemų batalionas (toliau – RISB) buvo aprūpintas dalimi reikalingos kompiuterinės ir programinės įrangos bei transporto, siekiant plėtoti valstybės kibernetinės gynybos pajėgumus;*

g) *LK parengė Lietuvos šaulių sąjungos įtraukimo į Lietuvos kibernetinės gynybos pajėgumus koncepcija, siekdami išsiaiškinti veiksnius, kurie skatintų į LK pritraukti aukštos kvalifikacijos kibernetinio saugumo specialistus ir juos išlaikyti;*

h) *LK 2019 m. lapkričio 11–22 d. organizavo kasmetines kibernetinio saugumo pratybas „Gintarinė migla 2019“, kurių tikslas – stiprinti LK kibernetinių pajėgumų kibernetinės gynybos ir tarptautinio bendradarbiavimo įgūdžius;*

2020 metų reikšmingi valstybės kibernetinio saugumo ir kibernetinių gynybos pajėgumų plėtros pasiekimai:

a) *2020 m. sausio mėn. NKSC pradėjo veikti karinis saugumo operacijų centras (toliau – MilCERT). MilCERT užtikrina krašto apsaugos sistemos (toliau – KAS) informacinių sistemų kibernetinį saugumą. Planuojama, kad pilną pajėgumą MilCERT pasieks po kelerių metų, kai bus parengta pakankamai personalo nenutrūkstamam KAS informacinių sistemų stebėjimui ir gynybai organizuoti;*

b) *2020 m. buvo toliau tęsiamas ES nuolatinio struktūrizuoto bendradarbiavimo projektas „Kibernetinės greitojo reagavimo pajėgos ir tarpusavio pagalba kibernetinio saugumo srityje“ ir pasiektas kibernetinių greitojo reagavimo pajėgų pradinis operacinis pajėgumas (anglų k. Initial Operational Capability). 2020 m. budinčių pajėgų rotacijai vadovavo Lietuva, jas sudarė kibernetinio saugumo specialistai iš Lietuvos, Lenkijos, Nyderlandų ir Rumunijos;*

c) *2020 m. spalio 20–22 dienomis surengtos kasmetinės nacionalinės kibernetinio saugumo pratybos „Kibernetinis skydas 2020“; NKSC atstovai nuotoliniu būdu tobulino savo kibernetinių incidentų valdymo įgūdžius tarptautinėse kibernetinio saugumo pratybose;*

d) *diegtos ir atnaujintos priemonės Kibernetinio saugumo informaciniame tinkle (toliau – KSIT), siekiant užtikrinti efektyvų ir abipusį pasitikėjimą skatinantį tinklo narių bendradarbiavimą;*

e) *įsigyta reikiama techninė ir programinė įranga, reikalinga aprūpinti RISB kibernetinės gynybos priemonėmis;*

f) *2020 m. kovo mėn. buvo parengtas ir patvirtintas Kibernetinio saugumo pajėgumo plėtros planas, kuriuo vadovaujantis bus stiprinami KAS institucijų, veikiančių kibernetinio saugumo srityje, ir kitų įstaigų kibernetinio saugumo pajėgumai;*

g) *2020 m. žengti dar keli žingsniai Kaune kuriant Regioninį kibernetinės gynybos centrą. 2020 m. spalio mėn. NKSC pradėjo vykdyti centro funkcijas, o JAV patvirtino skirsiančios 10 mln. dolerių kibernetinio saugumo mokymų infrastruktūrai sukurti Kaune. Centras turėtų tapti pagrindine Lietuvos ir JAV dvišalio bendradarbiavimo kibernetinėje srityje platforma, jame taip pat bus bendradarbiaujama su Sakartvelo bei Ukrainos kibernetinio saugumo specialistais. Pagrindiniai centro uždaviniai – skatinti inovatyvių kibernetinio saugumo technologijų kūrimą, rengti kibernetinio saugumo specialistus bei keistis informacija apie kibernetines grėsmes;*

h) *LK Gynybos štabas 2020 m. rugsėjo 14–25 d. organizavo kibernetinio saugumo pratybas „Gintarinė migla 2020“, kuriose buvo tobulinti kariuomenės ir civilinio sektoriaus IT specialistų įgūdžiai vykdant ypatingos svarbos informacinės infrastruktūros kibernetinę gynybą.*

Apibendrinus galima teigti, kad kariuomenės lygmenyje 2019–2020 buvo išvystyti/vystomi sekantys kibernetinės gynybos pajėgumai: RISB buvo aprūpintas dalimi reikalingos kompiuterinės ir programinės įrangos bei transporto, siekiant plėtoti valstybės kibernetinės gynybos pajėgumus, parengta Lietuvos šaulių sąjungos įtraukimo į Lietuvos kibernetinės gynybos pajėgumus koncepcija, pradėjo veikti karinis saugumo operacijų centras MilCERT, kuris pilną pajėgumą turėtų pasiekti po kelerių metų, taip pat pasiektas ES kibernetinių greitojo reagavimo pajėgų pradinis operacinis pajėgumas.

Tolimesni valstybės prioritetai kibernetinės gynybos pajėgumų vystyme, atsižvelgiant į NKSS tikslų, uždavinių ir priemonių bei paskirtų asignavimų visumą yra sekantys: įkurti Regioninį kibernetinio saugumo centrą[2] bei plėtoti Lietuvos kariuomenės RISB kibernetines gynybos priemones.

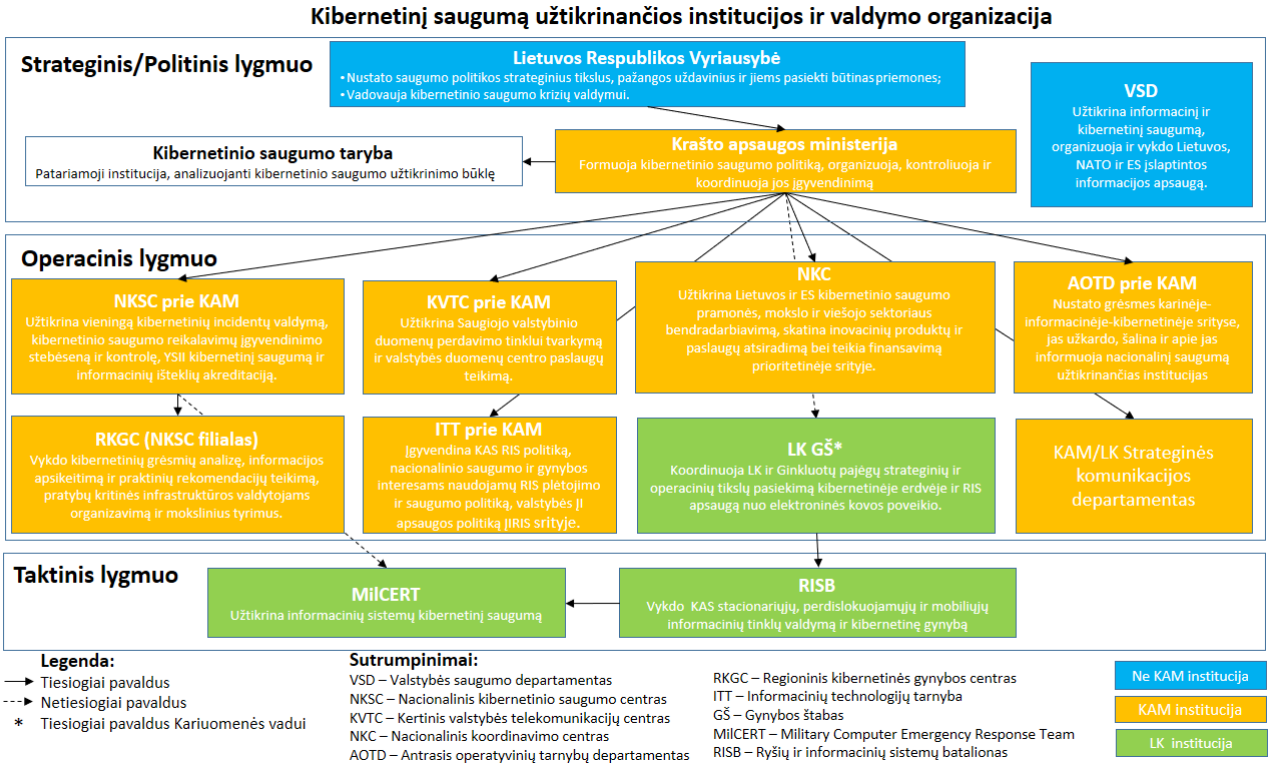
1.2. Kibernetinio saugumo valdymas ir atsakomybės

Siekiant suprasti kaip organizuojamas kibernetinio saugumo valdymas ir kokios nustatytos institucijų atsakomybės, reikalinga išnagrinėti įsatymu nustatytas nuostatas. Kibernetinio saugumo įstatymas nustato „kibernetinio saugumo principus, kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijas, šių institucijų įgaliojimus kibernetinio saugumo srityje, kibernetinio saugumo subjektų pareigas, tarpinstitucinį bendradarbiavimą, ryšių ir informacinių sistemų spragų paieškos ir

[2] Nuo 2021 liepos 1 d. Krašto apsaugos ministro įsakymu įsteigtas Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos filialas – Regioninis kibernetinės gynybos centras.

pranešimo apie jas ir kibernetinius incidentus pagrindus, taip pat nacionalinės kibernetinio saugumo sertifikavimo institucijos funkcijas ir įgaliojimus“.

Toliau nagrinėjamas kibernetinio saugumo valdymo ir institucijų atsakomybių pasidalinimas siekiant užtikrinti kibernetinio saugumo nuostatų įgyvendinimą strateginiame, operaciniame ir taktiniame lygiuose.



Šaltinis: sudaryta autoriaus

2 pav. Kibernetinį saugumą užtikrinančios institucijos ir valdymo organizacija

Strateginis/politinis lygmuo.

Kibernetinio saugumo politikos strateginius tikslus, pažangos uždavinius ir jiems pasiekti būtinas priemones nustato LRV, kurios įgaliojimai:

a) nustato kibernetinio saugumo politikos strateginius tikslus ir (arba) pažangos uždavinius tvirtindama Nacionalinį pažangos planą;

b) tvirtina Kibernetinio saugumo tarybos institucinę sudėtį;

c) tvirtina ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką ir ypatingos svarbos informacinės infrastruktūros ir jos valdytojų sąrašą;

d) tvirtina organizacinius ir techninius kibernetinio saugumo reikalavimus, taikomus kibernetinio saugumo subjektams;

e) tvirtina Nacionalinį kibernetinių incidentų valdymo planą;

f) vadovauja kibernetinio saugumo krizių valdymui.

Kibernetinio saugumo politiką formuoja, jos įgyvendinimą organizuoja, kontroliuoja ir koordinuoja Lietuvos Respublikos krašto apsaugos ministerija (toliau – KAM). KAM įgaliojimai kibernetinio saugumo srityje:

a) dalyvauja rengiant Nacionalinį pažangos planą dėl kibernetinio saugumo politikos strateginių tikslų ir (arba) pažangos uždavinių nustatymo;

b) rengia kibernetinio saugumo politikos pažangos uždavinius įgyvendinančias nacionalines plėtros programas, organizuoja, koordinuoja ir kontroliuoja jų įgyvendinimą;

c) teikia Vyriausybei tvirtinti organizacinius ir techninius kibernetinio saugumo reikalavimus, taikomus kibernetinio saugumo subjektams;

d) teikia Vyriausybei tvirtinti Nacionalinį kibernetinių incidentų valdymo planą;

e) teikia Vyriausybei tvirtinti ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką;

f) teikia Vyriausybei tvirtinti ypatingos svarbos informacinės infrastruktūros ir jos valdytojų sąrašą;

g) tvirtina tipinį kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planą;

h) tvirtina ypatingos svarbos informacinių infrastruktūrų kibernetinės gynybos planą;

i) nustato Nacionalinio kibernetinio saugumo centro reagavimo į kibernetinio saugumo subjektų ryšių ir informacinėse sistemose įvykusius kibernetinius incidentus tvarką;

j) tvirtina techninių kibernetinio saugumo priemonių sąrašą, kuriame nurodoma kibernetinio saugumo priemonių paskirtis ir tvarkomi duomenys (jeigu jie yra tvarkomi), techninių kibernetinio saugumo priemonių diegimo planą, nustato jų diegimo ir valdymo valstybės informaciniuose ištekliuose ir ypatingos svarbos informacinėje infrastruktūroje tvarką;

k) dalyvauja kibernetinio saugumo krizių valdyme;

l) steigia Kibernetinio saugumo informacinį tinklą ir tvirtinta jo nuostatus;

m) tvirtina Kibernetinio saugumo tarybos reglamentą ir personalinę sudėtį;

n) tvirtina nacionalinės spragų atskleidimo tvarkos aprašą.

Kibernetinio saugumo taryba (toliau – KST) yra „nuolatinė kolegiali nepriklausoma patariamoji institucija, analizuojanti kibernetinio saugumo užtikrinimo būklę Lietuvos Respublikoje ir teikianti

kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijoms, kibernetinio saugumo subjektams, mokslo ir studijų institucijoms ir informacinių technologijų srityje veiklą vykdantiems verslo subjektams (toliau – kibernetinio saugumo dalyviai) pasiūlymus dėl kibernetinio saugumo užtikrinimo būklės gerinimo“ (LR Kibernetinio saugumo įstatymas, 2018). KST:

a) teikia kibernetinio saugumo dalyviams pasiūlymus dėl kibernetinio saugumo prioritetų, plėtros krypčių, siektinų rezultatų ir jų įgyvendinimo būdų;

b) teikia kibernetinio saugumo dalyviams pasiūlymus dėl viešojo sektoriaus, verslo ir mokslo bendradarbiavimo galimybių kibernetinio saugumo užtikrinimo srityje;

c) analizuoja kibernetinio saugumo užtikrinimo tobulinimo tendencijas, teikia kibernetinio saugumo dalyviams išvadas ir pasiūlymus dėl kibernetinių incidentų valdymo;

d) teikia kibernetinio saugumo dalyviams rekomendacijas dėl kibernetinio saugumo stiprinimo.

Informacinėje – kibernetinėje erdvėje grėsmių vertinimą, jų užkardymą, šalinimą bei kitų nacionalinį saugumą užtikrinančių institucijų informavimą atlieka Valstybės saugumo departamentas (toliau – VSD) ir Antrasis operatyvinių tarnybų departamentas prie KAM (toliau – AOTD). VSD tikslas yra Lietuvos sprendimų priėmėjams pateikti tokią informaciją, kuri padėtų priimti pagrįstus sprendimus dėl ateities veiksmų politiniame ir visuomeniniame gyvenime. VSD ilgalaikis prioritetas – užtikrinti valstybės suverenitetą, teritorinę neliečiamybę ir vientisumą, konstitucinę santvarką, jos gynybinę ir ekonominę galią, energetinį, informacinį ir kibernetinį saugumą, organizuoti ir vykdyti Lietuvos, NATO ir ES įslaptintos informacijos apsaugą. VSD kartu su Antruoju operatyvinių tarnybų departamentu prie KAM kasmet pateikia visuomenei bendrą grėsmių nacionaliniam saugumui vertinimą.

Operacinis lygmuo

Kibernetinio saugumo politiką įgyvendina **Nacionalinis kibernetinio saugumo centras** (toliau – NKSC), Valstybinė duomenų apsaugos inspekcija, Lietuvos policija ir kitos institucijos, kurių funkcijos yra susijusios su kibernetiniu saugumu. Toliau darbe šių institucijų (išskyrus NKSC) atsakomybės nebus nagrinėjamos, kadangi nėra susijusios su analizuojama tematika.

NKSC prie KAM veiklos tikslai:

a) atlikti kibernetinių incidentų stebėseną, analizę, tyrimus ir su kibernetinių incidentų valdymu susijusius veiksmus;

b) atlikti Saugumo priežiūros tarnybos funkcijas;

c) atlikti Nacionalinės komunikacijų apsaugos tarnybos funkcijas;

d) atlikti informacinių išteklių bei kibernetinio saugumo subjektų atitikties teisės aktų nustatytiems kibernetinio saugumo ir elektroninės informacijos saugos reikalavimams vertinimo, priežiūros ir stebėsenos funkcijas;

e) plėtoti tarptautinį bendradarbiavimą kibernetinio saugumo srityje;

f) vykdyti tyrimų ir švietimo kibernetinio saugumo klausimais veiklą;

g) užtikrinti KAS valdomų ryšių ir informacinių sistemų kibernetinį saugumą;

h) atlikti nacionalinės kibernetinio saugumo sertifikavimo institucijos funkcijas;

i) koordinuoti kibernetinio saugumo subjektų ryšių ir informacinių sistemų spragų atsakingą atskleidimą.

Pažymėtina, kad nuo 2021 metų įsteigtas Regioninis kibernetinės gynybos centras kaip NKSC filialas, atsakingas už kibernetinių grėsmių analizę, informacijos apsikeitimą ir praktinių rekomendacijų teikimą, pratybų kritinės infrastruktūros valdytojams organizavimą ir mokslinius tyrimus.

Kertinis valstybės telekomunikacijų centras (toliau – KVTC) įsteigtas Saugiajam valstybiniam duomenų perdavimo tinklui (toliau – Saugusis tinklas) tvarkyti ir valstybės duomenų centro paslaugoms teikti. KVTC veiklos tikslai:

a) tvarkyti Saugųjį tinklą;

b) eksploatuoti valstybinius duomenų centrus;

c) teikti specialios paskirties ryšių ir informacinių sistemų paslaugas valstybės ir savivaldybių institucijoms, valstybės įstaigoms ir Lietuvos Respublikos strateginę reikšmę nacionaliniam saugumui turinčių įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių įstatyme nurodytoms valstybės įmonėms;

d) teikti informacinių technologijų paslaugas (toliau – IT paslaugos) valstybės institucijoms, iki joms šios paslaugos bus pradėtos teikti centralizuotai.

Informacinių technologijų tarnyba prie KAM (toliau – ITT) įstaiga prie ministerijos, įgyvendinanti krašto apsaugos sistemos (toliau – KAS) ryšių ir informacinių sistemų (toliau – RIS) politiką, nacionalinio saugumo ir gynybos interesams naudojamų RIS plėtojimo ir saugumo politiką, taip pat valstybės įslaptintos informacijos apsaugos politiką įslaptintos informacijos ryšių ir informacinių sistemų (toliau – ĮIRIS) srityje. ITT veiklos tikslai:

a) atlikti Nacionalinės šifrų paskirstymo tarnybos funkcijas;

b) atlikti institucijos, užtikrinančios Lietuvos Respublikos įslaptintos informacijos, užsienio valstybių, Europos Sąjungos (toliau – ES) ir tarptautinių organizacijų Lietuvos Respublikai perduotos įslaptintos informacijos, apdorojamos ar perduodamos ĮIRIS, apsaugą nuo elektromagnetinės spinduliuotės (toliau – TEMPEST), funkcijas;

c) vykdyti NATO RIS plėtrą ir priežiūrą Lietuvos Respublikoje ir kontroliuoti jų saugumą;

d) vykdyti ITT prie KAM tvarkomų tarpžinybinių ĮIRIS (toliau – tarpžinybinės ĮIRIS) plėtrą ir priežiūrą ir kontroliuoti jų saugumą;

e) valdyti Lietuvos Respublikos karinius radijo dažnius;

f) vykdyti KAS RIS plėtrą ir priežiūrą;

g) vykdyti informacinių technologijų paslaugų tarnybos funkcijas.

Lietuvos kariuomenės (toliau – LK) lygmenyje, Gynybos štabo (toliau – GŠ) Ryšių ir informacinių sistemų (toliau – RIS) valdybos J6 Kibernetinės gynybos ir elektroninės informacijos saugos skyrius koordinuoja LK ir Ginkluotų pajėgų strateginių ir operacinių tikslų pasiekimą kibernetinėje erdvėje ir RIS apsaugą nuo elektroninės kovos poveikio. Skyriaus uždaviniai:

a) įgyvendinti kibernetinės gynybos ir elektroninės informacijos saugos politiką kariuomenėje, koordinuoti LK ir Ginkluotų pajėgų operacinių tikslų pasiekimą kibernetinės gynybos srityje ir RIS apsaugą nuo elektroninės kovos poveikio;

b) planuoti ir kontroliuoti kibernetinės gynybos priemonių įgyvendinimą LK operacinėse pajėgose, dalyvaujančiose tarptautinėse operacijose, vykdančiose taikos meto ir valstybės gynybos užduotis, pratybų ir mokymo metu;

c) planuoti ir vykdyti LK RIS saugumo auditus.

Nuo 2022 m. KAM įsteigtas[3] Nacionalinis koordinavimo centras (toliau – NKC), kurio pagrindinis uždavinys didinti Lietuvos ir Europos Sąjungos kibernetinio saugumo pramonės, mokslo ir viešojo sektoriaus bendradarbiavimą, skatinti inovacinių produktų ir paslaugų atsiradimą bei teikti finansavimą prioritetinėje srityje. Taip pat planuojama, kad NKC teiks ekspertines žinias kibernetinio saugumo srityje, prisidės prie kibernetinio saugumo švietimo programų sklaidos Lietuvoje, ES strateginių dokumentų kibernetinio saugumo srityje įgyvendinimo ir ES kibernetinio saugumo bendruomenės kūrimo.

Kaip jau buvo minėta, VSD kartu su AOTD atlieka grėsmių informacinėje – kibernetinėje erdvėje vertinimą. AOTD yra krašto apsaugos ministrui pavaldi Krašto apsaugos sistemos (toliau – KAS) institucija, vykdanti žvalgybą ir kontržvalgybą gynybos, karinėje – politinėje, karinėje – ekonominėje, karinėje – technologinėje ir karinėje – informacinėje – kibernetinėje srityse, KAS institucijų veiklos užsienyje srityje, KAS institucijų valstybės ir tarnybos paslaptį sudarančios informacijos apsaugos srityje.

Taktinis lygmuo

RISB yra žemiausias lygmuo užtikrinantis praktinį kibernetinio saugumo LK nuostatų įgyvendinimą. Bataliono uždaviniai:

a) vykdyti KAS stacionariųjų, perdislokuojamųjų ir mobiliųjų informacinių tinklų valdymą ir kibernetinę gynybą;

[3] Įgyvendinant 2021 m. gegužės 20 d. Europos Parlamento ir Tarybos reglamentą (ES) Nr. 2021/887

b) būti pasirengus vykdyti valstybinės informacinių išteklių ir YSII kibernetinių incidentų valdymo padalinio veiklą.

Šiems uždaviniams įgyvendinti, batalionas vykdo sekančias funkcijas:

a) teikia pagalbą KAS ryšių ir informacinių sistemų tvarkytojams priimant sprendimus dėl kibernetinių incidentų;
b) vykdo atsako į kompiuterinius incidentus, įvykusius KAS, komandos (anglų k. *Military Computer Emergency Response Team,* sutr. MILCERT) veiklą;
c) valdo KAS stacionariose, perdislokuojamose ir mobiliose ryšių ir informacinėse sistemose įvykusius kibernetinius incidentus;
d) seka ir analizuoja globalias kibernetinių grėsmių tendencijas;
e) bendradarbiauja su NKSC bei kitų šalių kibernetinio saugumo centrais aptinkant, užkardant bei likviduojant kibernetinių incidentų padarinius;
f) teikia pagalbą atstatant kibernetinių incidentų paveiktų sistemų funkcionalumą;
g) dalyvauja nacionalinėse bei tarptautinėse kibernetinio saugumo pratybose;
h) stebi valstybės informacinių išteklių ir ypatingos svarbos informacinių infrastruktūrų kibernetinių incidentų valdymo sistemas;
i) rengia personalą vykdyti valstybės informacinių išteklių ir YSII kibernetinių incidentų valdymą;
j) esant poreikiui teikia pagalbą suvaldant kibernetinius incidentus ypatingos svarbos informacinėse struktūrose.

Apibendrinant galima teigti, jog *strateginiame* lygmenyje LRV nustato kibernetinio saugumo politikos strateginius tikslus ir (arba) pažangos uždavinius bei vadovauja kibernetinio saugumo krizių valdymui. KAM formuoja kibernetinio saugumo politiką, taip pat organizuoja, kontroliuoja ir koordinuoja jos įgyvendinimą. *Operaciniame* lygyje NKSC, KVTC ir ITT atsakingos už kibernetinio saugumo politikos įgyvendinimą. LK GŠ atsakingas už LK ir Ginkluotųjų pajėgų strateginių ir operacinių tikslų pasiekimą kibernetinėje erdvėje ir RIS apsaugą nuo elektroninės kovos poveikio, taip pat įgyvendina kariuomenės pajėgumų vystymo planus. *Taktiniame* lygyje RISB vykdo KAS stacionariųjų, perdislokuojamųjų ir mobiliųjų informacinių tinklų valdymą ir kibernetinę gynybą.

2. KIBERNETINIŲ PAJĖGUMŲ VERTINIMO MODELIAI

2.1. Šalies kibernetinių pajėgumų vertinimo modelių apžvalga

Per pastaruosius 20 metų kibernetiniai pajėgumai tapo nauju grėsmingu nacionalinės galios instrumentu (Craig, 2020). Šių pajėgumų panaudojimas gaunant valstybės paslaptis iš kitos valstybės, kaip ir tradicinio šnipinėjimo atveju, valstybės kibernetinius įrankius naudojo ir grėsmingiems tikslams pasiekti. Tai, pavyzdžiui, apima šalies ekonominio vystymosi skatinimas vagiant kitos šalies intelektinę nuosavybę, grasinant žlugdyti valstybių, kurias laiko priešininkėmis finansų institucijas, naftos pramonę, branduolinę energetiką, elektros tinklų ir ryšių infrastruktūrą, bandymai kištis į demokratinius procesus; karinių pajėgumų ardymas ir trikdymas karo metu, ir, vienu atveju, suvaržyti kitos valstybės galimybes kurti branduolinius ginklus. Todėl valstybės stengiasi sumažinti riziką, kurią sukelia kibernetinės grėsmės jų skaitmeninei ekonomikai, ypatingos svarbos nacionalinei infrastruktūrai ir piliečiams, dėdamos daug pastangų investuojant į gynybinius kibernetinio saugumo pajėgumus. Visa tai be abejonės skatina globalizuoto kibernetinės pramonės sektoriaus augimą. Valstybės įtraukia kibernetinius pajėgumus į savo nacionalines investicijų strategijas, karines doktrinas ir planus bei didina su kibernetine erdve susijusios veiklos tempą (Cavelty, 2018).

Literatūroje aptinkama keletas metodų šalies kibernetinės galios (pajėgumų) įvertinimui. Kibernetinio saugumo kompetencijos lygiui įvertinti skiriami lyginamasis vertinimo modelis ir brandos vertinimo modelis (Cho, 2020). Lyginamojo vertinimo modelis – tai vertinimo modelis, identifikuojantis vertinimo elementus, atitinkančius kibernetinio saugumo galimybes, ir nustatantis santykinį lyginamąjį pranašumą tarp vertinimo elementų. Kita vertus, brandos vertinimo modelis yra vertinimo modelis, skirstantis kibernetinio saugumo kompetencijų lygį į brandos lygius, o kompetencijos lygį nustato pagal tai, ar brandos lygis yra patenkintas. Taip pat pajėgumo brandos modelis nustato struktūrą ir metodiką, skirtą gebėjimams stiprinti ir pažangai kritinėse kibernetinio saugumo srityse įvertinti. Brandos modeliai gali padėti įvertinti esamų pajėgumų lygį ir nustatyti tobulintinas sritis.

Darbe kibernetinių pajėgumų įvertinimui analizuojami vertinimo modeliai bendram šalies kibernetiniam pajėgumo ir konkrečiai karinio pajėgumo įvertinimui siekiant nustatyti modelį, tinkamiausią analizuoti Lietuvos kariuomenės kibernetinės gynybos pajėgumą.

Tarptautinio strateginių studijų instituto (anglų k. *The International Institute For Strategic Studies*, 2020) parengta metodika, skirta įvertinti valstybės kibernetinius pajėgumus ir kaip jie prisideda prie nacionalinės galios stiprinimo. Per pastaruosius 20 metų kibernetiniai pajėgumai tapo nauju didžiuliu nacionalinės galios įrankiu (anglų k. *Instrument of national power*). Nemažai organizacijų sukūrė metodikas

kibernetinei galiai matuoti. Dauguma iš jų labiausiai orientuotos į kibernetinį saugumą ir indeksu pagrįstu vertinimu. Ši metodika skiriasi nuo indeksu pagrįstų metodikų, kadangi yra platesnė ir iš esmės kokybinė (anglų k. *Qualitative*), analizuojanti valstybės kibernetinę ekosistemą ir kaip ji susikerta su tarptautiniu saugumu, ekonomine konkurencija ir kariniais reikalais. Metodika išskiria septynias kategorijas, pagal kurias vertina nacionalinį kibernetinį pajėgumą:

a) **Strategija ir doktrina** (anglų k. *Strategy and doctrine*) – svarbiausi vyriausybės dokumentai, kuriuose nustatomi prioritetai ir biudžetai, aprašoma valdymo politika ar organizaciniai pokyčiai, kuriais siekiama didinti visuomenės informuotumą apie nacionalinę strategiją;

b) **Valdymas, vadovavimas ir kontrolė** (anglų k. *Governance, command and control*) – tai apima aukščiausio lygio vyriausybines ir karines struktūras, taip pat taip pat operacinio lygmens struktūras. Analizuojama kaip šios struktūros keitėsi laikui bėgant bei nagrinėjamas jų veiksmingumas.

c) **Pagrindiniai kibernetinės žvalgybos pajėgumai** (anglų k. *Core cyber–intelligence capability*) – gebėjimas nustatyti ir suprasti grėsmes ir galimybes kibernetinėje erdvėje. Yra daugybė informacijos šaltinių, kurie įtakoja situacijos suvokimą, tačiau svarbiausias yra pagrindinis kibernetinės žvalgybos pajėgumas (taip pat paprastai vadinamas "kibernetinio šnipinėjimo" pajėgumu).

d) **Kibernetinis įgalinimas ir priklausomybė** (anglų k. *Cyber empowerment and dependence*) – šalies gebėjimas apsisaugoti nuo kibernetinių pajėgumų turinčio oponento izoliuojantis nuo pasaulinio interneto. Bet kokia priklausomybė nuo interneto ryšio yra neatsiejama nuo pažeidžiamumo, tačiau taip pat suteikia priėjimą prie duomenų, pasaulinį pasiekiamumą ir tinklus, kurie įgalina dvidešimt pirmojo amžiaus ekonomiką, valstybės valdymą ir karybą.

e) **Kibernetinis saugumas ir atsparumas** (anglų k. *Cyber security and resilience*) – apima pagrindinius valstybės kibernetinio saugumo pajėgumus, įskaitant jos gebėjimą reaguoti ir atsigauti po reikšmingų kibernetinių incidentų ir ekstremaliųjų situacijų. Jis taip pat apima saugumo standartus, technines inovacijas, konkrečių sektorių rizikos valdymą, vietinių saugumo sistemų veiksmingumą, kibernetinio saugumo pramonės veiksmingumą ir tai, kokiu mastu šaliai pavyko sukurti ir išplėtoti kibernetinio saugumo specialistų darbo jėgą.

f) **Pasaulinė lyderystė kibernetinės erdvės srityje** (anglų k. *Global leadership in cyberspace affairs*), vertinama kokiu mastu šalis dalyvauja, daro įtaką ir bando vadovauti tarptautiniam bendradarbiavimui kibernetiniais klausimais. Todėl į šią kategoriją įtraukiama tarptautinė diplomatija, oficialūs aljansai, dalyvavimas tarptautiniuose forumuose ir tarptautiniame techniniame bendradarbiavime bei susitarimuose dėl tarpusavio pagalbos.

g) **Puolamieji kibernetiniai pajėgumai** (anglų k. *Offensive cyber capability*) – apima kibernetines operacijas, kurios iš esmės skirtos poveikiui pasiekti, o ne tos, kuriomis iš esmės siekiama rinkti žvalgybinę informaciją. Tokios operacijos gali būti įvairios – nuo operacijų, skirtų kognityviniam poveikiui, iki fizinio sunaikinimo – nesvarbu, ar taikos, ar karo metu, ir neatsižvelgiant į tai, ar operacijoms vadovauja civiliai ar kariškiai, ar taikiniai yra civiliai, ar kariškiai.

Oksfordo universiteto Pasaulinis kibernetinio saugumo pajėgumų centras (anglų k. *Global Cyber Security Capacity Centre*, sutr. *GCSCC*, 2021) sukūrė Kibernetinio saugumo pajėgumų modelį (toliau – KSPM), padedantį valstybėms lengviau įvertinti šalies kibernetinio saugumo pajėgumų brandą.

KSPM ne tik padeda valstybėms suprasti kas veikia, kas neveikia visose kibernetinio saugumo pajėgumų srityse, bet svarbiausia atsako į klausimą „Kodėl?“. Šis modelis parengtas konsultuojantis su daugiau kaip dviem šimtais tarptautinių ekspertų iš vyriausybių, tarptautinių organizacijų, akademinės bendruomenės, viešojo ir privačiojo sektorių bei pilietinės visuomenės. Pagal KSPM, kibernetinį saugumą sudaro penkios dimensijos, kurios kartu sudaro nacionalinio pajėgumo visumą, reikalingą šalims siekiant, kad kibernetinis saugumas būtų veiksmingas (Bellasio ir kt., 2018):

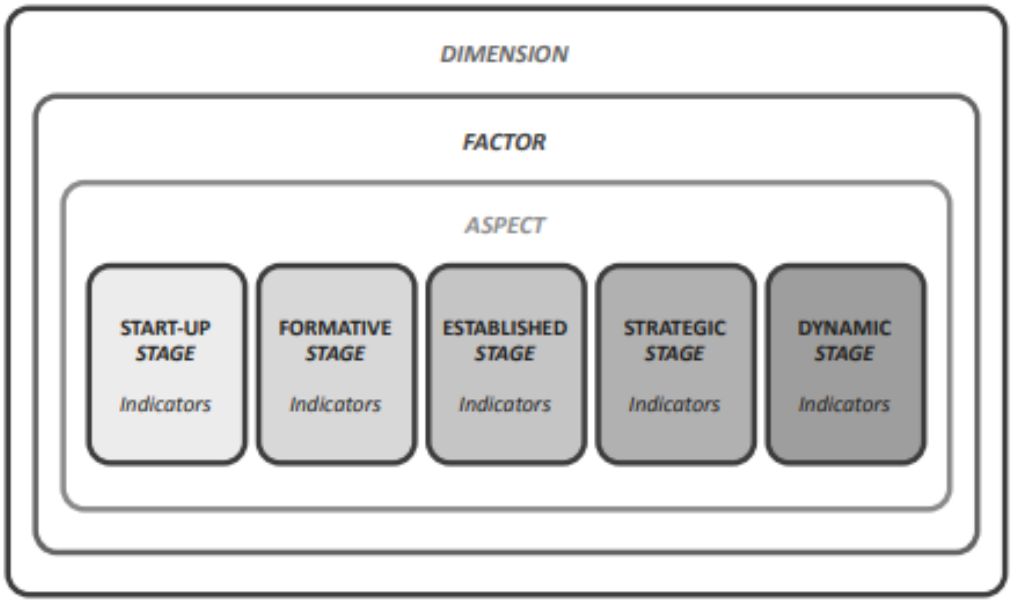
a) **Kibernetinio saugumo politika ir strategija** (anglų k. *Cybersecurity policy and strategy*) apima šalies pajėgumus, gebančius kurti ir įgyvendinti kibernetinio saugumo strategiją ir stiprinti savo kibernetinio saugumo atsparumą – gerinant reagavimą į incidentus, kibernetinę gynybą ir ypatingos svarbos infrastruktūros objektus apsaugos pajėgumus.

b) **Kibernetinio saugumo kultūra ir visuomenė** (anglų k. *Cybersecurity culture and society*), šis aspektas apžvelgia svarbius atsakingos kibernetinio saugumo kultūros elementus, pavyzdžiui: visuomenės supratimą apie su kibernetiniu saugumu susijusią riziką, pasitikėjimą interneto paslaugomis, e – valdžia ir e – prekybos paslaugomis bei naudotojų supratimas apie asmeninės informacijos apsaugą internete.

c) **Kibernetinio saugumo žinių ir gebėjimų ugdymas** (anglų k. *Building cybersecurity knowledge and capabilities*) apžvelgia programų prieinamumą, kokybę ir panaudojimą įvairioms suinteresuotųjų šalių grupėms, įskaitant vyriausybę, privatųjį sektorių ir visus gyventojus. Visa tai susieja su kibernetinio saugumo informuotumo didinimo programomis, formaliomis kibernetinio saugumo švietimo ir profesinio mokymo programomis.

d) **Teisinė ir reguliavimo sistema** (anglų k. *Legal and regulatory frameworks*). Šiuo aspektu nagrinėjamas vyriausybės gebėjimas rengti ir priimti nacionalinius teisės aktus, kurie tiesiogiai ir netiesiogiai susiję su kibernetiniu saugumu, ypač daug dėmesio skiriant kibernetinio saugumo reguliavimo reikalavimams, su kibernetiniais nusikaltimais ir kitiems susijusiems teisės aktams.

e) **Standartai ir technologijos** (anglų k. *Standards and technologies*) sprendžia veiksmingo ir plačiai paplitusio kibernetinio saugumo technologijų panaudojimo siekiant apsaugoti asmenis, organizacijas ir nacionalinę infrastruktūrą. Siekiant sumažinti kibernetinio saugumo riziką, šiuo aspektu konkrečiai nagrinėjama, kaip įgyvendinti kibernetinio saugumo standartų ir gerosios praktikos, procesų ir kontrolės priemonių diegimą, technologijų bei produktų kūrimą.



Šaltinis: Global Cyber Security Capacity Centre, 2021

3 pav. Kibernetinio saugumo pajėgumų modelio struktūra

Kiekvieną iš šių dimensijų sudaro daugybė faktorių (anglų k. *Factors*), kurie fiksuoja pagrindinius gebėjimus. Kartu jie atspindi skirtingus „lęšius“, per kuriuos galima įrodyti ir analizuoti kibernetinio saugumo gebėjimus. Jei faktorių sudaro keletas komponentų, jie vadinami aspektais (anglų k. *Aspects*). Aspektai – tai organizacinis metodas suskirstyti indikatorius (anglų k. *Indicators*) į mažesnes grupes, kad galima būtų lengviau suprasti. Kiekvienas indikatorius apibūdina žingsnius ar veiksmus, kurie parodo konkretų brandos lygį (anglų k. *Stage*).

Kiekvienai dimensijai KSPM išskiria penkis brandos lygius: pradinis (anglų k. *Start–up*), formuojamasis (anglų k. *Formative*), įkurtas (anglų k. *Established*), strateginis (anglų k. *Strategic*) ir dinamiškas (anglų k. *Dynamic*). Kad valstybė sėkmingai pasiektų tam tikrą brandos lygį, ji turi įrodyti atitikimą kiekvienam iš indikatorių. Siekiant padidinti šalies kibernetinio saugumo pajėgumų brandą, kiekvieno lygio indikatoriai turi būti įvykdyti.

KSPM leidžia valstybėms palyginti esamus nacionalinius kibernetinio saugumo pajėgumus. Įsivertinus nacionalinius kibernetinius pajėgumus pagal šį modelį, leidžia šalims suvokti, į kokias sritis reikalinga investuoti, norint pereiti į aukštesnį brandos lygį.

2.2. Karinių kibernetinių pajėgumų vertinimo modelių apžvalga

Reikia pripažinti, kad kibernetinės erdvės militarizacijos laipsnis priklauso ne tik nuo strateginių šalies tikslų, bet ir nuo išteklių prieinamumo (Gartzke, 2013; Liff, 2012). Gomez atliktas tyrimas rodo, kad pasirinkimas militarizuoti kibernetinę erdvę priklauso nuo jos technologinių pranašumų, palyginti su kitomis sritimis (pvz., sausuma, jūra ir oru), ir nuo pajėgumų, sukurtų reaguojant į suvokiamą grėsmių riziką (Gomez, 2016).

Siekiant nustatyti vyraujančias tendencijas karinių kibernetinių pajėgumų vystymui, reikalinga išnagrinėti atviruose šaltiniuose prieinamus šalių karinių kibernetinių organizacijų modelius. Bendrų kriterijų (sričių, kategorijų), keliamų kibernetiniams pajėgumams suradimas įtakos tolimesnei analizei.

Analizuojant Estijos, Nyderlandų, Norvegijos, Vokietijos, Suomijos ir JAV valstybių kariuomenes, Pernik išskyrė sekančias sritis karinių kibernetinių pajėgumų įvertinimui:

a) **Strateginės gairės** (anglų k. *Strategic guidelines*),
b) **Politinis leidimas dalyvavimui tarptautinėse operacijose** (anglų k. *Political authorisation of international deployments*),
c) **Organizacinė struktūra** (anglų k. *Organisational set–up*),
d) **Vadovavimo grandinė** (anglų k. *The chain of command*),
e) **Pagrindinės funkcijos** (anglų k. *Key functions*).

Pasak autorės (Pernik, 2018) „nėra bendro supratimo apie tai, kas yra kibernetinių pajėgų vadovybė (anglų k. *Cyber command*), nei išsamios apžvalgos apie esamas karines kibernetines pajėgas“. Taip pat autorė pabrėžia, kad „nėra universalios geros praktikos kuriant kibernetines pajėgas“. Išnagrinėjus keletos šalių pavyzdžius, autorė reziumavo, kad karinės kibernetinės organizacijos dažnai remiasi "poreikiu centralizuoti, konsoliduoti, ir racionalizuoti anksčiau buvusius suskaidytus pajėgumus ir organizacijas, kartu panaikinant besidubliuojančias funkcijas ir atsakomybę", kad būtų galima veiksmingai veikti šioje naujoje "operacinėje srityje".

Tyrime palyginimo būdu autorės išanalizuoti šalių kibernetiniai pajėgumai pagal minėtas sritis (strateginės gairės, politinis leidimas dalyvavimui tarptautinėse operacijose, organizacinė struktūra, vadovavimo grandinė, pagrindinės funkcijos) leidžia suvokti tiriamųjų šalių karinių kibernetinių pajėgumų

situaciją bei gerąsias praktikas, tačiau naudoti šį metodą pajėgumų vertinimui nepakanka detalesnių vertinimo kriterijų.

Karines kibernetines organizacijas (sutr. KKO) ir jų gebėjimą vykdyti puolamąsias kibernetines operacijas nagrinėjo Smeets. KKO, autoriaus teigimu, apibrėžiama kaip atkirų pajėgų vadovybė, pajėgų rūšis, tarnyba ar vienetas, priklausantis valstybės ginkluotosioms pajėgoms, kuri turi įgaliojimus ir uždavinį vykdyti puolamasias kibernetines operacijas siekiant suardyti (anglų k. *Disrupt*), atmesti (anglų k. *Deny*), pažeminti (anglų k. *Degrade*) ir sunaikinti (anglų k. *Destroy*). Autorius taip pat pažymi, kad kalbant apie NATO valstybių karinius kibernetinius pajėgumus, viešojoje erdvėje nėra prieinamos apžvalgos dėl valstybių narių KKO vystymo. Jis nagrinėja KKO pagal penkis organizacijos raidos etapus vadovaudamasis verslo pasaulyje paplitusiu gyvavimo ciklo (anglų k. *Life cycle*) modeliu (Smeets, 2019):

a) **Užuomazgos ir evoliucijos** (anglų k. *Seed and development*) etapas apima valdžios pripažinimą, kad yra svarbu investuoti į puolamuosius kibernetinius pajėgumus ir svarsto apie poreikį įsteigti KKO;
b) **Pradžios** (anglų k. *Startup*) etapas apima valdžios autorizaciją įsteigti KKO;
c) **Augimo** (anglų k. *Growth*) etape KKO yra pasiekusi pradinį operacinį pajėgumą;
d) **Plėtros** (anglų k. *Expansion*) etape KKO yra vykdžiusi puolamąsias kibernetines operacijas ir vertina tolimesnį organizacijos vystymąsi;
e) **Brandos** (anglų k. *Maturity*) etape KKO, remdamasi strategija, geba vykdyti pilno spektro operacijas prieš plataus mąsto taikinius.

Pagal šį modelį, kiekviena KKO gali eiti savo keliu – ji gali progresuoti ir regresuoti laikui bėgant, o perėjimui iš vieno į kitą etapą gali reikėti daugiau ar mažiau laiko. Pavyzdžiui, KKO gali prarasti savo pradinį operacinį pajėgumą arba visam laikui įstrigti Pradžios etape ir niekada nevykdyti puolamųjų kibernetinių operacijų. Taip pat, jei valstybė turi įsteigusi gerai funkcionuojantį signalų žvalgybos padalinį ir gali pasikliauti turima ekspertize, ji gali greitai pereiti iš Pradžios į Augimo etapą. Pabrėžtina tai, kad KKO judant iš vieno etapo į kitą, nacionalinė valdžia susiduria su skirtingais organizaciniais iššūkiais.

Blessing nagrinėdamas įvairių valstybių KKO, išskyrė penkiais etapais pagrįstą karinių kibernetinių pajėgų įgyvendinimo modelį pagal tai, kaip keitėsi KKO įgyvendinimas:

a) **Išankstinio priėmimo** etapo (anglų k. *Pre–Adoption*) tai kariuomenės, neturinčios kibernetinių pajėgumų;
b) **Pradinis** etapas (anglų k. *Introduction*), kada kariuomenė turi pradinę kibernetinių pajėgumų struktūrą, gali apimti įvairius organizacijos modelius taip pat būti pavaldume egzistuojančios karinės organizacijos;

c) **Modifikacijos** etapas (anglų k. *Modification*) apima bet kokius organizacinio modelio pokyčius nuo turėto Įvadiniame etape. Tai gali būti pasikeitimai vadovavimo lygmenyje, tačiau neapima pokyčių, jei įkuriama atskira kibernetinių pajėgų vadovybė;
d) **Plėtimosi** etape (anglų k. *Expansion*) didinamas vadovavimo mastas, tačiau organizacinis modelis turi išlikti kaip ir praeitame etape t.y. kibernetinė organizacija išlieka pavaldi didesnei karinei organizacijai;
e) **Visiško įgyvendinimo** etapas (anglų k. *Full Implementation*), jo metu sukuriama atskira kibernetinių pajėgų vadovybė, nepriklausomai nuo to, kokiame etape buvo ankstesnis kibernetinių pajėgų organizacinis modelis.

KKO įgyvendinimas yra dinamiškas procesas, susidedantis iš penkių tarpusavyje susijusių etapų: išankstinio priėmimo, pradinio, modifikavimo, plėtimosi ir visiško įgyvendinimo.

Pažymėtina, kad vystant KKO, įgyvendinimas gali sekti kiekvieną etapą iš eilės, tačiau gali būti ir taip, kad įgyvendinant kai kurie etapai gali būti ir praleisti (Blessing, 2020). Autoriaus teigimu kibernetinių pajėgų įgyvendinimui būdinga įtampa tarp dviejų konkuruojančių tikslų, traukiančių įgyvendinimo išteklius priešingomis kryptimis – sukurti organizaciją, kuri efektyviai veiktų kibernetinėje srityje, ir šios organizacijos integravimas į esamą krašto apsaugos sistemos biurokratiją. Siekiant visiškai įgyvendinti kibernetines pajėgas reikalinga apjungti abu tikslus: kibernetinės pajėgos turi būti veiksmingos kasdieninėje veikloje ir tarpžinybiniuose procesuose ir tuo pačiu gebėti greitai prisitaikyti veikti operacinėje aplinkoje.

Taip pat autorius pažymi, kad organizacijos dydis yra svarbus veiksnys nulemiantis kibernetinių pajėgumų įgyvendinimo dinamiką. Didelės karinės organizacijos yra labiau tolerantiškos rizikai, tačiau būdamos didžiulėmis organizacijomis taip pat turi daugiau konkuruojančių interesų. Tokiu būdu kibernetinės pajėgos gali būti lengviau įdiegtos į kariuomenės ekosistemą ir vėliau galima jas plėsti. Ir atvirkščiai, mažesnės karinės organizacijos yra mažiau tolerantiškos rizikai ir turi mažesnius išteklius, tačiau taip pat turi mažiau biurokratinių konkurentų. Atitinkamai mažų organizacijų įgyvendintojai gali sutelkti dėmesį į kibernetinės misijos kūrimą ir siekį gauti papildomų išteklių plėtrai be didesnių biurokratinių derybų. Tikėtina, kad tiek didelėse, tiek mažose organizacijose visiškam kibernetinių pajėgų įgyvendinimui yra svarbūs pateikiami „įrodymai apie koncepciją" (anglų k. *Proof of concept*), ypatingai kada operacinis kibernetinių pajėgų panaudojimo poveikis susiejamas su platesniais strateginiais interesais. Kadangi didesnės organizacijos turi platesnį strateginių interesų portfelį nei mažesnės organizacijos, jos gali turėti daugiau galimybių įrodyti kibernetinių pajėgų vertę.

Europos gynybos agentūros (anglų k. *European Defence Agency*) užsakymu 2012 metais RAND korporacija parengė kibernetinių pajėgumų brandos modelį (Robinson, Walczak, Brune, Esterle, Rodriguez, 2012), pagal kurį organizuotų pratybų metu buvo įvertinti šalių narių kariniai kibernetiniai pajėgumai.

Išslaptintame raporte pateikiamas brandos modelis pagal bendrai kariuomenėse naudojamą pajėgumų vystymo sudėtines DORSAPLIS: Doktrina, Organizavimas, Rengimas, Sistema, Aprūpinimas, Personalas, Lyderystė, Infrastruktūra ir Sąveikumas sritis (Andersson, K. 2020). Šis brandos modelis buvo parengtas išskirtinai nustatyti valstybių karinių kibernetinių pajėgumų brandą bei tobulintinas sritis, jis nustato kibernetinių pajėgumų brandos lygį pagal penkias kategorijas:

a) **Neegzistuojantis** (anglų k. *Non – existent*),
b) **Pradinis** (anglų k. *Initial*),
c) **Apibrėžtas** (anglų k. *Defined*),
d) **Subalansuotas** (anglų k. *Balanced*),
e) **Optimizuotas** (anglų k. *Optimised*).

Brandos modelis turi gana detalius indikatorius įvertinti kiekvieną DORSAPLIS sritį, taip pat jis atitinka kariuomenės karinio pajėgumo vystymo esmines dalis (Lietuvos karinė doktrina, 2016), todėl darbo tiriamojoje dalyje Lietuvos kariuomenės kibernetinių pajėgumų branda bus analizuojama remiantis šiuo modeliu. Taip pat svarbu pažymėti, kad DORSAPLIS modeliu vadovavosi JAV kariuomenės Mokymo ir doktrinų valdyba (anglų k. *Training and Doctrine Command*) ir Kariuomenės kibernetinis institutas įgyvendindami projektą „2050 Cyber Army“, kurio vienas iš tikslų buvo vizualizuoti Kibernetines pajėgas 2050 metams.

3. NATO KARINIŲ KIBERNETINIŲ PAJĖGUMŲ VYSTYMASIS IR TENDENCIJOS

3.1. NATO reikalavimai karinių kibernetinės gynybos pajėgų vystymui

„Cyberspace is the new battleground and making NATO cyber ready: well – resourced, well – trained, and well – equipped is a top priority..“

Jens Stoltenberg, NATO Secretary General

NATO viršūnių susitikimo Vašuvoje ir Briuselyje metu išsakyta vizija, kad „turime sugebėti veikti kibernetinėje erdvėje taip pat efektyviai kaip ir ore, sausumoje ir jūroje, kad sustiprintume ir palaikytume bendrą Aljanso atgrasymo ir gynybos poziciją“ nepalieka abejingų dėl kibernetinės erdvės reikšmingumo NATO vadovaujamose operacijose ateityje (Deschaux-Dutard, 2021). Tai nulemia ir dvi pagrindinės NATO veiklos kryptys: kibernetinės erdvės, kaip operacijų srities įgyvendinimas ir Kibernetinės Gynybos Įsipareigojimų (anglų k. Cyber Defence Pledge) vykdymas (Brent, 2019).

Karinėms įstaigoms ir tokiai organizacijai, kaip NATO, vystant kibernetinę erdvę kaip atskirą karinių operacijų vykdymo sritį (operacijų domeną), susiduriama su aiškiais kultūriniais ir organizaciniais iššūkiais, kurie turi tolesnį poveikį kitiems operacijų domenams (sausumos, oro bei jūrų). Kibernetinė erdvė negali veikti kaip atskira (izoliuota) operacijų erdvė, priešingai, ji privalo būti integruota į kitas operacijų sritis (Shea, 2018). Operacijos kibernetinėje erdvėje turi būti suprojektuotos taip, kad remtų konvencines karines operacijas, kaip pajėgų daugiklis (anglų k. *Force multiplier*) ir atvirkščiai. Tai reiškia, kad atskiros kariuomenės pajėgų rūšys turi suprasti, pasitikėti ir būti pasirengusios panaudoti visus pajėgumus ir nustatyti tas situacijas, kada panaudojus kibernetinį efektą, karinis uždavinys būtų atliekamas greičiau, efektyviau ar pigiau nei įprastas ginklas.

2017 m. lapkričio mėn. NATO Gynybos ministrų taryba priėmė sprendimą integruoti sąjungininkų nacionalinius kibernetinius pajėgumus į NATO misijas ir operacijas. NATO generalinis sekretorius pareiškė, kad „kibernetinių pajėgumų panaudojimas gali būti proporcingesnis atsakas, todėl aš džiaugiuosi, kad dabar integruojame nacionalinius kibernetinius pajėgumus į NATO misijas ir operacijas ir kad susitarėme dėl naudojimo principų“. Šis sekretoriaus pareiškimas tik sustiprino kibernetinių pajėgumų panaudojimo svarbą ateities kariniuose konfliktuose ir tuo pačiu paskatino NATO valstybes stiprinti nacionalinių kibernetinių pajėgumų vystymą. Jo matymu, kibernetinių pajėgumų integravimas į NATO vykdomas operacijas bus toks pat kaip ir konvencinių pajėgumų. Numatoma, kad kibernetiniai pajėgumai NATO operacijų vykdymo metu išliks visiškoje nacionalinėje kontrolėje (anglų k. *Full national control*).

Kalbant apie NATO kibernetinių pajėgų panaudojimą operacijose, svarbu paminėti, kad aljansas ne tik planuoja integruoti nacionalinius kibernetinius pajėgumus, tačiau vysto ir savo struktūras, stiprinančias situacijos suvokimą (anglų k. *Situational awareness*) kibernetinėje erdvėje, įgalinančias planuoti ir vykdyti kibernetines operacijas visuose lygiuose[4]. Patvirtintoje ir sustiprintoje NATO vadovavimo struktūroje (anglų k. *Command structure*)[5] 2018 metais pradėtas kurti kibernetinės erdvės operacijų centras (anglų k. *Cyberspace Operations Centre*) (Benien, 2020) ir planuojama, kad visišką operacinį pajėgumą (anglų k. *Full operational capability*) jis pasieks 2023 metais. NATO kibernetinės erdvės operacijų centro pagrindinis tikslas yra aprūpinti Vyriausiąjį sąjungininkų Europoje vadą (anglų k. *Supreme Allied Commander Europe (SACEUR)*) visomis reikiamomis priemonėmis veikti kibernetinėje erdvėje: koordinuoti suverenius kibernetinius pajėgumus, kuriuos savanoriškai teikia sąjungininkai (anglų k. *Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA)*) ir užtikrinti situacijos suvokimą bei koordinuoti NATO operacinę veiklą virtualioje erdvėje.

Kartu su atskiros karinių operacijų vykdymo srities (kibernetinės erdvės) pripažinimu, aljansas 2018 metais patvirtino Kibernetinės erdvės viziją ir strategiją. Šis reikšmingas Aljanso kibernetinės erdvės plėtros etapas buvo svarbus tolimesniam politikos, pajėgumų ir doktrinos vystymui (MacKenzie, 2019). NATO karinė kibernetinės erdvės vizija ir strategija remiasi dviem pagrindiniais principais: pirma, efektyvi gynyba priklauso nuo palaikomo pasirengimo lygio (anglų k. *Sustained level of readiness*) ir gebėjimo greitai sugeneruoti kibernetinius efektus prieš kylant bet kokiai krizei ar konfliktui. Antra, komplikuotas kibernetinės erdvės operacijų koordinavimas kur dauguma skirtingų subjektų privalo dirbti sklandžiai reikalauja centralizuoto priėjimo.

NATO Kibernetinės erdvės vizijos ir strategijos įgyvendinimui išskyrė penkias operacines (pastangų) linijas (anglų k. *Lines of effort*) (Shea, 2019):

a) **Pirmasis reikalavimas** - apsaugoti ir apginti NATO kibernetinę erdvę nuo visų kibernetinių grėsmių. Tai reiškia ne tik reagavimą į atskiras kibernetines atakas, bet, ir kas svarbiausia, kritinių tinklų atsparumo bet kuriuo metu išlaikymas. NATO ir kiekvienas sąjungininkas yra atsakingas už savo kibernetinės erdvės segmento apsaugą, tačiau NATO vaidina svarbų vaidmenį sudarant sąlygas, išlaikant situacijos suvokimą ir priemonių perkėlimą iš vienos sąjungininkės (ar taktinės situacijos) į kitą vystantis krizei ar konfliktui.

[4] Strateginiame, operaciniame ir taktiniame lygmenyse.
[5] NATO karinę vadovavimo struktūrą sudaro *Sąjungininkų operacijų vadovybė* ir *Sąjungininkų transformacijos vadovybė.*

b) **Antras reikalavimas** - būtinų kibernetinės erdvės pajėgumų stiprinimas. Nuo 2013 metų prasidėjus NATO Gynybos planavimo procesui[6], sąjungininkams buvo paskirti minimalūs kolektyviniai tikslai, siekiant nustatyti bazinę orientacinę liniją (anglų k. *Common baseline*) nacionaliniams elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padaliniams (anglų k. *Cyber emergency response teams (CERT)*), bazinei kriptografijai ir šifravimui bei švietimo ir mokymo stiprinimui. Laikui bėgant šie kolektyviniai tikslai tapo vis labiau reiklesni ir specialiai pritaikyti ir nukreipti į kiekvieno sąjungininko individualius trūkumus. Nustatytos spragos, ypač kai jos būdingos daugeliui sąjungininkų, o ne tik vienai šaliai narei, gali būti sprendžiamos per NATO Gynybos planavimo procesą arba išmanios gynybos (anglų k. *Smart Defense*)[7] bendradarbiavimo iniciatyvą. Šios iniciatyvos rėmuose NATO dabartiniu metu vykdo projektus, susijusius su tarptautinių pajėgumų plėtra (anglų k. *Smart Defence Multinational Cyber Defence Capability Development (MN CD2)*) ir kenkėjiškų programų dalijimosi platforma (anglų k. *Malware Information Sharing Platform (MISP)*). Tarptautinis kibernetinės gynybos švietimo ir mokymo projektas (anglų k. *Multinational Cyber Defence Education and Training (MN CD E&T)*) buvo baigtas. Kibernetinės Gynybos Įsipareigojimuose taip pat reikalaujama, kad sąjungininkai patys įsivertintų savo pasirengimo lygį ir brandą. Tai įpareigoja sąjungininkus laikytis „visos valdžios“ (anglų k. *Whole of government*) požiūrio ir privertė daugelį sąjungininkų geriau koordinuotis darbą tarp skirtingų ministerijų bei stiprinti savo nacionalines kibernetinės gynybos struktūras.

c) **Trečiasis reikalavimas** yra užtikrinti, kad NATO atgrasymas ir gynyba būtų palaikoma priimant kibernetinę erdvę kaip operacijų sritį. Norint pasiekti šiuos tikslus, aljansas turi labiau įsitraukti į atsparumo didinimą, nustatyti savo pažeidžiamumą ir įgyvendinti išsamius verslo tęstinumo planus. Įgyvendiniant šį užsibrėžtą tikslą NATO nutarė įkurti Reagavimo į kompiuterinius incidentus pajėgumą (anglų k. *NATO Computer Incident Response Capability (NCIRC)*), kurio pagrindinis tikslas yra saugoti NATO kompiuterinius tinklus teikiant centralizuotą ir visą parą veikiančią kibernetinės gynybos paramą. NCIRC taip pat palaiko greito reagavimo komandas, kurios gali būti dislokuotos remti NATO ar sąjungininkų tinklų apsaugą.

d) **Ketvirtuoju reikalavimu** siekiama kibernetinę erdvę integruoti į jungtines operacijas (anglų k. *Joint operations*). Kibernetinės erdvės įvertinimas turi būti atliktas per visas karines jungtinių

[6] NATO Gynybos planavimo proceso tikslas – laiku identifikuoti, vystyti ir panaudoti pajėgumus, reikalingus sąjungininkų misijoms vykdyti NATO pajėgų Europoje aukščiausiojo vado (SACEUR) operacijų rajone.

[7] Išmanioji gynyba leidžia šalims bendradarbiauti kuriant ir palaikant pajėgumus, kurių jos vienos negalėtų sau leisti sukurti ar įsigyti, taip atlaisvinant išteklius kitiems pajėgumams plėtoti.

operacijų funkcijas (anglų k. *Joint functions*)[8] t.y. nuo žvalgybos, vadovavimo ir kontrolės iki karių ir civilių bendradarbiavimo. Siekdama suvienyti informacijos rinkimą, sprendimų priėmimą ir operacijų vykdymą kibernetinėje erdvėje, NATO stengiasi pasiekti aukštą suderinamumo lygį tarp NATO ir nacionalinių operacinių kibernetinės erdvės organizacijų ir pajėgų. Tuo tikslu 2020 metais buvo patvirtinta viena iš kertinių NATO kibernetinės erdvės doktrinų – AJP 3-20 „Allied Joint Doctrine For Cyberspace Operations“, kuri reglamentuoja NATO kibernetinės erdvės operacijų planavimą, vykdymą bei vertinimą vykdant sąjungininkų jungtines operacijas (anglų k. *Allied joint operations*). Kibernetinių instrumentų panaudojimas NATO operacijose yra ypatingai jautrus, todėl tarptautinės teisės laikymasis yra būtiniausia sąlyga bet kokiam aljanso kibernetinių priemonių panaudojimui ir vadovavimasis sutartomis kovos veiksmų taisyklėmis (anglų k. *Rules of engagement*). Tuo tikslu NATO Bendros kibernetinės gynybos kompetencijos centras (anglų k. *NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE)*) parengė vadovą „Tallinn Manual on the International Law Applicable“, kuriuo siekiama išaiškinti, kaip tarptautinė teisė taikoma kibernetinėms operacijoms. Nors šis dokumentas ir nėra doktrina, tačiau jis buvo rengtas tarptautinių ekspertų, kurie perteikė gerąją tarptautinės teisės praktikos taikymą kibernetinei erdvei.

e) **Penktasis** ir paskutinis nuoseklios NATO kibernetinės erdvės vizijos ir strategijos įgyvendinimo reikalavimas yra skatinti vieningas pastangas (anglų k. *Unity of effort*) kuriant veiksmingus santykius tarp NATO ir šalių sąjungininkių. Naujosios NATO vadovavimo struktūros, kurios pagrindinis dėmesys skiriamas kolektyvinei gynybai, logistikai ir kovinėms operacijoms, vienas iš pagrindinių uždavinių bus palaikyti ir plėtoti koordinuotą kibernetinės erdvės vertinimą ir atsako į gynybą opcijų generavimą. Šios pastangos leis NATO parengti bendrus pasirengimo, reagavimo ir atsparumo planus ir suteiks progą NATO treniruotis realiomis sąlygomis. Efektyvi kibernetinė gynyba reikalauja realistiško situacijos suvokimo, kuris pasiekiamas turint gerus išankstinio perspėjimo indikatorius ir perspėjimus (anglų k. *Early warning indicators and warnings*) bei gebėjimą pavienes kibernetines atakas sujungti į didesnį gynybinį ar strateginį paveikslą (Janczewski ir kt., 2019).

Įgyvendinant šį reikalavimą, civilių ir kariškių bendradarbiavimas yra labiau kritinis kibernetinėje srityje nei bet kurioje kitoje gynybos srityje. NATO Industrijos kibernetinio bendradarbiavimo (anglų k. *NATO Industry Cyber Partnership*) iniciatyva įsteigta pramonei, kuri suteikia galimybę dalyvauti „Threat Vector“ seminaruose, kur nacionalinės žvalgybos tarnybos dalinasi strateginio lygio tendencijomis ir

[8] Jungtinių operacijų funkcijas sudaro: manevras, ugnies parama, vadovavimas ir kontrolė, žvalgyba, informacija, išsilaikymas, pajėgų apsauga ir civilių-kariškių bendradarbiavimas (AJP-3 Allied joint doctrine for the conduct of operations).

grėsmių naujienomis. Industrijos atstovai taip pat kviečiami stebėti aljanso kibernetines pratybas bei prisidėti prie pratybų scenarijaus kūrimo. Inovacijų srityje NATO įkurtas inovacijų centras (anglų k. *Innovation hub*), kuriame ekspertai ir inovatoriai iš viso pasaulio bendradarbiauja sprendžiant NATO iššūkius ir kuriant sprendimus. Šiuo metu inovacijų centre veikia šios iniciatyvos, susijusios su kibernetine erdve: kibernetinė psichologija, kibernetinės erdvės suvokimas ir dirbtinis intelektas saugumo užtikrinimui. Ši platforma suteikia pramonei galimybes išbandyti savo prototipus ir produktus imituojamuose NATO tinkluose, kad aljansas galėtų likti technologinės kreivės priešakyje. Geresnis naujovių ir jų galimo poveikio supratimas padeda daug anksčiau numatyti naujus, ekonomiškai efektyvesnius sprendimus rengiant reikalavimus naujiems vystomiems pajėgumams.

3.2 Estijos kariniai kibernetiniai pajėgumai

NATO generalinis sekretorius, 2019 metais kalbėdamas Kibernetinės Gynybos Įsipareigojimų konferencijoje pabrėžė, kad norint, kad atgrasymas būtų visiškai veiksmingas prieš valstybinius ir nevalstybinius priešininkus (anglų k. *State and non – state adversaries*), NATO ir jos valstybės narės turi būti pasirengusios išnaudoti visus savo turimus kibernetinius pajėgumus, įskaitant ir nacionalinius puolamuosius kibernetinius pajėgumus. Atgrasymas yra priešininko ketinimo sumenkinimas siekiant pabrėžti būsimų išlaidų dydį jei priešininkas imtųsi nepageidaujamo veiksmo.

Nuo 2016 m. sekantys sąjungininkai patvirtino savo norą priskirti puolimo ir gynybinius kibernetinius pajėgumus NATO operacijoms: Estija, Danija, Nyderlandai, Jungtinė Karalystė ir Jungtinės Amerikos Valstijos (Davis, 2019). Šiame darbe bus analizuojami Estijos ir JAV kariuomenių kibernetiniai pajėgumai.

Pradedant nuo 1990-ųjų ir 2000-ųjų pradžioje Estijos vyriausybė skyrė didelį dėmesį investicijoms į informacinių technologijų plėtrą. Siekdama tapti tarptautiniu informacinių technologijų lyderiu, Estijos valstybinė ir privati infrastruktūra tapo labai priklausoma nuo interneto. Estijos kritinė infrastruktūra tapo labiau nei bet kurios kitos pasaulio šalies priklausoma nuo kibernetinio saugumo: nuo įprastų e–valdžios operacijų, e–bankininkystės iki naudojimo kariuomenėje. Taip internetas tapo neatsiejama valstybės funkcionavimo dalimi. Didžioji viso to dalis buvo politiniai tikslai: Estijos valdžia norėjo greitai atsikratyti sovietinio palikimo ir globalizuotis pasitelkdami technologijas.

Lūžio taškas stiprinti kibernetinio saugumo pajėgumus įvyko 2007 metais, kada Estijos valdžia nusprendė perkelti bronzinio kario statulą. Šio įvykio pasekmėje, apie 3 savaites Estijos valdžios institucijos ir privačios kritinės infrastruktūros įstaigos patyrė kibernetines atakas, kurios sąlygojo grėsmę Estijos nacionaliniam saugumui. Tuo metu Estijoje nebuvo atsakingos institucijos, atsakingos už kibernetinį

saugumą ar gynybą (Boeke, 2017). Tuometinis CERT–EE tapo tecnhinio koordinavimo centru, tačiau nebuvo politinio koordinavimo mechanizmo. Estijos Gynybos ministerijai priklausančiam štabo ir ryšių batalionui buvo pavesta užtikrinti Estijos Gynybos ministerijos strateginės komunikacijos ir informacinių technologijų veikimą. Šio bataliono specialistai buvo pasitelkti kaip konsultantai, kadangi buvo paveikta tik civilinė infrastruktūra ir atakos neįtakojo Gynybos ministerijos veiklos. Po šio incidento Estijos valdžia suprato, kad kibernetinės atakos nebuvo pirmiausia susiję su karinės gynybos sritimi. Estijos gynybos ministerija stengėsi aktyviai mažinti savo įtaką koordinuojant tarptautinę pagalbą bei šalies vidaus politikoje (Blessing, 2019). Gynybos ministerija suformulavo šiuos artimojo laikotarpio tikslus: pirmiausia, kartu su Ekonomikos ir ryšių ministerija parengti nacionalinę kibernetinio saugumo strategiją, antra, kooperuojantis su NATO įkurti kibernetinį kompetencijos centrą (anglų k. *Cyber center of excellence*) ir galiausiai karinių kibernetinių gebėjimų stiprinimas rezervo karių pagrindu. Per beveik metus laiko, Estija patvirtino kibernetinio saugumo strategiją ir kartu su NATO įkūrė NATO kibernetinės gynybos kompetencijos centrą (anglų k. *NATO Cooperative Cyber Defense Center of Excellence*). Strategijoje buvo stipriai akcentuojamas visos šalies (anglų k. *Whole of nation*) požiūris: organizacinės, techninės ir reguliavimo informacijos saugumo priemonės turėjo būti įgyvendintos Gynybos, Švietimo ir mokslinių tyrimų, Teisingumo, Ekonomikos ir ryšių, Tarptautinių reikalų ir Užsienio reikalų ministerijose (Tumkevič, 2017). Taip pat strategijoje Estijos kariuomenės vaidmuo įvardintas kaip remiantysis: remti naujai įsteigtą NATO kibernetinio saugumo kompetencijos centrą ir veikti kaip partneris kibernetinio saugumo magistro studijose Talino technikos universitete.

2009–2012 metų periodu pagal tuo metu Estijos parlamento nustatytą ginkluotųjų pajėgų struktūrą, Štabo ir ryšių batalionui oficialiai delegavo su kibernetine veikla susijusias pareigas bei įformino kariuomenės santykius su NATO kibernetinės gynybos kompetencijos centru. Tuo pačiu periodu Gynybos ministerija prioritetą daugiau skyrė civilinei kibernetinio saugumo dimensijai nei karinių kibernetinių pajėgumų plėtrai. Nepaisant to, ministerija netiesiogiai vystė žmogiškąjį talentą kibernetinėje ervėje savo rezervo padaliniuose siekiant stiprinti tiek civilinius tiek karinius gebėjimus. Estijos gynybos lygoje (angl. *Estonian Defense League*)[9] rezervistų pagalba buvo suformuotas kibernetinės gynybos vienetas (anglų k. *Defence League's Cyber Unit*). Taip pat 2011 m. Estijos valdžia nusprendė kibernetinio saugumo politikos koordinavimo atsakomybę iš Gynybos ministerijos perduoti Ekonomikos ir ryšių ministerijai. Šis pokytis turėjo pabrėžti šalies vidaus kibernetinio saugumo svarbą prieš nacionalinį saugumą ir taip padidinti vyriausybės suvokimą.

[9] Estijos gynybos lyga yra sukarinta gynybos organizacija, kurios tikslas yra garantuoti valstybės nepriklausomybės ir suvereniteto išsaugojimą, jos sausumos teritorijos vientisumą ir konstitucinę santvarką.

2013 m. patvirtinus gynybos plėtros planą, Gynybos ministerija žengė svarbų žingsnį sujungiant civilinę ir karinę kibernetinę patirtį. 2014 m. įkurtas kibernetinės politikos departamentas, kurio pagrindinė užduotis buvo koordinuoti su kibernetine veikla susijusias iniciatyvas, rengti pasiūlymus politikos formavimui bei būti pirminiu kontaktu visoms valdžios institucijoms. Ši struktūrinė reorganizacija lėmė du svarbius pokyčius (Blessing, 2020): nepaisant to, kad buvo siekiama bendro tikslo supaprastinti ir sustiprinti ministerijos pastangas kibernetinėje erdvėje, civiliniai ir kariniai mąstymo būdai, kaip pasiekti šį tikslą, labai skyrėsi. Kibernetinės politikos departamentas konsolidavo informacinių ir ryšių technologijų (IRT) paslaugas (vien tik paslaugų lygį) – ne kibernetinius pajėgumus. Dirbantys kariuomenėje tvirtino, kad IRT paslaugos turi būti supaprastintos, kad galėtų remti karinę veiklą. Ir priešingai civiliams, kurie dirbo ministerijoje, jie teigė, kad IRT konsolidavimas turėtų teikti pirmenybę taikos meto funkcijų vykdymui, siekiant geresnio integravimosi ir koordinacijos su kitomis ministerijomis. Konsoliduodamas IRT paslaugas, Kibernetinės politikos departamentas nustatė ministerijos ir kariuomenės bendrų tikslų siekimą ir dubliuojančias atsakomybes. Kitas pokytis buvo tas, kad egzistavęs civilių ir karių žmogiškųjų resursų paskirstymas buvo decentralizuotas ir visiškai neveiksmingas, atsižvelgiant į išteklių ribotumą. Civiliniu lygmeniu beveik kiekvienas gynybos ministerijai pavaldus padalinys ir departamentas turėjo savo vyriausiąjį informacijos pareigūną, vyriausiąjį informacijos saugumo pareigūną ar vyriausiąjį technologijų pareigūną. Ministerijos vadovybė nusprendė, kad centralizavus šiuos žmogiškuosius išteklius ne tik supaprastins kibernetinės veiklos procesus, bet taip pat padės sutaupyti pinigų. Kariuomenėje tuo tarpu, štabo ir ryšių batalionas buvo atsakingas už karinio tinklo gynybą, kiekviena iš pajėgų rūšių (sausumos, oro, jūrų ir specialių operacijų) turėjo savo padalinius skirtus paremti jų vykdomas operacijas. Laikui bėgant tokia struktūra tapo neveiksminga. Kibernetinės politikos departamento sukūrimas paskatino peržiūrėti, kaip Estijos gynybos pajėgos galėtų geriau organizuoti savo pastangas kibernetinėje srityje.

Tolimesnės diskusijos Kibernetinės politikos departamente dėl kibernetinių kariuomenės elementų konsolidavimo stipriai augo, kai departamentas bendradarbiavo kuriant antrąją Nacionalinę kibernetinę strategiją. 2014 m. išleistoje antroje strategijos versijoje buvo viešai pripažintas kariuomenės vaidmuo kibernetinėje erdvėje. Nors pripažinimas ir buvo ribotas, tačiau jis nurodė karių ketinimą plėtoti kibernetinius pajėgumus NATO kolektyvinės gynybos tikslais.

Vėliau sekė Estijos kariuomenės reorganizacija (kibernetinės gynybos srityje), kurią sąlygojo trys pagrindiniai argumentai. Pirma, augantis aukšto lygmens koordinavimo poreikis kovojant su tinklo atakomis reikalavo turėti visa apimančią instituciją kariuomenėje. Atskirų kariuomenės kibernetinių padalinių sujungimas į naują sistemą ar organizaciją palengvino koordinavimą tiek Estijos ekosistemos viduje, tiek išorėje su NATO sąjungininkais. Tokiu būdu vien turimas štabo ir ryšių bataliono pajėgumas tapo nepakankamu. Antra, štabo ir ryšių batalionui trūko resursų veikti didesniu mastu. Svarbiausia, kad

batalionui trūko žmogiškųjų išteklių, o likęs talentas kariuomenėje buvo išsklaidytas kituose padaliniuose. Nauja organizacija struktūroje, esanti aukštesnėje vadovavimo grandinėje, gebėtų sutelkti esamus talentus ir labiau pritrauktų vyriausybės išteklius įdarbinti ir apmokyti naujus kibernetinius specialistus. Galiausiai, pertvarkius kariuomenės kibernetinius padalinius, atsirado galimybė sumažinti biurokratines kliūtis, susijusias su vadovavimu ir kontrole. Didėjant operaciniam greičiui kibernetinėje erdvėje reikalinga trumpesnė nei buvo vadovavimo grandinė. Pavyzdžiui, kad Kibernetinės politikos departamento nurodymas pasiektų karinius vienetus, jis turėjo pereiti kelis biurokratijos lygius: Kibernetinės politikos departamentas buvo pavaldus gynybos ministrui, Vadovavimo, kontrolės, ryšių ir kompiuterių valdyba (atsakingas už kibernetinį planavimą) buvo pavaldus generalinio štabo viršininkui, o štabo ir ryšių batalionas buvo tiesiogiai pavaldus kariuomenės vadui. Judant tokia vadovavimo grandine buvo rizikuojama prarasti koordinavimą tiek strateginiame, tiek operaciniame lygmenyse. Buvo vadovautasi prielaida, kad centralizavus vadovavimo ir valdymo grandinę, operacinis greitis padidėtų, o kai kurie klausimai galėtų pasiekti aukštesnį politinį lygį greičiau ir reakcija į kibernetines atakas būtų greitesnė. Pagrindinė viso to išvada buvo ta, kad Estijos kariuomenėje turėtų būti sukurta nauja į kibernetinę erdvę orientuota vadovybė (anglų k. Cyber-focused command).

2015m. Kibernetinės politikos departamentas pradėjo vidinį darbą rengdamas kibernetinės politikos planą Gynybos ministerijai. Šio plano rėmuose taip pat buvo įtrauktas ir kariuomenės kibernetinių pajėgumų konsolidavimas į naują kibernetinių pajėgų vadovybę. Pagrindiniai iššūkiai tuo metu buvo įtikinti karinę vadovybę, įskaitant ir pajėgų vadus, kad naujos pajėgų vadovybės įsteigimas nebus didžiulė rizika, t. y. kad tai nepakenks pagrindiniam kariuomenės tikslui. Daugelis vadų bijojo, kad įkūrus naują struktūrą, iš pajėgų bus perskirstyti resursai, tačiau Kibernetinės politikos departamento sudaryta darbo grupė, nustatė sritis, kuriose kariuomenė galėtų investuoti į kibernetinius pajėgumus, nepakenkiant pajėgų kariniams prioritetams.

Kibernetinės pajėgų vadovybės organizavimo prasme, naujos vieningos organizacijos sukūrimas buvo vienintelė galima alternatyva. Nuspręsta, kad naujoji kibernetinių pajėgų vadovybė bus iš dalies modeliuojama pagal Estijos specialiųjų operacijų pajėgas organizacinę struktūrą - nepriklausomą pajėgų rūšį, pavaldžią tiesiogiai kariuomenės vadui.

2017 m. Gynybos ministerijos paskelbtame plėtros plane buvo paskelbta, kad Estijos kariuomenė oficialiai įsteigs naują kibernetinių pajėgų vadovybę. Šis sprendimas buvo suformuotas kaip tiesioginė 2016 m. NATO sprendimo pripažinti kibernetinę erdvę karine sritimi pasekmė.

2018 m. Estijos parlamento sprendimu priimtas kariuomenės struktūros pakeitimas apėmė oficialų kibernetinių pajėgų vadovybės įsteigimą. Į jos pavaldumą įtraukta: štabo ir ryšių batalionas, informacijos ir ryšių technologijos centras, strateginės komunikacijos centras, štabo ir aprūpinimo kuopa, kibernetinių ir

informacinių operacijų centras. Planuota, kad kibernetinių pajėgų vadovybė pasieks pilną operacinį pajėgumą 2023 m. (Blessing, 2020).

3.3 JAV kariniai kibernetiniai pajėgumai

1998 m. JAV Gynybos departamentas įkūrė kompiuterinių tinklų gynybos jungtines užduoties vykdymo pajėgas (anglų k. *Joint Task Force – Computer Network Defense (JTF-CND)*), kurių pagrindinis uždavinys buvo apsaugoti JAV Gynybos departamento kompiuterinius tinklus. Šios pajėgos buvo įkurtos reaguojant į 1997 ir 1998 m. pratybose nustatytus kompiuterinių tinklų pažeidžiamumus ir identifikavus, kad Gynybos departamente nėra koordinuojančio elemento, kuris rūpintųsi kompiuterinių tinklų apsauga (Blessing, 2020). Pradiniame etape JTF-CND padalinio vadovavimo ir kontrolės funkcijos pavestos JAV oro pajėgų vadui bei Gynybos informacinių sistemų agentūrai (anglų k. *Defense Information Systems Agency (DISA)*). Jau 1999 m. JTF-CND pasiekė pilną operacinį pajėgumą (anglų k. *Full operational capability*). JTF-CND formavimo etape buvo galvojama apie padalinio gebėjimą vykdyti kompiuterinių tinklų atakas, tačiau buvo abejojama ar galima tokiam mažam vienetui suteikti gana svarbius įgaliojimus puolamuojų operacijų vykdymui.

2000 m. JTF-CND padalinys buvo perkeltas JAV kosmoso pajėgų (anglų k. *U.S. Space Command (USSPACECOM)*) pavaldumui ir tokiu būdu gavo įgaliojimus vykdyti kompiuterinių tinklų atakas. Vėliau 2001 m., JTF-CND padalinio vaidmuo tik stiprėjo, prasiplėtė ir jo uždavinys: JTF-CND nebebuvo vien tik atsakingas už kompiuterinių tinklų gynybą, oficialiu mandatu įgalino vykdyti ekploatacijos (anglų k. *Exploitation*)[10] ir puolimo operacijas. Siekiant atspindėti minėtus padalinio įgaliojimus, jis buvo pervadintas į kompiuterinių tinklų operacijų jungtines užduoties vykdymo pajėgas (anglų k. *Joint Task Force – Computer Network Operations (JTF-CNO)*). 2004 m. Patvirtinus Nacionalinę karinę strategiją, kurioje netiesiogiai nurodyta, kad kibernetinė erdvė palyginama su tradicinėmis karinėmis sritimis, JTF-CNO toliau vystėsi ir buvo pervadintas į globalų tinklų operacijų jungtines užduoties vykdymo pajėgas (anglų k. *Joint Task Force – Global Network Operations (JTF-GNO)*).

2005 m. atsakomybės vykdyti kompiuterinių tinklų operacijas buvo išdalintos: už kompiuterinių tinklų atakų vykdymą paskirta jungtinė funkcinė komponento vadavietė – tinklų kovos (anglų k. *Joint Functional Component Command – Network Warfare (JFCC-NW)*), kuriam vadovavimo įgaliojimus turėjo JAV Strateginė vadovybė (anglų k. *United States Strategic Command (USSTRATCOM))*. Kompiuterinių tinklų gynybos funkcijas toliau atliko JTF-GNO padalinys, kuriam vadovavo USSTRATCOM ir Gynybos

[10] Kibernetinės erdvės eksploatavimo (panaudojimo) veiksmai apima karinės žvalgybos veiklą, manevrą, informacijos rinkimą ir kitus veiksmus, reikalingus pasirengti būsimoms karinėms operacijoms.

ir Informacinių sistemų agentūra (anglų k. *Defense Information Systems Agency (DISA)*). JAV oro pajėgų vadovybė ėmėsi iniciatyvos toliau vystyti kibernetinius pajėgumus ir 2005 m. performulavo misiją: „skristi ir kovoti ore, kosmose ir kibernetinėje erdvėje“. Siekiant įgyvendinti naują uždavinį JAV oro pajėgose įkurtas Kibernetinės erdvės užduoties vykdymo pajėgos (anglų k. *Cyberspace Task Force*), kurių tikslas buvo teikti rekomendacijas strategijų, operacinių koncepcijų ir doktrinų vystymui (Porche ir kt., 2017). 2006 m. idėja įsteigti atskirą vadovybę kibernetinei misijai oro pajėgose pradėjo materializuotis. Kibernetinės erdvės užduoties vykdymo pajėgos parengė dvi opcijas tolimesniam kibernetinių pajėgų vystymui: įkurti vienetą, kuris būtų pavaldus pagrindinei vadovybei (anglų k. *Major Command*) arba vienetą, tolygų pagrindinei vadovybei (Galvin, 2018). Pasirinkta opcija formuoti atskirą pagrindinę vadovybę vien oro pajėgų vieneto pagrindu (Eighth Air Force). 2007 m. priimtas sprendimas aktyvuoti laikiną Oro pajėgų kibernetinės erdvės vadovybę (anglų k. *Air Force Cyberspace Command (Provisional) AFCYBER(P)*) kaip naują pagrindinę vadovybę, kuri turėjo konsoliduoti turimus kibernetinius pajėgumus. Naujai įsteigta vadovybė turėjo įsteigti tris komponentus: tradicinį elektroninių ryšių, elektroninės ir tinklų kovos. Tačiau nesutarimai oro pajėgų viduje dėl naujos AFCYBER(P) atsakomybės ir funkcijų, spaudimo iš Gynybos ministerijos bei oro pajėgų vadovybės pasikeitimai suspendavo AFCYBER(P) veiklą. Tuo pat metu kai oro pajėgos vystė AFCYBER(P) projektą, idėja apie jungtinį (ne vienos pajėgų rūšies) požiūrį į kibernetinę erdvę sulaukė palaikymo ir Gynybos ministerijoje.

2007 m. JAV planas panaudoti puolamąsias kibernetines priemones prieš sukilėlius Irake (Schulze, 2020) palankiai buvo sutiktas JAV prezidento, kuris pritarė platesniam kibernetinių priemonių panaudojimo planui. 2008 m. išleista Prezidento nacionalinė saugumo direktyva (anglų k. *National Security Presidential Directive (NSPD)*) paspartino Nacionalinės kibernetinio saugumo iniciatyvos (anglų k. *Comprehensive National Cybersecurity Initiative*) įgyvendinimą, kuri numatė federalinės valdžios funkcijas ir atsakomybes kibernetinio saugumo srityje (Starr ir kt., 2018). Svarbu paminėti, kad Prezidento nacionalinė saugumo direktyva suteikė pagrindą ir impulsą Gynybos departamentui įvertinti esamą kariuomenės jungtinę užduoties vykdymo pajėgų struktūrą kompiuterinių tinklų operacijų vykdymui. Tuo pat metu buvo atlikti Gynybos departamento kibernetinių pajėgumų tyrimai, kurie parodė, kad gynybos departamentas buvo nepakankamai pasirengęs kovai su kibernetinėmis grėsmėmis. Tuometinė kibernetinės erdvės jungtinių užduoties vykdymo pajėgų struktūra užtikrino specialistų ekspertizę tik vienose pajėgose, jungtinių užduoties vykdymo vienetų vadai dažniausiai neturėjo nei resursų nei įgaliojimų koordinuotis su kitomis pajėgomis. Po išsamiai atliktos analizės, kilo keli klausimai dėl karinių kibernetinių pajėgų: pirmiausia, ar kariuomenė turėtų išlaikyti pagrindinę atsakomybę kibernetinėje srityje, koks yra tinkamas karinis organizacinis modelis, kokie potencialūs vadovavimo įgaliojimai ir naujai sukurtų karinių organizacijų ryšys su Nacionaline saugumo agentūra (anglų k. *National Security Agency*). Po ilgų diskusijų buvo

nuspręsta 2010 m. įkurti Kibernetinių pajėgų vadovybę (anglų k. *U.S. Cyber Command (USCYBERCOM*)) sujungiant JTF–GNO (atsakingą už kibernetinės erdvės gynybines operacijas) ir JFCC-NW (atsakingą už puolamųjų kibernetinių operacijų planavimą). USCYBERCOM pavaldume taip pat buvo įkurti kibernetiniai vienetai visose pajėgose: U.S. Army Cyber Command (ARCYBER), Air Forces Cyber (AFCYBER), Fleet Cyber Command (FLTCYBER), and the U.S. Marine Corps Forces Cyberspace Command (MARFORCYBER). Nepaisant to, vadovavimo grandinėje USCYBERCOM liko pavaldus strateginei vadovybei (anglų k. *U.S. Strategic Command (USSTRATCOM)*). Taip pat siekiant apjungti puolamųjų ir gynybinių kompiuterinių tinklų operacijų vykdymą, nuspręsta, kad vadovauti USCYBERCOM ir NSA turi vienas pareigūnas.

Įsteigus USCYBERCOM, vidinės diskusijos dėl kibernetinių operacijų vykdymo atsakomybių tarp Gynybos departamento ir Centrinės žvalgybos agentūros (anglų k. *Central Intelligence Agency*) buvo tęsiamos: kas turėtų imtis vadovaujančio vaidmens kovoje prieš al-Qaeda taikinius? Gynybos departamentas kibernetinę operaciją matė kaip dalį antiteroristinės operacijos, tačiau Centrinės žvalgybos agentūra įvardijo tai kaip slaptas žvalgybines operacijas.

Tolesnę USCYBERCOM evoliuciją sąlygojo sekantys veiksniai:

2011 metais Gynybos departamentas oficialiai kibernetinę erdvę pripažino kaip operacijų sritį išleisdamas Veikimo kibernetinėje erdvėje strategiją (anglų k. *Strategy for Operating in Cyberspace*). 2013 metais išleista kibernetinės erdvės doktrina[11], kurioje buvo pateiktos tolesnės gairės dėl kompiuterinių tinklų operacijų vaidmens, atsakomybių, planavimo ir koordinavimo procesų, taip pat pagrindas tolesnei doktrinos plėtrai.

2014 m. Rusijai aneksuojant Krymą, JAV kariuomenės ekspertai pastebėjo reikšmingą puolamųjų kibernetinių operacijų naudojimą taktiniame lygmenyje bei kombinuotą kompiuterinių tinklų, elektroninės kovos (anglų k. *Electronic warfare (EW)*) ir konvencinių operacijų integravimą. Šios Rusijos vykdytos operacijos smarkiai skyrėsi nuo įvykdytų 2007 m. Estijoje ir 2008 m. Gruzijoje kada buvo naudojamos paskirstyto atkirtimo nuo paslaugų atakos (anglų k. *Distributed denial of service (DDoS*))[12], išpuoliai buvo nukreipti prieš elektros tinklus ir kitas fizines sistemas, taip pat priešo pajėgų judėjimo realiu laiku stebėjimas sukompromituojant karių mobilius telefonus (Blessing, 2020).

2016 m. USCYBERCOM sėkmingai įvykdyta operacija „Glowing Symphony“ prieš „Islamo valstybės“ teroristinę organizaciją, kurios metu buvo sukompromituotos Islamo respublikos (anglų k. *Islamic State of Iraq and Syria (ISIS*)) internete naudojamos žiniasklaidos priemonės, sunaikinti serveriai Vokietijoje, taip pat sutrikdyti ISIS narių pajėgumai bendrauti ir skelbti propagandą. Prieš vykdant šią

[11] Joint Publication 3-12, Cyberspace Operations.
[12] DDoS (distributed denial-of-service) - tai paskirstyta atkirtimo nuo paslauos ataka, kai auką puola daug kompiuterių.

operaciją daugelis Gynybos departamento vadų ir civilių iš esmės nesuprato ISIS vykdytų operacijų kibernetinėje erdvėje bei USCYBERCOM kibernetinių puolamųjų galimybių. Operacija „Glowing Symphony“ tik patvirtino kibernetinių pajėgumų panaudojimo koncepciją – kompiuterinių tinklų operacijų integravimas į tradicines karines operacijas, taip pat skaitmeninis užpuolimas toliau paskatino persvarstyti konfliktus kibernetinėje erdvėje ir tai, kaip USCYBERCOM galėtų sąveikauti su kitomis pajėgomis. Taip pat pasitvirtino ir vieno vadovaujančio asmens dviejoms organizacijoms struktūra: iš pradžių tokia organizacinė struktūra stabdė USCYBERCOM plėtrą, tačiau operacija „Glowing Symphony“ parodė svarbų kariuomenės ir tarpžinybinį koordinacijos efektyvumą kibernetinėje srityje.

Stiprėjantis USCYBERCOM vaidmens kibernetinėje erdvėje pripažinimas nulėmė tai, kad 2018 m. USCYBERCOM pripažinta kaip kovinė vadovybė (anglų k. *combatant command*)[13].

Pagrindiniai USCYBERCOM pavaldūs elementai: 2012 m. Jungtinis štabas ir JAV kibernetinė vadovybė (USCYBERCOM) nurodė pajėgoms bendrai sukurti kibernetinių užduočių vienetą (anglų k. *Cyber Mission Force (CMF)*), susidedantį iš 133 kibernetinių užduočių komandų (anglų k. *Cyber Mission Teams (CMT)*), keturių Jungtinių pajėgų štabų (anglų k. *Joint Force Headquarters-Cyber*) ir vieno nacionalinių kibernetinių užduočių vieneto (anglų k. *Cyber National Mission Force(CNMF)*)[14]. Pagrindiniai CMF uždaviniai yra sekantys: pirma, vykdyti gynybines kibernetinės erdvės operacijas – užduotys skirtos išlaikyti galimybę draugiškoms pajėgoms naudotis kibernetine erdve, apsaugoti duomenis, tinklus, tinklą naudojančius pajėgumus ir kitas sistemas; antra, vykdyti puolamąsias kibernetinės erdvės operacijas – užduotys skirtos demonstruoti galią (anglų k. *Project power*) kibernetinėje erdvėje; trečia, vykdyti Gynybos departamento informacinių tinklų operacijas – užduotys, skirtos planuoti, kurti, konfigūruoti, apsaugoti, valdyti, prižiūrėti ir palaikyti ginkluotųjų pajėgų informacinius tinklus ir remiančius tinklus. CMF nustatytus uždavinius vykdo paskirstydamas užduotis sekančiai:

a) Nacionalinės kibernetinių užduočių komandos (anglų k. *Cyber National Mission Teams(CNMT)*) vykdo šalies gynybą sekdamos priešininkų veiklą, blokuodamos atakas ir manevruodamos kibernetinėje erdvėje siekiant jas nugalėti,
b) Kibernetinės kovos komandos (anglų k. *Cyber Combat Mission Teams(CCMT)*) vykdo karines kibernetines operacijas remdamos kovines vadovybes,
c) Kibernetinės apsaugos komandos (anglų k. *Cyber Protection Teams(CPT)*) vykdo Gynybos departamento informacinių tinklų gynybą, saugo prioritetines misijas ir rengia kibernetinį personalą kovos veiksmams,

[13] Kovinė vadovybė (anglų k. *combatant command*) – tai jungtinė JAV gynybos departamento karinė vadovybė, kurią sudaro dviejų ar daugiau ginkluotųjų pajėgų vienetai.
[14] 2018 m CNMF komandos pasiekė pilną operacinį pajėgumą.

d) Kibernetinės paramos komandos (anglų k. *Cyber Support Teams(CST)*) teikia analitinę ir planavimo paramą Nacionalinėms kibernetinių užduočių ir Kovos komandoms.

Reguliarios kibernetinės atakos vykdomos prieš JAV tebėra ties ginkluoto konflikto „raudona linija“, siekiant kad būtų išvengta ginkluotųjų pajėgų atsako. Dėl to, kad į kibernetines atakas neįmanoma reaguoti už kibernetinės erdvės ribų, JAV nusprendė prieš priešininkus gintis aktyviai ir prevenciškai. Toks požiūris apriboja priešininkų veiksnumą, eikvoja jų išteklius, verčia sutelkti dėmesį į savo gynybą ir galiausiai atbaido juos nuo tam tikrų puolamųjų veiksmų (Marrone ir Sabatino, 2021). Naujoje CYBERCOM vizijoje „pasiekti ir išlaikyti pranašumą kibernetinėje erdvėje siekiant įtakoti priešininko elgesį..“ pabrėžiamas pranašumo kibernetinėje erdvėje išlaikymas, kurį pasiekti JAV mato per nuolatinį buvimą kibernetinėje erdvėje. Nuolatinis priešininko įtraukimas į „kovą“ negali būti sėkmingas, jei veiksmai bus apriboti tik Gynybos departamento tinkluose – siekiant apginti kritinius karinius ir nacionalinius interesus, JAV pajėgos privalo taip pat vykdyti operacijas prieš priešininkus jų virtualioje vietovėje (Nakasone, 2019).

4. LIETUVOS KARIUOMENĖS KIBERNETINIŲ GYNYBOS PAJĖGŲ BRANDOS TYRIMAS

4.1. Tyrimo metodologija

Teorinėje dalyje išnagrinėti reikalavimai kibernetinės gynybos vystymui nacionalinio saugumo ir kibernetinio saugumo strategijose, skirtingų institucijų atsakomybės kibernetinio saugumo politikos formavime ir įgyvendinime, nustatytų strateginių ir operacinių tikslų pasiekimas kibernetinėje erdvėje bei atsakomybės už kariuomenės kibernetinės gynybos pajėgumų vystymo įgyvendinimą. Taip pat išnagrinėti įvairūs kibernetinių pajėgumų vertinimo modeliai.

Tyrimo problema. *Ar LK kibernetinės gynybos pajėgumai pakankami siekiant užtikrinti efektyvią LK kibernetinės erdvės gynybą?*

Tyrimo tikslas: nustatyti LK kibernetinės gynybos pajėgumų brandos lygį ir pateikti su šia sritimi susijusius pasiūlymus.

Tyrimo uždaviniai:

1. Nustatyti LK kibernetinės gynybos pajėgumų vystymo sričių privalumus ir trūkumus.
2. Pateikti rekomendacijas LK kibernetinės gynybos pajėgumų vystymui.

Tyrimo metodai: tyrimui atlikti pasirinkta kiekybinio tyrimo strategija atliekant ekspertų apklausą. Apklausos klausimynas sudarytas pritaikant RAND korporacijos sukurtą kibernetinių pajėgumų brandos vertinimo modelį (Robinson ir kt., 2012). Kiekybinio tyrimo strategijai buvo taikomi šie duomenų analizės metodai: kiekybinė ir kokybinio turinio analizė (anglų k. *Content*) bei lyginamoji duomenų analizė.

Tyrimo imtis: Tyrimo imčiai taikyta netikimybinė tikslinė atranka. Informantais tikslingai parinkti Krašto apsaugos sistemos strateginiame, operaciniame ir taktiniame lygiuose dirbantys kibernetinio saugumo specialistai (N=7), kurių funkcijos tiesiogiai susiję su kariuomenės kibernetinės gynybos pajėgumų vystymu ir įgyvendinimu.

Tyrimo ribotumas:

a) ribotas kiekis kibernetinio saugumo/gynybos specialistų, dirbančių KAS su LK kibernetinės gynybos pajėgumų vystymu/įgyvendinimu;
b) detali informacija, susijusi su LK kibernetinės gynybos pajėgumų vystymu, yra įslaptinta.

Tyrimo dizainą sudaro trys pagrindiniai etapai:

Pirmasis etapas - tyrimo loginis pagrindimas, remiantis mokslinės literatūros teorinėmis įžvalgomis, kurios atskleidžia kibernetinės gynybos sampratą, kibernetinės gynybos nacionalinėje gynybos ir kibernetinio saugumo strategijoje bei kibernetinio saugumo valdymas ir atsakomybės, identifikuoja kibernetinių pajėgumų vertinimo modelius.

Antrame etape pagrindžiama tyrimo organizavimo metodika atliekant tyrimą, taikant kiekybinio tyrimo strategiją. Atliekama kokybinė mokslinės literatūros ir dokumentų turinio analizė bei organizuojama apklausa.

Trečiame etape naudojantis apklausos rezultatais, nustatomas Lietuvos kariuomenės kibernetinių pajėgumų brandos lygis bei identifikuojamos šio pajėgumo tobulinimo sritys.

Tyrimo kriterijai:

Tyrimo kriterijus sudarė atskiros pajėgumų vystymo sritys pagal DORSAPLIS: Doktrina, Organizavimas, Rengimas, Sistema, Aprūpinimas, Personalas, Lyderystė, Infrastruktūra ir Sąveikumas.

1. Doktrininės dalies *indikatoriai, kuriais tikrinamas kriterijus:* šių strategijų egzistavimas: kibernetinio saugumo, nacionalinės ypatingos svarbos informacinės infrastruktūros, kibernetinės gynybos ir tarptautinės kibernetinės; doktrinų egzistavimas: operacijų kompiuteriniuose tinkluose, kibernetinės gynybos ir kibernetinio atgrasymo; taip pat įtvirtinta nuostata, kad kibernetinė ataka laikoma ginkluota ataka.

2. Organizavimo dalies *indikatoriai, kuriais tikrinamas kriterijus:* nacionalinės iniciatyvinės (valdymo) grupės ir operacinio lygmens kibernetinio saugumo organizacijos kariuomenėje egzistavimas; Kibernetinio saugumo (gynybos) organizacijos, atsakingos už gynybines ir puolamąsias operacijas kibernetinėje erdvėje egzistavimas; Kibernetinio saugumo (gynybos) padalinio ryšys su nacionaliniais pajėgumais, dirbančiais kovos su elektroniniais nusikaltimais srityje; ryšys su CERT bei ekspertų iš kitų organizacijų turėjimas; ekspertų iš privataus sektoriaus buvimas kibernetinio saugumo (gynybos) padalinyje ir kibernetinio saugumo (gynybos) padalinio ryšių palaikymas su kitomis atsako į incidentus organizacijomis.

3. Rengimo dalies *indikatoriai, kuriais tikrinamas kriterijus:* kibernetinis saugumas kaip mokymo dalykas vadovaujančio lygmens kursuose ir kibernetinės gynybos specialistų rengimas/karjeros kelio egzistavimas; Kibernetinio saugumo (gynybos) padalinio dalinimasis gerąja praktika/įgyta patirtimi su kitomis institucijomis; nacionalinio lygio įdarbinimo konkursų vykdymas ir dalyvavimas ES/NATO pratybose.

4. Sistemos ir aprūpinimo dalies *indikatoriai, kuriais tikrinamas kriterijus:* karinių kibernetinių gynybos pajėgumų priklausomybė nuo privačių išteklių ir privataus sektoriaus vaidmuo karinių kibernetinių gynybos pajėgumų veikloje bei technologinių priemonių naudjimas.

5. Personalo dalies *indikatoriai, kuriais tikrinamas kriterijus:* pagrindinis indikatorius - kibernetinės gynybos specialistų įdarbinimas ir jų išlaikymas. Kiti indikatoriai susiję su personalo valdymu - tapatybės ir prieigos valdymas, grėsmės iš vidaus valdymas, personalo patikrinimas ir užtikrinimas, rangovų ir trečiųjų šalių tikrinimas, “Juodų” ar “pilkų” kepurių verbavimas ir įdarbinimas.

6. Lyderystės dalies *indikatoriai, kuriais tikrinamas kriterijus:* pagrindinis šios srities indikatorius yra autorizavimas naudoti kibernetinės gynybos pajėgumus strateginiame lygmenyje, po to pagal svarbą operaciniame ir galiausiai taktiniame lygmenyse. Kitas svarbus indikatorius yra aiškiai nustatytas nacionalinių incidentų eskalavimo mechanizmas ir paskutinis indikatorius yra leidimo privataus sektoriaus tinklų stebėjimui suteikėjas.

7. Infrastruktūros dalies *indikatoriai, kuriais tikrinamas kriterijus:* pagrindinis šios srities indikatorius – nacionalinio lygmens kriminalistinių tyrimų infrastruktūros turėjimas, taip pat svarbūs indikatoriai – nacionalinės interaktyvios technologijų aplinkos (pvz. laboratorijos) egzistavimas bei infrastruktūra kibernetinės gynybos organizavimui. Mažiausiai reikšmingas indikatorius - infrastruktūra puolamųjų kibernetinių pajėgumų vystymui ir testavimui.

8. Sąveikumo dalies *indikatoriai, kuriais tikrinamas kriterijus:* šioje srityje svarbiausi indikatoriai – ar kibernetinio saugumo (gynybos) padalinyje įdiegta įmonės sąveikos sistema (anglų k. *Enterprise interoperability framework*) ir sąveikumo užtikrinimas strateginiame lygmenyje. Taip pat ne mažiau svarbus indikatorius yra ar įmonės sąveikos sistema bendra su kitomis valdžios institucijomis?

Tyrimo organizavimas. Tyrime buvo pakviesti dalyvauti KAS kibernetinio saugumo/gynybos ekspertai naudojant tikslinę kriterinę imtį: dirbantys kibernetinio saugumo politikos formavime, jos įgyvendinimo koordinavime bei ekspertai tiesiogiai atsakingi už kibernetinės gynybos vykdymą. Tyrimas atliktas 2022 m. kovo mėn. informantus apklausiant raštu: apklausos klausimynai buvo išsiųsti el. paštu ir tiesiogiai dalyvaujant apklausoje. Informantams buvo pateiktas klausimynas pagal pajėgumų vystymo sritis DORSAPLIS (priedas Nr.1). Kadangi klausimai apima gana plačias pajėgumų vystymo sritis, ne visi informantai buvo susipažinę su kiekvienos pajėgumų srities specifika. Laikantis konfidencialumo, tyrime dalyvavę asmenys pristatomi priskiriant jiems kodus: informantas Nr.1 (I 1), informantas Nr.2 (I 2), informantas Nr.3 (I 3), informantas Nr.4 (I 4), informantas Nr.5 (I 5), informantas Nr.6 (I 6) ir informantas Nr.7 (I 7).

Tyrimas atliktas laikantis pagrindinių etikos principų: savanoriškumo, privatumo, anonimiškumo ir konfidencialumo (Kardelis, 2002). Tyrimo pradžioje buvo kreiptasi į ekspertus, pateikiant klausimyną ir nurodant, kad tyrimas atliekamas magistro baigiamojo darbo tema. Tyrimo dalyviai informuoti, kad jų pateikti atsakymai išliks anoniminiai, tyrimo duomenys bus pateikti tik apibendrinti, jie nebus naudojami kitiems tikslams, taip pat nebus nurodomi asmeniniai duomenys.

2 lentelė. Tyrimo ekspertai

Kodas	Institucija	Veiklos sritis
Informantas Nr.1	Lietuvos kariuomenės Ryšių ir informacinių sistemų batalionas	Kibernetinės gynybos vykdymas
Informantas Nr.2	Lietuvos kariuomenės Ryšių ir informacinių sistemų batalionas	Kibernetinės gynybos vykdymas
Informantas Nr.3	Lietuvos kariuomenės Ryšių ir informacinių sistemų batalionas	Kibernetinės gynybos vykdymas
Informantas Nr.4	Lietuvos kariuomenės Sausumos pajėgų štabas	Ryšių ir informacinės sistemos
Informantas Nr.5	Lietuvos kariuomenės Gynybos štabas	Kibernetinės gynybos politikos įgyvendinimo koordinavimas
Informantas Nr.6	Krašto apsaugos ministerija	Kibernetinio saugumo politikos formavimas
Informantas Nr.7	Krašto apsaugos ministerija	Kibernetinio saugumo politikos formavimas

4.2. Tyrimo rezultatų analizė ir interpretavimas

Tyrimo organizavimui, rezultatų įvertinimui ir LK kibernetinių gynybos pajėgumų brandos lygio nustatymui, remtasi RAND kibernetinių pajėgumų brandos vertinimo modelio (toliau - modelis). Kibernetinių pajėgumų brandos vertinimo modelį sudaro atskirose pajėgumų srityse nustatytos minimalios ribos pasiekti tam tikrą brandos lygį (*neegzistuojantis (B1), pradinis (B2), apibrėžtas* (B3), *subalansuotas (B4)* ir *optimizuotas (B5)*), taip pat nustatytos vertės perėjimui iš vieno brandos lygio į kitą (priedas Nr.2). Priklausomai nuo pajėgumo srities, kiekvienas klausimas įvertintas skirtinga verte. Pažanga kiekvienoje srityje nustatoma pagal minimalų taškų skaičių, reikalingą pereiti nuo vieno brandos lygio į kitą.

Pagal šį brandos vertinimo modelį, pajėgumų sritims „Doktrina“, „Organizavimas“ ir „Rengimas“ didesnė taškų vertė skiriama brandos lygiui esant anktyvoje stadijoje nei vėlesniame etape. Taip yra todėl, kad šiose pajėgumų srityse reikia daug laiko, išteklių ir pastangų norint apibrėžti ir pasiekti, kad visos suinteresuotosios šalys susitartų dėl bendros strategijos, organizacijos įgaliojimų ir vaidmens.

Pajėgumų sritims kaip „Lyderystė“ ir „Infrastruktūra“ remiantis vertinimo modeliu mažesnė taškų vertė skiriama ansktyvuose brandos lygiuose, tačiau vėlesniuose etapuose pažanga sudėtingėja, todėl skiriama taškų vertė yra didesnė.

„Sistema“ ir „Aprūpinimas“ pajėgumų srities (kuri visų pirma susijusi su technologinių sprendimų diegimu) brandos lygio progresija daugiau yra linijinė, darant prielaidą, kad technologija yra neutrali priemonė t.y. jos panaudojimą lemia personalo kvalifikacija ir gebėjimai.

Likusiose pajėgumų srityse „Personalas“ ir „Sąveikumas“ brandos progresas panašus į "S" kreivę, atitinkančią pirmų dviejų anksčiau aprašytų variantų kombinaciją.

Brandos lygiui nustatyti, skaičiavimai atlikti sekančia tvarka:

a) Indikatoriaus (klausimo) atsakymai sumuojami pagal informantų pateiktus atsakymus „Taip“, „Ne“, „Nežinau“, siekiant nustatyti daugiausia atsakymų turintį variantą. Teigiamas atsakymas į klausimą vertinamas tada, kai bent du ir daugiau informantų atsakymai teigiami ir bent du atsakymai neigiami, o likusieji pažymėti „Nežinau“. Taip yra dėl to, kad klausimynas apima gana platų spektrą pajėgumų vystymo sričių ir ekspertai, dalyvavę apklausoje negali turėti nuodugnių žinių visose srityse, o eksperto, išmanančio konkretų dalyką, balsas gali būti neužskaitytas.

b) Indikatoriai (klausimai), turintys skaitinę vertę, apskaičiuojami sumuojant kiekvieno indikatoriaus vertes (priedas Nr.3).

c) Indikatoriai (klausimai), kurie nurodyti brandos lygio skaitine išraiška nuo 1 iki 5, jų vertė apskaičiuojama pagal atitinkamos pajėgumos srities brandos lygio progreso skalėje nurodytas vertes (priedas Nr.2).

d) Kriterijaus (pajėgumų srities) vertė apskaičiuojama pagal formulę: *procentinė taškų suma = apskaičiuota taškų suma x 100% / didžiausia galima taškų suma*. Gauta procentinė taškų suma palyginama pagal brandos lygio progreso pagal pajėgumų sritis skalę (priedas Nr.2).

Doktrininė dalis apima dokumentus, nustatančius pagrindinius principus, kuriais vadovaujasi karinės pajėgos ar kariniai elementai, siekdami nacionalinių tikslų. Šios srities klausimyno dalį sudarė 8 klausimai. Vadovaujantis modelio reikalavimais, strategijos ir doktrinos išskiriamos pagal jų svarbą:

a) Kibernetinio Saugumo strategija (klausimas Nr.1), plataus masto nacionalinio lygmens dokumentas, kuriame turėtų būti nurodyta, kokios strategijos šalis turi imtis, kad taptų saugi kibernetinėje erdvėje, taip pat turėtų būti nurodyti gynybos tikslai, vaidmuo ir įgaliojimai siekiant strateginių saugumo tikslų. Visi informantai patvirtino šios strategijos egzistavimą.

b) Nacionalinė Ypatingos Svarbos Informacinės Infrastruktūros (YSII) strategija (klausimas Nr.3), kurioje aprašoma, kaip apsaugoti ypatingos svarbos informacijos infrastruktūrą ir infrastruktūros kibernetinės erdvės technologinius elementus, kurie yra esminiai užtikrinti socialinę ir ekonominę gerovę. Šios strategijos egzistavimą taip pat patvirtino visi informantai. Vadovaujantis metodikos reikalavimais, abiejų (kibernetinio saugumo ir YSII) strategijų egzistavimas užtikrina *pradinį (B2)* brandos lygį.

c) Kibernetinės Gynybos strategija (klausimas Nr. 2), kurioje turėtų būti nurodytas galutinis tikslas, kaip ginkluotosios pajėgos turėtų veikti siekdamos užtikrinti nacionalinių kibernetinio saugumo tikslų įgyvendinimą. 43% informantų nurodė, kad tokia strategija neegzistuoja, 28% informantų nežinojo apie šios strategijos egzistavimą, tačiau darė prielaidą, kad ji gali būti įslaptinta (I 6 ir I 7). Kadangi šio fakto patvirtinti neįmanoma, darytina išvada, kad ji neegzistuoja.

d) Kibernetinės Gynybos doktrina (klausimas Nr.7), kurioje turėtų būti apibrėžta kaip Kibernetinės Gynybos strategija galėtų būti įgyvendinta pasitelkiant įvairias priemones, įskaitant operacijas kompiuteriniuose tinkluose, informacinius veiksmus, informacijos dalijimąsi bei koordinavimą su kitomis valdžios institucijomis ir privačiu sektoriumi. 43% informantų nurodė, kad tokia doktrina neegzistuoja, o 57% apklaustųjų apie ją neturėjo duomenų.

e) Operacijų kompiuteriniuose tinkluose doktrinos (klausimas Nr.4), kuri turėtų būti kaip vadovas (anglų k. *handbook*), reglamentuojantis įvairių tipų operacijų kompiuteriniuose tinkluose vykdymą. 57% informantų paneigė tokios doktrinos egzistavimą, o 28% nebuvo susipažinę. Kibernetinės Gynybos strategijos ir Operacijų Kompiuteriniuose Tinkluose doktrinos egzistavimas užtikrintų perėjimą iš *pradinio (B2)* į *apibrėžtą (B3)* brandos lygį, tačiau šie dokumentai nėra parengti.

f) 57% informantų nurodė, kad Kibernetinio Atgrasymo doktrina (klausimas Nr. 5) neegzistuoja, o 43% apklaustųjų neturėjo duomenų.

g) Nuostatos, kad kibernetinė ataka laikoma ginkluota ataka (klausimas Nr. 6) negalėjo patvirtinti daugiau nei pusė (57%) informantų. Tačiau kiti informantai mano priešingai (I 2 ir I 7) ir linkę manyti, kad tokia nuostata egzistuoja. Atkreiptinas dėmesys, kad NATO šalys partnerės vieningai sutaria, kad kibernetinės atakos padaryta žala gali būti prilyginta konvencinės atakos padarytiems nuostoliams. Darytina prielaida, kad ši nuostata neužtvirtinta nacionaliniuose dokumentuose.

h) Tarptautinės kibernetinės strategijos egzistavimą (klausimas Nr. 8) patvirtino 86% informantų.

3 lentelė. Doktrinos pajėgumų srities atsakymų suvestinė

Pajėgumų Sritis	Atsakymų suvestinė	Brandos lygis				
		B1	B2	B3	B4	B5
DOKTRINA						
1. Kibernetinio Saugumo strategijos egzistavimas (Existence of CS strategy)	25		■			
2. Specifinės Kibernetinės Gynybos strategijos egzistavimas (Specific CD strategy)	0			■		
3. Nacionalinės Ypatingos Svarbos Informacinės Infrastruktūros strategijos egzistavimas (National Critical Information Infrastructure Protection strategy)	25		■			
4. Operacijų Kompiuteriniuose Tinkluose doktrinos egzistavimas (Computer Network OperationsDoctrine)	0			■		
5. Kibernetinio Atgrasymo doktrinos egzistavimas (Cyber deterrence doctrine)	0					■
6. Nuostata, kad kibernetinė ataka laikoma ginkluota ataka? (Cyber-attacks as armed attack?)	0					■
7. Kibernetinės Gynybos doktrinos egzistavimas (Cyber Defence Doctrine)	0				■	
8. Tarptautinės kibernetinės strategijos egzistavimas (International Strategy)	4.17					■
Bendra taškų suma	54.17					■

Išanalizavus doktrininės dalies rezultatus, gauta atsakymų taškų suma ir vertė procentais siekė 54.17%. Šią reikšmę palyginus su brandos lygių progreso lentele (priedas Nr.2), kur brandos lygiui B2 pasiekti reikalinga min. 50%, o B3 min. 75%. Darytina išvada, kad šios srities brandos lygis yra *pradinis (B2).*

Organizacinė dalis apima veiklai vykdyti reikalingų struktūrų įkūrimą ir įteisinimą bei nustato veiklos sritis. Vertinant šią pajėgumų sritį, svarbiausi indikatoriai, užtikrinantys perėjimą nuo *neegzistuojančio (B1)* brandos lygio iki *pradinio (B2)* yra egzistuojanti nacionalinio lygmens vadovybė arba koordinuojanti institucija (ministrų kabinetas / prezidento ar ministro pirmininko lygmuo) ir operacinio lygmens gynybos organizacija, kurios abi yra vienodai svarbūs šios pajėgumų srities aspektai ir abu jie yra būtini. Šios srities klausimyną sudarė 9 klausimai.

a) Į klausimą Nr. 1 „Nacionalinės iniciatyvinės (valdymo) grupės egzistavimas“ informantai vienbalsiai patvirtino, kad nacionaliniame lygmenyje egzistuoja tokia institucija (Kibernetinio saugumo taryba).

b) Dėl operacinio lygmens Kibernetinio saugumo organizacijos kariuomenėje egzistavimo (klausimas Nr.2) 66% informantų nurodė, kad tokia institucija egzistuoja. Atkreiptinas dėmesys, kad šios organizacijos atitikmuo Lietuvos kariuomenėje tenka LK GŠ RIS valdybos J6 Kibernetinės gynybos ir elektroninės informacijos saugos skyriui (I 5). Darytina išvada, kad

abiejų klausimų (Nr.1 ir Nr.2) atsakymai užtikrina perėjimą iš *neegzistuojančio(B1)* į *pradinį (B2)* brandos lygį.

c) Į klausimą Nr.3 „Kibernetinio saugumo (gynybos) organizacija atsakinga už gynybines operacijas kibernetinėje erdvėje“, 100 % atsakiusiųjų informantų patvirtino tokios institucijos egzistavimą. Institucija, atsakinga už šias funkcijas LK yra GŠ (I 5), kito informanto nuomone taikos metu šias funkcijas atlieka NKSC (I 1). Brados lygio nustatymui šis indikatorius turi gana svarią vertę.

d) Kibernetinio saugumo (gynybos) organizacija, atsakinga už puolamąsias operacijas kibernetinėje erdvėje (klausimas Nr. 4). 50 % informantų nurodė, kad tokia institucija egzistuoja, tačiau tai yra kitų, ne LK, institucijų – AOTD prie KAM (I 1, I 5) atsakomybė. Vertinant brandos lygį, organizacijos, atsakingos už gynybines operacijas egzistavimas yra dvigubai svarbesnis nei turėjimas institucijos, atsakingos už puolamąsias operacijas. Atsižvelgiant į vertinimo modelio nuostatas, gebėjimas vykdyti puolamąsias operacijas kibernetinėje erdvėje yra antraeilės svarbos dalykas nei gebėjimai vykdyti gynybines operacijas. Darytina išvada, kad abu indikatoriai (organizacijos, atsakingos už gynybos ir puolamąsias operacijas egzistavimas) tenkina *apibrėžto (B3)* brandos lygio reikalavimus.

e) Norint pereiti į *subalansuotą (B4)* brandos lygį, sekančių trijų indikatorių reikalavimai turėtų būti patenkinti:

1) ekspertų iš kitų organizacijų turėjimas kibernetinio saugumo (gynybos) padalinyje (klausimas Nr.5). 43% informantų patvirtino teiginį ir tiek pat informantų nesutiko su juo. Atkreiptinas dėmesys, kad padalinio funkcijoms užtikrinti, kviečiami aktyviojo rezervo kariai (I 1), todėl darytina išvada, kad ekspertai iš kitų organizacijų yra sudėtinė padalinio dalis;
2) kibernetinio saugumo (gynybos) padalinio ryšys su nacionaliniais pajėgumais, dirbančiais kovos su elektroniniais nusikaltimais srityje (klausimas Nr.7) informantų apklausoje pasiskirstė po lygiai (28% informantų) patvirtino ir tiek pat paneigė teiginį, o 43% apklaustųjų negalėjo įvardinti. Pažymėtina, kad LK GŠ deda pastangas, kad toks ryšys atsirastų (I 5) bei informantas Nr.7 nurodė, kad toks ryšys egzistuoja su Policijos departamentu. Apibendrinant galima teigti, kad šis indikatorius tenkina reikalavimus;
3) kibernetinio saugumo (gynybos) padalinio ryšį su Kompiuterinių incidentų tyrimo tarnyba (anglų k. *Computer Emergency Response Team (CERT)*) (klausimas Nr.8) teigiamai nurodė 86% informantai.

f) *Optimizuotam (B5)* brandos lygiui pasiekti reikalinga užtikrinti, kad kibernetinio saugumo (gynybos) padalinyje būtų ekspertai iš privataus sektoriaus (klausimas Nr. 6) - 43 % informantų šiam teiginiui pritarė. Atkreiptinas dėmesys, kad šie ekspertai yra aktyviojo rezervo kariai (I 1). Taip pat turi būti užtikrinti kibernetinio saugumo (gynybos) padalinio ryšiai su kitomis atsako į incidentus organizacijomis (klausimas Nr.9), kur 57 % informantų patvirtino šį faktą.

4 lentelė. Organizacijos pajėgumų srities atsakymų suvestinė

Pajėgumų Sritis	Atsakymų suvestinė	Brandos lygis				
		B1	B2	B3	B4	B5
ORGANIZACIJA						
1. Nacionalinės iniciatyvinės (valdymo) grupės egzistavimas (Existence of national steering group)	25		■			
2. Operacinio lygmens Kibernetinio saugumo organizacijos kariuomenėje egzistavimas (Cyber-security org in defence)	25		■			
3. Kibernetinio saugumo (gynybos) organizacija atsakinga už gynybines operacijas kibernetinėje erdvėje (Responsibility for defence)?	25			■		
4. Kibernetinio saugumo (gynybos) organizacija atsakinga už puolamąsias operacijas kibernetinėje erdvėje (Responsibility for offence)?	12.5			■		
5. Ar kibernetinio saugumo (gynybos) padalinyje yra ekspertų iš kitų organizacijų (Expertise from other orgs in unit)?	12.5				■	
6. Ar kibernetinio saugumo (gynybos) padalinyje yra ekspertų iš privataus sektoriaus (Expertise from private sector in unit)?	6.25					■
7. Kibernetinio saugumo (gynybos) padalinio ryšys su nacionaliniais pajėgumais, dirbančiais kovos su elektroniniais nusikaltimais srityje (Linked to national cybercrime capability)	12.5				■	
8. Kibernetinio saugumo (gynybos) padalinio ryšiai su CERT (Co-ordination (linked to n/g CERT))	12.5				■	
9. Kibernetinio saugumo (gynybos) padalinio ryšiai su kitomis atsako į incidentus organizacijomis (Linked to other incident response)	6.25					■
Bendra taškų suma	137.5					

Išanalizavus organizacinės dalies rezultatus, gauta atsakymų taškų suma ir vertė procentais siekė 100%. Darytina išvada, kad šios srities brandos lygis *optimizuotas (B5).*

Rengimo sritis apima reikalingų specialistų pradinį mokymą, kvalifikacijos palaikymą ir kėlimą, mokymų ir kursų naujam personalui rengimą. Vadovaujantis modelio reikalavimais, vienoda vertė skiriama klausimams susijusiems su kibernetinio saugumo dalyko mokymu vyresniųjų štabo karininkų kursuose bei kibernetinės gynybos specialistų rengimu. Šie abu faktoriai lemia *pradinį (B2)* brandos lygį. Analizuojant šios pajėgumų srities brandos lygį, kriterijų sudarė 7 indikatoriai.

a) Į klausimą Nr.1 „Kibernetinis saugumas kaip mokymo dalykas vadovaujančio lygmens kursuose“ 57% apklaustųjų nurodė neigiamai, 28% neturėjo duomenų ir tik vienas informantas (I 6) į klausimą atsakė teigiamai. Darytina prielaida, kad taktinio lygmens informantai galėjo ir nežinoti apie mokymo dalykus, dėstomus vyresniųjų karininkų kursuose.

b) Ne mažiau svarbu yra turėti kibernetinės gynybos specialistų karjeros kelią (klausimas Nr.2), kuriuo vadovaujantis specialistai gebėtų išlaikyti kvalifikaciją ir gebėjimus. Atsakymai į šį klausimą pasiskirstė sekančiai: 43% informantų sutiko su teiginiu, tačiau 57% apklaustųjų nurodė, kad specialistų rengimo/kvalifikacijos mechanizmo nėra.

c) Kibernetinio saugumo (gynybos) padalinio dalinimasis gerąja praktika/įgyta patirtimi su kitomis institucijomis (klausimas Nr.7) yra kitas svarbus šios srities indikatorius, turintis tokią pačią vertę kaip ir pirmi du klausimai. Informantų atsakymai pasiskirstė prieštaringai: 43% informantų nurodo, kad dalijimasis patirtimi nevyksta ir tiek pat apklaustųjų visgi pripažįsta, kad šis procesas organizuojamas. Atkreiptinas dėmesys, kad pagal 2022 m. KAM veiklos planą, numatyta „perduoti NKSC ir KAM ekspertų žinias ir patirtį Ukrainos ir Sakartvelo institucijoms kritinių infrastruktūrų apsaugos srityje” bei “teikti ekspertinę ir (ar) finansinę paramą ne mažiau kaip 3 NATO ir ES paramos iniciatyvos Rytų partnerystės šalims, ypač Ukrainai, Sakartvelui ir Moldovai” (I 7). Be to tas pats informantas nurodo, kad “tokia patirtis nuolat perduodama ES darbo grupėse, NKSC nuolat organizuoja mokymus valstybės institucijų darbuotojams, dalyvaujama konferencijose, dalyvaujama iniciatyvoje “Saugus internetas”, skirtoms mokykloms ir pan. NKSC publikuoja informaciją savo interneto svetainėje.” Apibendrinant darytina išvada, kad dalinimasis gerąja praktika/įgyta patirtimi su kitomis institucijomis vyksta.

d) 100% informantų sutiko su teiginiu, kad kibernetinio saugumo padalinys dalyvauja pratybose (klausimas Nr.3).

e) Kalbant apie kibernetinio saugumo (gynybos) padalinio ekspertų teorinę kvalifikaciją (klausimas Nr.4) susumavus informantų rezultatus, gautas *apibrėžtas (B3)* brandos lygis.

f) Informantų įvertinimai dėl kibernetinio saugumo (gynybos) padalinio ekspertų praktinės kvalifikacijos (klausimas Nr.5) siekė taip pat *apibrėžtą (B3)* brandos lygį.

g) Į klausimą Nr.6 „Ar vykdomi nacionalinio įdarbinimo konkursai?“, 43% informantų išsakė neigiamą nuomonę, 28% informantų teigimu yra vykdomi įdarbinimo konkursai. Atkreiptinas dėmesys, kad valstybės tarnautojų ir darbuotojų, dirbančių pagal darbo sutartį pareigybėms užimti (jei tokių yra LK kibernetinio saugumo/gynybos padalinyje) konkursai organizuojami teisės aktų nustatyta tvarka.

5 lentelė. Rengimo pajėgumų srities atsakymų suvestinė

Pajėgumų Sritis	Atsakymų suvestinė	Brandos lygis				
		B1	B2	B3	B4	B5
RENGIMAS						
1.Kibernetinis saugumas kaip mokymo dalykas vadovaujančio lygmens kursuose (pvz. vyresniųjų štabo karininkų kursuose) (CS covered in syllabus at command level)?	0					
2.Kibernetinės gynybos specialistų rengimas/karjeros kelias (Specific CD training competency /career path or skillsprofile)?	0					
3.Dalyvavimas pratybose (Participation in exercises)	12.5					
4.Kibernetinio saugumo (gynybos) padalinio ekspertų teorinė ekspetizė (Estimate of theoretical expertise at national level)?	75			3		
5.Kibernetinio saugumo (gynybos) padalinio ekspertų praktinė ekspertizė (Estimate of applied expertise atnational level)?	75		3			
6.Ar vykdomi nacionalinio lygio įdarbinimo konkursai (Conduct national level recruitment competitions)?	0					
7.Kibernetinio saugumo (gynybos) padalinio dalinimasis gerąja praktika/įgyta patirtimi su kitomis institucijomis (Sharing good practice / Lessons learned)?	25					
Bendra taškų suma	187.5					

Išanalizavus rengimo dalies rezultatus, gauta atsakymų taškų suma ir vertė procentais siekė 62,5%. Šią reikšmę palyginus su brandos lygių progreso lentele (priedas Nr.2), brandos lygiui B2 pasiekti reikalinga min. 50%, o B3 min. 75%. Darytina išvada, kad šios srities brandos lygis yra *pradinis (B2)*.

Sistemų ir aprūpinimo sritis apima būtiniausias priemones, reikalingas pajėgumui (LK vienetams/ KAS institucijoms) efektyviai veikti. Esminis šios srities indikatorius yra karinių kibernetinių gynybos pajėgumų priklausomybė nuo privačių išteklių (klausimas Nr.1), kur 64% informantų įvertino teigiamą priklausomybę. Ši priklausomybė daugiau siejama su programine įranga (I 2). Visgi 33% apklaustųjų nurodė neigiamą priklausomybę.

Privataus sektoriaus vaidmuo karinių kibernetinių gynybos pajėgumų veikloje (klausimas Nr.2) pasak apklaustųjų įtakos neturi, atsakymų vidurkis siekė 3 balus (skalėje nuo 1-5, kur 1 = nėra kritinis ir 5 = kritinis).

Pagal priemonių naudojimo lygmenį (klausimas Nr.3), nustatytas brandos lygis yra *apibrėžtas (B3)* (rezultatas gautas apskaičiavus brandos lygių vidurkį). Atkreiptinas dėmesys, kad priemonių naudojimo efektyvumas priklauso nuo kitų pajėgumo sričių: pvz. blogai sukonfigūruota moderni ugniasienė gali labiau pakenkti saugumui nei mažiau moderni technologija, kurią įdiegė ir gerai valdo aukštos kvalifikacijos darbuotojai.

6 lentelė. Sistemos ir aprūpinimo pajėgumų srities atsakymų suvestinė

Pajėgumų Sritis	Atsakymų suvestinė	Brandos lygis				
		B1	B2	B3	B4	B5
SISTEMA, APRŪPINIMAS						
1.Karinių kibernetinių gynybos pajėgumų priklausomybė nuo privačių išteklių (Reliance upon privately owned assets)	Taip					
2.Privataus sektoriaus vaidmuo karinių kibernetinių gynybos pajėgumų veikloje (Perception of role of private sector)	3					
3.Priemonių naudojimo lygmuo (Degree of usage of):						
a) Perimetru pagrįstos priemonės (pvz. ugniasienė) (Perimeter based measures)	100					5
b) Daugiasluoksnė „Gynybos į gylį“ koncepcija (Defence in depth)	75				4	
c) Viešojo rakto infrstruktūra (Public Key Infrastructure)	50			3		
d) Veiklos atkūrimo priemonės (Disaster recovery tools)	50			3		
e) Duomenų praradimo prevencija (Data Loss Prevention)	50			3		
f) Grėsmių žvalgyba ir duomenų apjungimo (Threat intelligence & data fusion)	25		2			
g) Duomenų vizualizavimas (Data visualization)	25		2			
h) Įsilaužimo prevencija (Intrusion prevention)	50			3		
j) Įsilaužimo stebėjimas ir apsauga nuo grėsmių (Honeypots/honeynets)	50			3		
k) Saugus susirašinėjimas/duomenų apsikeitimas (Secured messaging / data exchange)	75				4	
l) Kriminalistikos platformos (Forensic platforms)	25		2			
Bendra taškų suma	575					

Išanalizavus sistemos ir aprūpinimo dalies rezultatus, gauta atsakymų taškų suma ir vertė procentais siekė 52,7%. Šią reikšmę palyginus su brandos lygių progreso lentele (priedas Nr.2), brandos lygiui B3 pasiekti reikalinga min. 50%, o B4 min. 75%. Darytina išvada, kad šios srities brandos lygis yra *apibrėžtas (B3)*.

Personalo organizavimo dalis apima būtino kvalifikuoto (karinio) personalo pareigybes (specialybių), reikalingas pajėgumui (LK vienetams / KAS institucijoms) efektyviai veikti bei kvalifikuoto personalo išlaikymą. Atsižvelgiant į modelio reikalavimus, didžiausia vertė tenka indikatoriui, susijusiam su įdarbinimu ir kibernetinės gynybos specialistų išlaikymu (klausimas Nr.1), nes tai gali būti laikoma svarbiu mechanizmu, padedančiu pritraukti ir išlaikyti aukštos kvalifikacijos talentus kariuomenės kibernetinės gynybos pajėgumuose. 57% informantų nurodė, kad tokio mechanizmo nėra, tačiau 43% apklaustųjų pripažino, kad specialistų įdarbinimo ir išlaikymo mechanizmas egzistuoja. Informantai

pripažįsta, kad specialistų išlaikymas yra probleminė sritis (I 2) ir kad nėra svertų kaip minėtus specialistus išlaikyti (I 3).

2-6 klausimų apskaičiuotos vertės pateiktos lentelėje apačioje. Dėl „juodų“ ar „pilkų“ kepurių verbavimo ir įdarbinimo (klausimas Nr. 6), pažymėtina, kad teisiškai šie procesai yra reglamentuoti, tačiau praktikoje jie neveikia (I 1). „Juodos“ kepurės žinomos kaip piktavaliai įsilaužėliai, kurių pagrindinė motyvacija yra kolektyvinė, asmeninė ar finansinė nauda. „Pilkos“ kepurės – tai saugumo tyrėjai, korporacijos ar mėgėjai, kurie laviruoja tarp etiško ir neteisėto įsilaužimo.

7 lentelė. Personalo pajėgumų srities atsakymų suvestinė

Pajėgumų Sritis	Atsakymų suvestinė	Brandos lygis				
		B1	B2	B3	B4	B5
PERSONALAS						
1.Kibernetinės gynybos specialistų įdarbinimo ir išlaikymo mechanizmas (Recruitment and Retention for CD specialists)	0					
2. Tapatybės ir prieigos valdymas (Identity and Access Management)	87.5				4	
3. Grėsmės iš vidaus valdymas (Insider Threat Management)	87.5				4	
4.Personalo patikrinimas ir užtikrinimas (Personnel Vetting and assurance)	100					5
5. Rangovų ir trečiųjų šalių tikrinimas (Vetting contractors and third parties)	87.5				4	
6. 'Juodų' ar 'pilkų' kepurių verbavimas ir įdarbinimas? (Recruitment and employment of 'black' or 'grey' hats?)	0	1				
Bendra taškų suma	362.5					

Išanalizavus personalo dalies rezultatus, gauta atsakymų taškų suma ir vertė procentais siekė 61,7%. Šią reikšmę palyginus su brandos lygių progreso lentele (priedas Nr.2), brandos lygiui B3 pasiekti reikalinga min. 37,5%, o B4 – min. 87,5%. Darytina išvada, kad šios srities brandos lygis yra *apibrėžtas (B3).*

Lyderystės sritis apima visų lygmenų vadų, reikalingų pajėgumui (LK vienetams / KAS institucijoms) efektyviai veikti, parengimo lygį. Vertinant šią pajėgumų sritį, svarbiausias indikatorius yra strateginio lygmens autorizavimas panaudoti kibernetinės gynybos pajėgumus, vidutiniškai svarbus operacinio lygmens ir mažiausiai svarbus – taktinio lygmens (klausimas Nr.1). Taip yra dėl galimų nenumatytų pasekmių panaudojus šiuos pajėgumus ir poreikio turėti aiškų suvokimą aukščiausiame lygyje kaip reaguoti į nacionalinio lygmens incidentus. Informantų atsakymai pasiskirstė sekančiai: 28% apklaustųjų nurodė, kad autorizavimas yra strateginiame lygmenyje, 43% operaciniame lygmenyje ir 57%

galvoja, kad leidimas galimas taktiniame lygmenyje. Darytina prielaida, kad aiškaus atsakomybių atsidalinimo priimant sprendimą dėl kibernetinės gynybos pajėgumų panaudojimo nėra.

57% informantų patvirtino, kad yra aiškus nacionalinių incidentų eskalavimo mechanizmas (klausimas Nr.2). Šis indikatorius pagal svarbą yra toks pat svarbus kaip ir gebėjimas strateginiame lygmenyje autorizuoti kibernetinių gynybos pajėgumų panaudojimą.

43% apklaustųjų mano, kad reikalinga teismo nutartis norint gauti leidimą privataus sektoriaus tinklų stebėjimui (klausimas Nr.3). Atkreiptinas dėmesys, kad tokiu atveju NKSC diegia sensorius YSII sistemose pagal sudarytas sutartis su YSII valdytojais (I 6) arba NKSC kreipiasi į tiekėją (I 7).

8 lentelė. Lyderystės pajėgumų srities atsakymų suvestinė

Pajėgumų Sritis	Atsakymų suvestinė	Brandos lygis				
		B1	B2	B3	B4	B5
LYDERYSTĖ						
1.Kokiame lygmenyje leidžiamas Kibernetinės gynybos pajėgumų panaudojimas:						
a) Taktiniame lygmenyje (Tactical Level of authorisation for CD capabilities)?	12.5		■			
b) Operaciniame lygmenyje (Operational Level of authorisation for CD capabilities)?	25			■		
c) Strateginiame lygmenyje (Strategical Level of authorisation for CD capabilities)?	0				■	
2. Aiškus nacionalinių incidentų eskalavimo mechanizmas (Clear escalation mechanism for national incidents)	50				■	
3. Kas suteikia leidimą privataus sektoriaus tinklų stebėjimui:						
a) Reikalinga teismo nutartis (Court Order level of authorization required for surveillance of private sectornetworks)	25			■		
b) Valstybės tarnautojo sprendimas (Civil Servant level of authorization required for surveillance of private sector networks)	0			■		
c) Kito lygmens sprendimas (Other level of authorization required for surveillance of private sector networks)	0	■				
Iš viso taškų	162.5					

Išanalizavus lyderystės dalies rezultatus, gauta atsakymų taškų suma ir vertė procentais siekė 60%. Šią reikšmę palyginus su brandos lygių progreso lentele (priedas Nr.2), matyti, kad brandos lygiui B4 pasiekti reikalinga min. 50%, o B5 100%. Darytina išvada, kad šios srities brandos lygis yra *subalansuotas (B4)*.

Infrastruktūros dalis apima būtiną infrastruktūrą, reikalingą užtikrinti kibernetinės gynybos operacijų vykdymą, taip pat tyrimų laboratorijas ir pan. Atsižvelgiant į modelio reikalavimus, svarbiausias indikatorius šioje srityje yra nacionalinio lygmens kriminalistinių tyrimų infrastruktūros (anglų k. *forensics*

research facility) turėjimas, kuri gebėtų analizuoti kenkėjiškus kodus, įsilaužimo į tinklus įkalčius (anglų k. *artefacts of network penetration*) bei nustatyti įsilaužimo indikatorius (anglų k. *indicators of compromise*). Tokia infrastruktūra ne būtinai turėtų būti vienoje vietoje, tai gali būti paslauga, teikiama kitos institucijos ar net privataus sektoriaus. Analizuojant informantų atsakymus šiuo klausimu (klausimas Nr.4), 60% informantų nurodė, kad tokia infrastruktūra egzistuoja. Pabrėžtina, kad tuo užsiima Lietuvos kriminalinės policijos biuro Sunkaus ir organizuoto nusikalstamumo tyrimo 5-oji valdyba (I 7).

80% apklaustųjų sutiko su teiginiu, kad egzistuoja nacionalinė interaktyvi technologijų aplinka (klausimas Nr.1) bei infrastruktūra kibernetinės gynybos organizavimui (klausimas Nr.2) – tai infrastruktūra (pvz. laboratorija), kurioje galima testuoti specifinius produktus/galimybes ar tam tikrų produktų įtaką karinei įrangai.

Galiausiai 60% informantų nepritarė teiginiui, kad egzistuoja infrastruktūra puolamųjų kibernetinių pajėgumų vystymui ir testavimui.

9 lentelė. Infrastruktūros pajėgumų srities atsakymų suvestinė

Pajėgumų Sritis	Atsakymų suvestinė	Brandos lygis				
		B1	B2	B3	B4	B5
INFRASTRUKTŪRA						
1.Nacionalinės interaktyvios technologijų aplinkos (pvz. laboratorijos) egzistavimas (Existence of a national range)	25					
2.Egzistuoja infrastruktūra kibernetinės gynybos organizavimui (Dedicated physical facility to address CD)	25					
3.Egzistuoja infrastruktūra puolamųjų kibernetinių pajėgumų vystymui ir testavimui (Existence of a facility to develop &test offensive capabilities)	0					
4.Egzistuoja nacionalinio lygmens kriminalistinių tyrimų infrastruktūra (Existence of a national level forensics research facility)	37.5					
Bendra taškų suma	87.5					

Išanalizavus infrastruktūros dalies rezultatus, gauta atsakymų taškų suma ir vertė procentais siekė 87,5%. Šią reikšmę palyginus su brandos lygių progreso lentele (priedas Nr.2), matyti, kad brandos lygiui B4 pasiekti reikalinga min. 50%, o B5 – 100%. Darytina išvada, kad šios srities brandos lygis yra *subalansuotas* (B4).

Pastaba: klausimyne tikslingai nebuvo įtraukti vertinimo modelyje nurodyti klausimai, susiję su Europos Sąjungos Bendros saugumo ir gynybos politikos (anglų k. *Common Security and Defence Policy*) vykdymo misijomis, kadangi autoriaus vertinimu tai išeina už atliekamo tyrimo ribų.

Sąveikumo dalis apima pajėgumo suderinamumą su kitais pajėgumais, įskaitant ir sąveikumą su sąjungininkų pajėgumais (LK vienetais / KAS institucijomis). Vadovaujantis vertinimo modelio

reikalavimais, įmonės sąveikos sistemos (anglų k. *Enterprise Interoperability Framework*) taikymas kibernetinio saugumo (gynybos) padalinyje (klausimas Nr. 1) yra svarbus indikatorius užtikrinant kibernetinę gynybą, kadangi ji leidžia turėti bendrą suvokimą skirtinguose sąveikumo lygmenyse (pvz. ES sąveikumo modelis) (Europos komisija, 2017): teisiniame, organizaciniame, semantiniame ir techniniame, kuriuos apima integruotas viešųjų paslaugų valdymas. 50% informantų pripažino, kad įmonės sąveikos sistema nėra įdiegta, tiek pat informantų nurodė neturintys duomenų.

Į klausimą Nr. 2 „Ar įmonės sąveikos sistema bendra su kitomis valdžios institucijomis?“ 50% apklaustųjų nepritarė teiginiui, tačiau vienas informantas (I 7) nurodė, kad visgi KAM, NKSC, LK, Policijos departamentas ir kt. institucijos turi tam tikras sąveikos formas. Taip pat pažymėtina, kad Kibernetinio saugumo informacinis tinklas, kurį valdo NKSC, apjungia daugelį organizacijų (I 7).

Nepasaint to, kad informantų atsakymai į klausimą Nr.2 buvo neigiami, tačiau faktas išlieka tas, kad kibernetinio saugumo subjektai naudodamiesi Kibernetinio saugumo informaciniu tinklu (LR kibernetinio saugumo įstatymo 13 str.) gali „dalytis informacija apie galimus ir įvykusius kibernetinius incidentus, taip pat rekomendacijomis, nurodymais, techniniais sprendimais ir kitomis priemonėmis, užtikrinančiomis kibernetinį saugumą ir kibernetinio saugumo informacinio tinklo narių tarpusavio bendradarbiavimą kibernetinio saugumo srityje“. Darytina prielaida, kad informantai gali būti nesusipažinę su Kibernetinio saugumo informacinio tinklu, kuriuo siunčiami duomenys, susiję su kibernetiniais incidentais, yra konfidencialūs, todėl autoriaus nuomone atsakymas į klausimą Nr.2 turėtų būti teigiamas.

83% informantų nurodo, kad kibernetinės gynybos sąveikumo vystymas nėra pakankamas (klausimas Nr.3). Tuo pačiu pabrėžtina, kad reiktų daugiau sąveikumo formų organizaciniu aspektu (sektorinių, SOC, CERT/CSIRT, tarp įvairių visuomenės grupių), galbūt ir techninių (kuriant bendravimo platformas) (I 7).

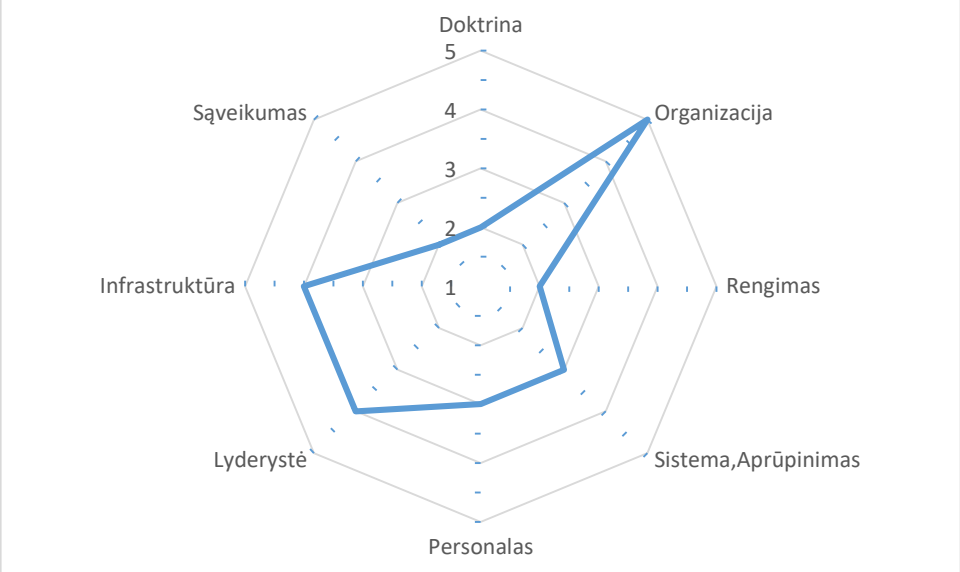
Atsižvelgiant į metodikos reikalavimus dėl sąveikumo lygmens užtikrinimo (klausimas Nr.4), svarbiausiu laikomas sąveikumo užtikrinimas strateginiame lygmenyje, po to operciniame ir galiausiai taktiniame. Atitinkamai informantų nuomonės pasiskirstė sekančiai: 83% mano, kad sąveika užtikrinama taktiniame lygmenyje, 50% gavoja, kad sąveika užtikrinama operaciniame lygmenyje ir tik 33% informantų mano, kad sąveika užtikrinama strateginiame lygmenyje.

Išanalizavus sąveikos dalies rezultatus, gauta atsakymų taškų suma ir vertė procentais siekė 35,7% (žr. Lentelę Nr.10). Šią reikšmę palyginus su brandos lygių progreso lentele (priedas Nr.2), matyti, kad brandos lygiui B2 pasiekti reikalinga min. 25%, o B3 min. 37,5%. Darytina išvada, kad šios srities brandos lygis yra *pradinis (B2).*

10 lentelė. Sąveikumo pajėgumų srities atsakymų suvestinė

Pajėgumų Sritis	Atsakymų suvestinė	Brandos lygis				
		B1	B2	B3	B4	B5
SĄVEIKUMAS						
1.Ar kibernetinio saugumo (gynybos) padalinyje įdiegta Įmonės sąveikos sistema (Enterprise interoperability framework)?	0					
2.Ar Įmonės sąveikos sistema bendra su kitomis valdžios institucijomis (Common with other government departments)	25					
3.Ar pakankamas kibernetinės gynybos sąveikumo vystymas (Sufficient development of CD interoperability)?	0					
4.Kokiame lygmenyje užtikrinamas sąveikumas:						
a) Taktiniame lygmenyje (Tactical Level of interoperability)	25					
b) Operaciniame lygmenyje (Operational Level of interoperability)	12.5					
c) Strateginiame lygmenyje (Strategic Level of interoperability)	0					
Bendra taškų suma	62.5					

Apibendrinta pajėgumų sričių brandos lygių rezultatų suvestinė pateikiama 4 pav.



1- neegzistuojantis, 2 - pradinis, 3 - apibrėžtas, 4 – subalansuotas, 5 - optimizuotas

4 pav. Pajėgumų sričių brandos lygių suvestinė

IŠVADOS IR SIŪLYMAI

1. NATO kibernetinės srities pripažinimas kaip atskiro operacijų domeno daro įtaką sąjungininkų karinių doktrinų ir pajėgumų vystymui. Kibernetinės Gynybos Įsipareigojimuose taip pat reikalaujama, kad sąjungininkai patys įsivertintų savo pasirengimo lygį ir brandą. Tai įpareigoja sąjungininkus laikytis „visos valdžios“ (anglų k. *Whole of government*) požiūrio ir privertė daugelį sąjungininkų geriau koordinuotis darbą tarp skirtingų ministerijų bei stiprinti savo nacionalines kibernetinės gynybos struktūras. Vystant nacionalinius kariuomenės kibernetinės gynybos pajėgumus dažnai susiduriama su dviem konkuruojančiais tikslais: sukurti organizaciją, kuri efektyviai veiktų kibernetinėje srityje ir šios organizacijos integravimas į esamą krašto apsaugos sistemos biurokratiją. Siekiant visiškai įgyvendinti kibernetines pajėgas reikalinga apjungti abu tikslus: kibernetinės pajėgos turi būti veiksmingos kasdieninėje veikloje ir tarpžinybiniuose procesuose ir tuo pačiu gebėti greitai prisitaikyti veikti operacinėje aplinkoje.

2. Visos valdžios požiūris. Kibernetinė erdvė ypatinga tuo, kad vien tik civiliniais ar kariniais kibernetiniais pajėgumais efektyvaus rezultato pasiekti neįmanoma, todėl vystant kariuomenės kibernetinius pajėgumus išskirtinis dėmesys turi būti skiriamas tarpžinybiniam/ tarpinstituciniam bendradarbiavimui. Taip pat svarbu akcentuoti, kad vystomi pajėgumai gebėtų integruotis ar esant poreikiui dalyvauti NATO vykdomose operacijose.

3. Suvokimas dėl nacionalinių kibernetinių pajėgumų svarbos. Nagrinėtose šalyse (Estija, JAV) supratimą apie poreikį vystyti kariuomenės kibernetinius pajėgumus sąlygojo reagavimas į priešiškai nusiteikusių valstybių kibernetines atakas, NATO Kibernetinės Gynybos Įsipareigojimų vykdymas, taip pat eksperimentavimas, remiant vykstančias karines operacijas (JAV). Dinamika kibernetinėje erdvėje reikalauja greito aukščiausio lygio sprendimų priėmimo ir vykdymo, todėl atitinkamos organizacinės struktūros sukūrimas yra kritinis. Kaip gerosios praktikos pavyzdžiai, nagrinėtose NATO šalių valstybių kariuomenėse kibernetiniai pajėgumai evoliucionavo iki atskirų kibernetinių pajėgų (pajėgų vadovybės), ko pasekoje atsiranda aiški vadovavimo grandinė, organizacinė struktūra ir įgaliojimai.

4. Aktyvi kibernetinė gynyba. JAV pajėgos, įgijusios didžiulę patirtį saugant savo kibernetinę erdvę nuo atakų, finansuojamų priešiškų valstybių (Rusijos, Kinijos, Šiaurės Korėjos) suprato, kad vien ginantis ir nesiimant atsakomųjų veiksmų laukiamo efekto nepasieks. Estijos supratimas dėl aktyvios gynybos panašus į JAV. Jos požiūriu šalis turi teisę atsakyti tiek individualiai tiek kolektyviai į kibernetines atakas tokiomis pat priemonėmis. Abiejų šalių požiūris į aktyvią kibernetinę gynybą sutampa, todėl Lietuvos atveju, neabejotinai verta mąstyti apie aktyvios kibernetinės gynybos nuostatų įtvirtinimą nacionaliniu lygiu bei tokio pobūdžio gebėjimų vystymą.

5. Atlikus ekspertinį tyrimą pagal RAND korporacijos karinių gynybos pajėgumų brandos vertinimo modelį, nustatyta, kad **doktrinų**, **rengimo** ir **sąveikumo** pajėgumų vystymo sritys yra *pradiniame (B2)* brandos lygyje. Vadovaujantis modelio reikalavimais, **doktrinų** pajėgumų vystymo srityje reikalinga patvirtinti Kibernetinės Gynybos strategiją ir doktriną bei Operacijų Kompiuteriniuose Tinkluose doktriną. **Rengimo** pajėgumo vystymo srityje būtina užtikrinti kibernetinio saugumo kaip mokymo dalyko dėstymą vyresniųjų karininkų kursuose, taip pat patvirtinti kibernetinio saugumo specialistų rengimo/kvalifikacijos mechanizmą. Ypatingai yra svarbu turėti mokymo mechanizmus, kurie užtikrintų operacinio lygmens ir sprendimo priėmėjų lygmens personalo rengimą. **Sąveikumo** pajėgumo vystymo srityje reikalinga diegti įmonės sąveikos sistemą, vystyti kibernetinės gynybos sąveikumą bei sąveikumą užtikrinti strateginiame lygmenyje. *Apibrėžtas (B3)* brandos lygis nustatytas **sistemų ir aprūpinimo** bei **personalo** pajėgumų vystymo srityse. Verta pažymėti, kad **sistemų ir aprūpinimo** pajėgumo efektyvumas dažniausiai priklauso ne tik nuo turimų technologinių įrankių, tačiau nuo personalo kvalifikacijos ir gebėjimų kaip efektyviai šie įrankiai išnaudojami. **Personalo** srityje didžiausias trūkumas yra kibernetinės gynybos specialistų įdarbinimo ir jų išlaikymo mechanizmo nebuvimas. **Lyderytės** ir **infrastruktūros** pajėgumų srityse nustatytas *subalansuotas (B4)* brandos lygis. **Lyderystės** srityje reikalinga atkreipti dėmesį į aiškaus mechanizmą dėl kibernetinių gynybos pajėgumų autorizavimo strateginiame lygmenyje. Tuo tarpu siekiant **infastruktūros** srityje užtikrinti aukščiausią brandos lygį, reikalinga įsteigti infrastruktūrą puolamųjų kibernetinių pajėgumų vystymui ir testavimui. Aukščiausias *optimizuotas (B5)* brandos lygis nustatytas **organizacijos** pajėgumų vystymo srityje.

Pasiūlymai:

- Siekiant apibrėžti LK kibernetinių pajėgumų panaudojimą kibernetinėje erdvėje, rekomenduojama parengti Kibernetinės Gynybos strategiją ir doktriną bei Operacijų Kompiuteriniuose Tinkluose doktriną.
- Siekiant išlaikyti kompetetingą personalą Krašto apsaugos sistemoje, parengti kibernetinio saugumo specialistų įdarbinimo, išlaikymo bei kvalifikacijos kėlimo mechanizmus.
- Remiantis gerąją NATO šalių praktika bei siekiant nustatyti aiškias LK atsakomybes ir vadovavimą vykdant operacijas kibernetinėje erdvėje, siūloma įvertinti galimybes steigti Kibernetinės gynybos pajėgų vadovybę (kaip atskirą pajėgų rūšį).

LITERATŪRA

1. Andersson, K. (2020). *Notes on military capability concepts and their relevance for analysis of system characteristics.* Prieiga per internetą: http://fhs.diva-portal.org/smash/get/diva2:1473159/FULLTEXT01.pdf
2. Blessing, J. (2020). *The diffusion of cyber forces: military innovation and the dynamic implementation of cyber force structure (doctoral dissertation).* New York: Syracuse University.
3. Bellasio, J., Flint, R., Ryan, N., Søndergaard, S., Monsalve, C., Meranto, A. and Knack, A. (2018). *Developing Cybersecurity Capacity, A proof-of-concept implementation guide.* Prieiga per internetą: https://www.rand.org/pubs/research_reports/RR2072.html
4. Benien, T. (2020). *NATO's new Cyber Operations Centre*. Prieiga per internetą: https://www.monch.com/mpg/ebooks/military-technology/2020/05trya8lb/36/#zoom=z
5. Brent, L. (2019). *NATO's role in cyberspace*. Prieiga per internetą: https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html
6. Boeke, S. (2017). *National cyber crisis management: Different European approaches*. Prieiga per internetą: https://www.researchgate.net/publication/319483832_National_cyber_crisis_management_Different_European_approaches
7. Cavelty, M. (2018). *Europe's cyber-power.* Prieiga per internetą: https://www.tandfonline.com/doi/full/10.1080/23745118.2018.1430718
8. Cho,S. (2020). *An Assessment Model for Defense Cybersecurity Capability*. Prieiga per internetą: https://www.jdaat.org/archive/view_article?pid=jdaat-2-2-39
9. Craig, A. (2020). *Capabilities and Conflict in the Cyber Domain, An Empirical Study (doctoral dissertation).* Cardiff: Cardiff University.
10. Davis, S. (2019). *NATO in the cyber age: strengthening security & defence, stabilising deterrence.* Prieiga per internetą: https://www.nato-pa.int/document/2019-nato-cyber-age-strenghtening-security-and-defence-stabilising-deterrence
11. Deschaux-Dutard, D. (2021). *Is NATO ready for cyber war?* Prieiga per internetą: https://www.frstrategie.org/en/publications/nato-briefs-series/nato-ready-cyber-war-2021
12. Europos komisija. (2017). *Europos sąveikumo Sistema.Įgyvendinimo strategija*. Prieiga per internetą: https://eur-lex.europa.eu/legal-content/lt/TXT/?uri=CELEX%3A52017DC0134
13. Galvin, T. (2018). *Leading change in military organizations.* Prieiga per internetą: https://publications.armywarcollege.edu/pubs/3556.pdf

14. Global Cyber Security Capacity Centre (2021). *Cybersecurity Capacity Maturity Model for Nations.* Prieiga per internetą: https://gcscc.ox.ac.uk/the-cmm#/
15. Gomez, M. (2016). *Arming Cyberspace: The Militarization of a Virtual Domain*. Prieiga per internetą: https://gsis.scholasticahq.com/article/27786-arming-cyberspace-the-militarization-of-a-virtual-domain
16. Janczewski, R., Pilarski, G. and Marczyk, M. (2019). *Terminology As A Barrier To NATO's Interoperability In Cyberspace Operations*. Prieiga per internetą: https://sciendo.com/fr/article/10.2478/kbo-2019-0113
17. Lietuvos Respublikos vyriausybė. (2018) Nutarimas Nr. 818. „*Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo*". 2018 rugpjūčio 13 d. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr
18. Lietuvos Respublikos Vyriausybė (2018). Nutarimas Nr. 818 „*Dėl nacionalinės kibernetinio saugumo strategijos patvirtinimo*". 2018 m. rugpjūčio 13 d. Prieiga per internetą: https://eseimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f?jfwid=dg8d31595
19. Lietuvos Respublikos Vyriausybė (2019). Nutarimas Nr. 709 „*Dėl nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinio veiklos plano patvirtinimo*". 2019 m. liepos 3 d. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/faeb5eb4a6c811e9aab6d8dd69c6da66/asr
20. Lietuvos Respublikos Vyriausybė (2021). Nutarimas Nr. 155 „*Dėl aštuonioliktosios Lietuvos Respublikos vyriausybės programos nuostatų įgyvendinimo plano patvirtinimo"*. 2021 m. kovo 10 d. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/bef7d43286fe11eb998483d0ae31615c?jfwid=i3h7ws9m4
21. Lietuvos Respublikos krašto apsaugos ministras. Įsakymas Nr. V-134 „*Dėl krašto apsaugos ministro 2016 m. rugpjūčio 19 d. įsakymo Nr. V-773 „Dėl krašto apsaugos sistemos pajėgumų planavimo metodikos tvirtinimo" pakeitimo"*. 2022 m. vasario 15d.
22. Lietuvos kariuomenės Mokymo ir doktrinų valdyba. (2016). *Lietuvos karinė doktrina*. Prieiga per internetą: https://www.kariuomene.lt/data/public/uploads/2021/03/lkd-2016_patalpinta-svetainese-6.pdf
23. Lietuvos Respublikos krašto apsaugos ministras. Įsakymas Nr. V-817. Dėl krašto apsaugos ministro 2021 m. kovo 17 d. įsakymo NR. V-187 „*Dėl Lietuvos Respublikos krašto apsaugos ministro valdymo sričių 2021–2023 metų strateginio veiklos plano patvirtinimo" pakeitimo"*. 2021 spalio 25 d. Prieiga per internetą: https://kam.lt/download/72497/kas%202021-2023%20svp_patikslintas%202021-10-25%20v-817.pdf
24. Marrone, A. and Sabatino, E. (2021). *Cyber Defence in NATO Countries: Comparing Models.* Prieiga per internetą: https://www.iai.it/en/pubblicazioni/cyber-defence-nato-countries-comparing-models

25. MacKenzie, P. (2019). *NATO's Vision and Strategy on the Cyberspace Domain*. Prieiga per internetą: https://www.japcc.org/wp-content/uploads/JAPCC_J28_screen.pdf
26. Nacionalinis kibernetinio saugumo centras (2019). *Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinio veiklos plano 2019 metų asignavimų panaudojimas.* Prieiga per internetą: https://www.nksc.lt/aktualu.html
27. Nacionalinis kibernetinio saugumo centras (2020). *Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinio veiklos plano 2020 metų asignavimų panaudojimas.* Prieiga per internetą: https://www.nksc.lt/aktualu.html
28. NATO Allied joint publication AJP-3.20, Edition A, Version 1. (2020). *Allied Joint Doctrine For Cyberspace Operations.* Prieiga per internetą: https://standards.globalspec.com/std/14362050/ajp-3-20
29. Nakasone, P. (2019). *A Cyber Force for Persistent Operations*. Prieiga per internetą: http://cs.brown.edu/courses/csci1950-p/sources/2019_01_22_JFQ_CyberRoleForPersistentOperations_Nakasone.pdf
30. Petrauskaitė, A., Kazlauskaitė - Markelienė, R., Gedminienė, R. (2016). *Šalies saugumas ir gynyba*. Vilnius: Generolo Jono Žemaičio Lietuvos Karo Akademija
31. Pernik, P. (2018). *Preparing for Cyber Conflict: Case Studies of Cyber Command*. Prieiga per internetą: https://icds.ee/en/preparing-for-cyber-conflict-case-studies-of-cyber-command/
32. Porche, I., Paul, C., Serena, C., Clarke, C., Johnson, E. and Herrick, D. (2017). *Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below.* Prieiga per internetą: https://www.rand.org/pubs/research_reports/RR1600.html
33. Robinson, N., Walczak, A., Brune, S., Esterle, A. and Rodriguez, P. (2013). *Stocktaking study of military cyber defence capabilities in the European Union.* Prieiga per internetą: https://www.rand.org/pubs/research_reports/RR286.html
34. Smeets, M. (2019). *NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis.* Prieiga per internetą: https://ccdcoe.org/uploads/2019/06/Art_09_NATO-Members-Organizational-Path.pdf
35. Starr, S., Kuehl, D. and Pudas, T. (2018). *Perspectives On Building A Cyber Force Structure.* Prieiga per internetą: https://ccdcoe.org/uploads/2018/10/Starr-Perspectives-on-Building-a-Cyber-Force-Structure.pdf
36. Schulze, M. (2020). *Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations.* Prieiga per internetą: https://ccdcoe.org/uploads/2020/05/CyCon_2020_10_Schulze.pdf

37. Shea, J. (2018). *Cyberspace as a Domain of Operations: What Is NATO's Vision and Strategy?* Prieiga per internetą: https://www.usmcu.edu/Portals/218/HD%20MCUP/MCUP%20Pubs/MCUJ_Fall2018_9_2_web.pdf?ver=2018-12-31-062028-253
38. Stoltenberg, J. (2017). *Press conference by NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council at the level of Defence Ministers*. Prieiga per internetą: https://www.nato.int/cps/en/natohq/opinions_148417.htm
39. The International Institute For Strategic Studies (2021). *Cyber capabilities and national power: a net assessment.* Prieiga per internetą: https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power
40. Tumkevič, A. (2017). *Cybersecurity In Central Eastern Europe: From Identifying Risks To Countering Threats.* Prieiga per internetą: https://www.researchgate.net/publication/312508248_CYBERSECURITY_IN_CENTRAL_EASTERN_EUROPE_FROM_IDENTIFYING_RISKS_TO_COUNTERING_THREATS
41. United States Army Training and Doctrine Command and Army Cyber Institute at the United States Military Academy. (2016). *The 2050 Cyber Army Technical Report*. Prieiga per internetą: https://info.publicintelligence.net/USArmy-TRADOC-Cyber2050.pdf
42. United States Army Field Manual 3-12. (2021). *Cyberspace Operations and Electromagnetic Warfare.* Prieiga per internetą: https://irp.fas.org/doddir/army/fm3-12.pdf

Vrubliauskas A. (2022). *Kibernetinių pajėgų modeliavimo ypatumai: NATO valstybių patirtis ir Lietuvos perspektyva* (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas

ANOTACIJA

Magistro baigiamojo darbo tikslas – nustatyti Lietuvos kariuomenės kibernetinės gynybos pajėgumų brandos lygį. Pirmoje dalyje nagrinėjami reikalavimai kibernetinei gynybos vystymui nacionalinio saugumo ir kibernetinio saugumo strategijose, taip pat analizuojamas kibernetinio saugumo valdymas ir institucijoms nustatytos atsakomybės strateginiame, operaciniame ir taktiniuose lygmenyse. Antrojoje dalyje mokslinės literatūros analizės metodu nagrinėjami šalies kibernetinių pajėgumų vertinimo modeliai. Trečiojoje dalyje apibrėžiami NATO reikalavimai karinių kibernetinės gynybos pajėgumų vystymui bei pateikiami Estijos ir JAV kariuomenių kibernetinių pajėgumų vystymo pavyzdžiai. Ketvirtojoje dalyje aptariama tyrimo metodologija ir pateikiamas LK kibernetinių pajėgumų brandos lygio tyrimas ir jo rezultatai.

Pagrindiniai žodžiai: kibernetinės gynybos pajėgumai, brandos lygis.

Vrubliauskas A. (2022). *Cyber Force Modelling: experience of NATO countries and Lithuania's perspective* (Master 's Thesis). Vilnius: Mykolas Romeris University

ANNOTATION

The Master's thesis aims to determine the maturity level of the Lithuanian Armed Forces' cyber defense capabilities. The first part of the thesis examines the requirements for cyber defense development in national security and cyber security strategies, as well as analyses cyber security governance and institutional responsibilities at strategic, operational, and tactical levels. The second part, using the scientific literature review method, analyses models for assessing a country's cyber capabilities. The third part outlines NATO requirements for the development of military cyber defense capabilities and discusses two case studies of cyber capability development in the Estonian and US militaries. The fourth part introduces the methodology of the study and presents the results of the Lithuanian Armed Forces Cyber Capability Maturity Level Study.

Key words: cyber defense capabilities, maturity level.

Vrubliauskas A. (2022). *Kibernetinių pajėgų modeliavimo ypatumai: NATO valstybių patirtis ir Lietuvos perspektyva* (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas

SANTRAUKA

Kibernetinės gynybos pajėgumų magistro baigiamojo darbo tema aktuali Krašto apsaugos sistemos institucijoms, dirbančioms kibernetinės gynybos vystymo srityje. NATO pripažinus kibernetinę erdvę kaip atskirą karinių operacijų vykdymo sritį, sąjungininkai paspartino nacionalinių kibernetinių gynybos pajėgumų vystymą. Tačiau vieningai sutariama, kad kibernetinių gynybos pajėgumų vystymą sąjungininkės mato kiekviena savaip ir universalaus kibernetinės gynybos pajėgumo modelio, kuris tiktų visoms šalims, nėra. Dėl to buvo iškelta mokslinė problema: ar LK kibernetinės gynybos pajėgumai pakankami siekiant užtikrinti efektyvią LK kibernetinės erdvės gynybą? Tyrimo objektas - LK kibernetinės gynybos pajėgumai. Šio tyrimo tikslas yra nustatyti LK kibernetinės gynybos pajėgumų brandos lygį. Taip pat buvo iškelti sekantys uždaviniai: ištirti kibernetinio saugumo valdymo struktūrą ir atsakomybes bei kibernetinių pajėgumų vertinimo modelius, išanalizuoti NATO reikalavimus kibernetiniams pajėgumams, nustatyti LK kibernetinės gynybos pajėgumų vystymo sričių privalumus ir trūkumus, taip pat pateikti rekomendacijas LK kibernetinės gynybos pajėgumų vystymui. Tyrimo metodika: tyrimui atlikti pasirinkta kiekybinio tyrimo strategija atliekant ekspertų apklausą. Kiekybinio tyrimo strategijai buvo taikoma šie duomenų analizės metodai: kiekybinė ir kokybinio turinio analizė (anglų k. Content) bei lyginamoji duomenų analizė. Tyrimo rezultatai atskleidė, kad LK kibernetinių pajėgų brandos lygis pagal pajėgumų sritis yra sekantis: doktrinų, rengimo ir sąveikumo pajėgumų vystymo sritys yra pradiniame (B2) brandos lygyje, sistemų ir aprūpinimo bei personalo pajėgumų vystymo srityse nustatytas apibrėžtas (B3) brandos lygis, o lyderytės ir infrastruktūros pajėgumų sritys yra subalansuotame (B4) brandos lygyje.

Atsižvelgiant į gautus tyrimo rezultatus, magistro baigiamajame darbe pateikiamos išvados ir siūlymai dėl LK kibernetinių pajėgumų vystymo.

Vrubliauskas A. (2022). *Cyber Force Modelling: experience of NATO countries and Lithuania's perspective* (Master 's Thesis). Vilnius: Mykolas Romeris University

SUMMARY

The Master's thesis on Cyber Defence Capabilities is relevant for the institutions of the National Defence working in the field of cyber defense development. With the recognition of cyberspace as a separate domain of military operations by NATO, the Allies have accelerated the development of national cyber defense capabilities. However, everyone agrees that the development of cyber defense capabilities is seen by each Allied nation in its own way and that there is no universal model of cyber defense capability that is suitable for all countries. This has led to the scientific question: are the cyber defense capabilities of the Lithuanian Army (LA) sufficient to ensure the effective defense of the LA's cyberspace? The object of the study is the LA cyber defense capability. This study aims to determine the maturity level of the cyber defense capabilities of the LA. The following objectives were also set: to examine the structure and responsibilities of cyber security governance and cyber capability assessment models, to analyze NATO requirements for cyber capabilities, to identify the strengths and weaknesses in the areas of cyber defense capability development in the LA, and to make recommendations for the development of the LA's cyber defense capability. Research methodology: a quantitative research strategy was chosen for the study employing a survey of experts. The following data analysis methods were used for the quantitative research strategy: quantitative and qualitative content analysis and comparative data analysis. The results of the study revealed that the maturity level of the LA cyber force by capability area is as follows: doctrine, training, and interoperability capability domains are at the initial maturity level, systems and sustainment and personnel capability domains are at the defined maturity level, and leadership and infrastructure capability areas are at the balanced maturity level.

At the end of the master‘s thesis conclusions and proposals for the development of the cyber capabilities of the LA were presented.

PRIEDAI

1 PRIEDAS

TYRIMO KLAUSIMYNAS

Sveiki, esu Aurelijus Vrubliauskas, Mykolo Romerio universiteto Viešojo valdymo ir verslo fakulteto Kibernetinio saugumo valdymo programos studentas. Šiuo metu rengiu baigiamąjį magistro darbą ir atlieku tyrimą, kurio tikslas nustatyti Lietuvos kariuomenės kibernetinės gynybos pajėgumų brandos lygį.

Prašyčiau Jūsų kaip tyrinėjamos srities eksperto atsakyti į pridedamo klausimyno klausimus.

Visi tyrimo metu surinkti asmens duomenys išliks konfidencialūs ir bus naudojami tik šio tyrimo tikslais ir tik kaip apibendrinti rezultatai.

Į klausimus prašome atsakyti el. paštu NVK iki kovo 25 d.

Iš anksto dėkoju.

Pajėgumų Sritis	Atsakymas			Pastabos
	Taip	Ne	Nežinau	
DOKTRINA				
1. Kibernetinio Saugumo strategijos egzistavimas (Existence of CS strategy)				
2. Specifinės Kibernetinės Gynybos strategijos egzistavimas (Specific CD strategy)				
3. Nacionalinės Ypatingos Svarbos Informacinės Infrastruktūros strategijos egzistavimas (National Critical Information Infrastructure Protection strategy)				
4. Operacijų Kompiuteriniuose Tinkluose doktrinos egzistavimas (Computer Network Operations Doctrine)				
5. Kibernetinio Atgrasymo doktrinos egzistavimas (Cyber deterrence doctrine)				
6. Nuostata, kad kibernetinė ataka laikoma ginkluota ataka? (Cyber-attacks as armed attack?)				
7. Kibernetinės Gynybos doktrinos egzistavimas (Cyber Defence Doctrine)				
8. Tarptautinės kibernetinės strategijos egzistavimas (International Strategy)				
Iš viso taškų				
ORGANIZACIJA				
1. Nacionalinės iniciatyvinės (valdymo) grupės egzistavimas (Existence of national steering group)				
2. Operacinio lygmens Kibernetinio saugumo organizacijos kariuomenėje egzistavimas (Cyber-security org in defence)				
3. Kibernetinio saugumo (gynybos) organizacija atsakinga už gynybines operacijas kibernetinėje erdvėje (Responsibility for defence)?				
4. Kibernetinio saugumo (gynybos) organizacija atsakinga už puolamąsias operacijas kibernetinėje erdvėje (Responsibility for offence)?				
5. Ar kibernetinio saugumo (gynybos) padalinyje yra ekspertų iš kitų organizacijų (Expertise from other orgs in unit)?				
6. Ar kibernetinio saugumo (gynybos) padalinyje yra ekspertų iš privataus sektoriaus (Expertise from private sector				

in unit)?				
7. Kibernetinio saugumo (gynybos) padalinio ryšys su nacionaliniais pajėgumais, dirbančiais kovos su elektroniniais nusikaltimais srityje (Linked to national cybercrime capability)				
8. Kibernetinio saugumo (gynybos) padalinio ryšiai su CERT (Co-ordination (linked to n/g CERT))				
9. Kibernetinio saugumo (gynybos) padalinio ryšiai su kitomis atsako į incidentus organizacijomis (Linked to other incident response)				
Iš viso taškų				

Pajėgumų Sritis	**Atsakymas**			**Pastabos**
	Taip	**Ne**	**Nežinau**	
RENGIMAS				
1.Kibernetinis saugumas kaip mokymo dalykas vadovaujančio lygmens kursuose (pvz. vyresniųjų štabo karininkų kursuose) (CS covered in syllabus at command level)?				
2.Kibernetinės gynybos specialistų rengimas/karjeros kelias (Specific CD training competency /career path or skillsprofile)?				
3.Dalyvavimas pratybose (Participation in exercises)				
4.Kibernetinio saugumo (gynybos) padalinio ekspertų teorinė ekspetizė (Estimate of theoretical expertise at national level)?				Pasirinkimas pagal brandos lygius: 1-Neegzistuojantis; 2-Pradinis; 3-Apibrėžtas; 4-Subalansuotas; 5-Optimizuotas
5.Kibernetinio saugumo (gynybos) padalinio ekspertų praktinė ekspertizė (Estimate of applied expertise atnational level)?				
6.Ar vykdomi nacionalinio lygio įdarbinimo konkursai (Conduct national level recruitment competitions)?				
7.Kibernetinio saugumo (gynybos) padalinio dalinimasis gerąja praktika/įgyta patirtimi su kitomis institucijomis (Sharing good practice / Lessons learned)?				
Iš viso taškų				
SISTEMA, APRŪPINIMAS				
1.Karinių kibernetinių gynybos pajėgumų priklausomybė nuo privačių išteklių (Reliance upon privately owned assets)				
2.Privataus sektoriaus vaidmuo karinių kibernetinių gynybos pajėgumų veikloje (Perception of role of private sector)				1-5 (1 = nėra kritinis ir 5 = kritinis)
3.Priemonių naudojimo lygmuo (Degree of usage of):				Pasirinkimas pagal brandos lygius: 1-Neegzistuojantis; 2-Pradinis; 3-Apibrėžtas; 4-Subalansuotas; 5-Optimizuotas
a) Perimetru pagrįstos priemonės (pvz. ugniasienė) (Perimeter based measures)				
b) Daugiasluoksnė „Gynybos į gylį“ koncepcija (Defence in depth)				
c) Viešojo rakto infrstruktūra (Public Key Infrastructure)				
d) Veiklos atkūrimo priemonės (Disaster recovery tools)				
e) Duomenų praradimo prevencija (Data Loss Prevention)				
f) Grėsmių žvalgyba ir duomenų apjungimo (Threat intelligence & data fusion)				

g) Duomenų vizualizavimas (Data visualization)				
h) Įsilaužimo prevencija (Intrusion prevention)				
j) Įsilaužimo stebėjimas ir apsauga nuo grėsmių (Honeypots/honeynets)				
k) Saugus susirašinėjimas/duomenų apsikeitimas (Secured messaging / data exchange)				
l) Kriminalistikos platformos (Forensic platforms)				
Iš viso taškų				

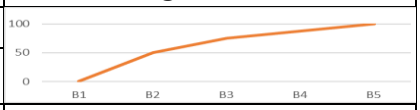
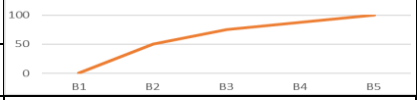
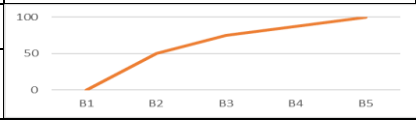
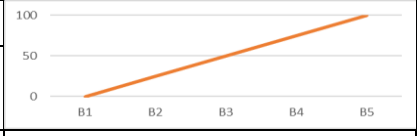
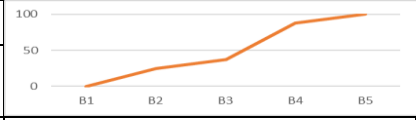
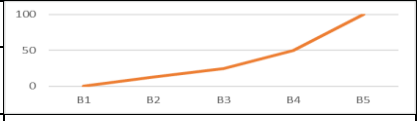
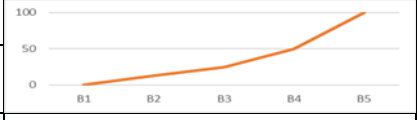
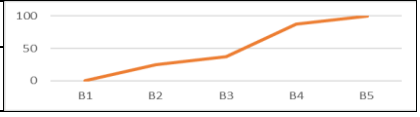
Pajėgumų Sritis	**Atsakymas**			**Pastabos**
	Taip	**Ne**	**Nežinau**	
PERSONALAS				
1.Kibernetinės gynybos specialistų įdarbinimo ir išlaikymo mechanizmas (Recruitment and Retention for CD specialists)				
2. Tapatybės ir prieigos valdymas (Identity and Access Management)				Pasirinkimas pagal brandos lygius: 1-Neegzistuojantis; 2-Pradinis; 3-Apibrėžtas; 4-Subalansuotas; 5-Optimizuotas
3. Grėsmės iš vidaus valdymas (Insider Threat Management)				
4.Personalo patikrinimas ir užtikrinimas (Personnel Vetting and assurance)				
5. Rangovų ir trečiųjų šalių tikrinimas (Vetting contractors and third parties)				
6. 'Juodų' ar 'pilkų' kepurių verbavimas ir įdarbinimas? (Recruitment and employment of 'black' or 'grey' hats?)				
Iš viso taškų				
LYDERYSTĖ				
1.Kokiame lygmenyje leidžiamas Kibernetinės gynybos pajėgumų panaudojimas:				
a) Taktiniame lygmenyje (Tactical Level of authorisation for CD capabilities)?				
b) Operaciniame lygmenyje (Operational Level of authorisation for CD capabilities)?				
c) Strateginiame lygmenyje (Strategical Level of authorisation for CD capabilities)?				
2.Aiškus nacionalinių incidentų eskalavimo mechanizmas (Clear escalation mechanism for national incidents)				
3.Kas suteikia leidimą privataus sektoriaus tinklų stebėjimui:				
a) Reikalinga teismo nutartis (Court Order level of authorization required for surveillance of private sector networks)				
b) Valstybės tarnautojo sprendimas (Civil Servant level of authorization required for surveillance of private sector networks)				
c) Kito lygmens sprendimas (Other level of authorization required for surveillance of private sector networks)				
Iš viso taškų				
INFRASTRUKTŪRA				
1.Nacionalinės interaktyvios technologijų aplinkos (pvz. laboratorijos) egzistavimas (Existence of a national range)				

2.Egzistuoja infrastruktūra kibernetinės gynybos organizavimui (Dedicated physical facility to address CD)				
3.Egzistuoja infrastruktūra puolamųjų kibernetinių pajėgumų vystymui ir testavimui (Existence of a facility to develop &test offensive capabilities)				
4.Egzistuoja nacionalinio lygmens kriminalistinių tyrimų infrastruktūra (Existence of a national level forensics research facility)				
Iš viso taškų				

Pajėgumų Sritis	**Atsakymas**			**Pastabos**
	Taip	**Ne**	**Nežinau**	
SĄVEIKUMAS				
1.Ar kibernetinio saugumo (gynybos) padalinyje įdiegta Įmonės sąveikos sistema (Enterprise interoperability framework)?				
2.Ar Įmonės sąveikos sistema bendra su kitomis valdžios institucijomis (Common with other government departments)				
3.Ar pakankamas kibernetinės gynybos sąveikumo vystymas (Sufficient development of CD interoperability)?				
4.Kokiame lygmenyje užtikrinamas sąveikumas:				
a) Taktiniame lygmenyje (Tactical Level of interoperability)				
b) Operaciniame lygmenyje (Operational Level of interoperability)				
c) Strateginiame lygmenyje (Strategic Level of interoperability)				
Iš viso taškų				

2 PRIEDAS

BRANDOS LYGIO PROGRESAS PAGAL PAJĖGUMŲ SRITIS

DOKTRINA	**B1**	**B2**	**B3**	**B4**	**B5**	**Progreso kreivė**
Procentiniai taškai brandos lygiui	0	50	25	12.5	12.5	
Procentinė taškų suma	0	50	75	87.5	100	
ORGANIZACIJA	**B1**	**B2**	**B3**	**B4**	**B5**	
Procentiniai taškai brandos lygiui	0	50	25	12.5	12.5	
Procentinė taškų suma	0	50	75	87.5	100	
RENGIMAS	**B1**	**B2**	**B3**	**B4**	**B5**	
Procentiniai taškai brandos lygiui	0	50	25	12.5	12.5	
Procentinė taškų suma	0	50	75	87.5	100	
SISTEMA, APRŪPINIMAS	**B1**	**B2**	**B3**	**B4**	**B5**	
Procentiniai taškai brandos lygiui	0	25	25	25	25	
Procentinė taškų suma	0	25	50	75	100	
PERSONALAS	**B1**	**B2**	**B3**	**B4**	**B5**	
Procentiniai taškai brandos lygiui	0	25	12.5	50	12.5	
Procentinė taškų suma	0	25	37.5	87.5	100	
LYDERYSTĖ	**B1**	**B2**	**B3**	**B4**	**B5**	
Procentiniai taškai brandos lygiui	0	12.5	12.5	25	50	
Procentinė taškų suma	0	12.5	25	50	100	
INFRASTRUKTŪRA	**B1**	**B2**	**B3**	**B4**	**B5**	
Procentiniai taškai brandos lygiui	0	12.5	12.5	25	50	
Procentinė taškų suma	0	12.5	25	50	100	
SĄVEIKUMAS	**B1**	**B2**	**B3**	**B4**	**B5**	
Procentiniai taškai brandos lygiui	0	25	12.5	50	12.5	
Procentinė taškų suma	0	25	37.5	87.5	100	

INDIKATORIŲ VERTĖS

Pajėgumų Sritis	Vertė	Brandos lygis				
		B1	B2	B3	B4	B5
DOKTRINA						
1. Kibernetinio Saugumo strategijos egzistavimas (Existence of CS strategy)	25					
2. Specifinės Kibernetinės Gynybos strategijos egzistavimas (Specific CD strategy)	12.5					
3. Nacionalinės Ypatingos Svarbos Informacinės Infrastruktūros strategijos egzistavimas (National Critical Information Infrastructure Protection strategy)	25					
4. Operacijų Kompiuteriniuose Tinkluose doktrinos egzistavimas (Computer Network OperationsDoctrine)	12.5					
5. Kibernetinio Atgrasymo doktrinos egzistavimas (Cyber deterrence doctrine)	4.17					
6. Nuostata, kad kibernetinė ataka laikoma ginkluota ataka? (Cyber-attacks as armed attack?)	4.17					
7. Kibernetinės Gynybos doktrinos egzistavimas (Cyber Defence Doctrine)	12.5					
8. Tarptautinės kibernetinės strategijos egzistavimas (International Strategy)	4.17					
Bendra maksimali taškų suma	100					
ORGANIZACIJA						
1. Nacionalinės iniciatyvinės (valdymo) grupės egzistavimas (Existence of national steering group)	25					
2. Operacinio lygmens Kibernetinio saugumo organizacijos kariuomenėje egzistavimas (Cyber-security org in defence)	25					
3. Kibernetinio saugumo (gynybos) organizacija atsakinga už gynybines operacijas kibernetinėje erdvėje (Responsibility for defence)?	25					
4. Kibernetinio saugumo (gynybos) organizacija atsakinga už puolamąsias operacijas kibernetinėje erdvėje (Responsibility for offence)?	12.5					
5. Ar kibernetinio saugumo (gynybos) padalinyje yra ekspertų iš kitų organizacijų (Expertise from other orgs in unit)?	12.5					
6. Ar kibernetinio saugumo (gynybos) padalinyje yra ekspertų iš privataus sektoriaus (Expertise from private sector in unit)?	6.25					
7. Kibernetinio saugumo (gynybos) padalinio ryšys su nacionaliniais pajėgumais, dirbančiais kovos su elektroniniais nusikaltimais srityje (Linked to national cybercrime capability)	12.5					
8. Kibernetinio saugumo (gynybos) padalinio ryšiai su CERT (Co-ordination (linked to n/g CERT))	12.5					
9. Kibernetinio saugumo (gynybos) padalinio ryšiai su kitomis atsako į incidentus organizacijomis (Linked to other incident response)	6.25					
Bendra maksimali taškų suma	137.5					

Pajėgumų Sritis	Vertė	Brandos lygis				
		B1	B2	B3	B4	B5
RENGIMAS						
1.Kibernetinis saugumas kaip mokymo dalykas vadovaujančio lygmens kursuose (pvz. vyresniųjų štabo karininkų kursuose) (CS covered in syllabus at command level)?	25					
2.Kibernetinės gynybos specialistų rengimas/karjeros kelias (Specific CD training competency /career path or skillsprofile)?	25					
3.Dalyvavimas pratybose (Participation in exercises)	12.5					
4.Kibernetinio saugumo (gynybos) padalinio ekspertų teorinė ekspetizė (Estimate of theoretical expertise at national level)?	100	1	2	3	4	5
5.Kibernetinio saugumo (gynybos) padalinio ekspertų praktinė ekspertizė (Estimate of applied expertise atnational level)?	100	1	2	3	4	5
6.Ar vykdomi nacionalinio lygio įdarbinimo konkursai (Conduct national level recruitment competitions)?	12.5					
7.Kibernetinio saugumo (gynybos) padalinio dalinimasis gerąja praktika/įgyta patirtimi su kitomis institucijomis (Sharing good practice / Lessons learned)?	25					
Bendra maksimali taškų suma	300					
SISTEMA, APRŪPINIMAS						
1.Karinių kibernetinių gynybos pajėgumų priklausomybė nuo privačių išteklių (Reliance upon privately owned assets)	Taip/Ne					
2.Privataus sektoriaus vaidmuo karinių kibernetinių gynybos pajėgumų veikloje (Perception of role of private sector)	1-5					
3.Priemonių naudojimo lygmuo (Degree of usage of):						
a) Perimetru pagrįstos priemonės (pvz. ugniasienė) (Perimeter based measures)	100	1	2	3	4	5
b) Daugiasluoksnė „Gynybos į gylį“ koncepcija (Defence in depth)	100	1	2	3	4	5
c) Viešojo rakto infrstruktūra (Public Key Infrastructure)	100	1	2	3	4	5
d) Veiklos atkūrimo priemonės (Disaster recovery tools)	100	1	2	3	4	5
e) Duomenų praradimo prevencija (Data Loss Prevention)	100	1	2	3	4	5
f) Grėsmių žvalgyba ir duomenų apjungimo (Threat intelligence & data fusion)	100	1	2	3	4	5
g) Duomenų vizualizavimas (Data visualization)	100	1	2	3	4	5
h) Įsilaužimo prevencija (Intrusion prevention)	100	1	2	3	4	5
j) Įsilaužimo stebėjimas ir apsauga nuo grėsmių (Honeypots/honeynets)	100	1	2	3	4	5
k) Saugus susirašinėjimas/duomenų apsikeitimas (Secured messaging / data exchange)	100	1	2	3	4	5
l) Kriminalistikos platformos (Forensic platforms)	100	1	2	3	4	5
Bendra maksimali taškų suma	1100					

Pajėgumų Sritis	Vertė	Brandos lygis				
		B1	B2	B3	B4	B5
PERSONALAS						
1.Kibernetinės gynybos specialistų įdarbinimo ir išlaikymo mechanizmas (Recruitment and Retention for CD specialists)	87.5				■	
2. Tapatybės ir prieigos valdymas (Identity and Access Management)	100	1	2	3	4	5
3. Grėsmės iš vidaus valdymas (Insider Threat Management)	100	1	2	3	4	5
4.Personalo patikrinimas ir užtikrinimas (Personnel Vetting and assurance)	100	1	2	3	4	5
5. Rangovų ir trečiųjų šalių tikrinimas (Vetting contractors and third parties)	100	1	2	3	4	5
6. 'Juodų' ar 'pilkų' kepurių verbavimas ir įdarbinimas? (Recruitment and employment of 'black' or 'grey' hats?)	100	1	2	3	4	5
Bendra maksimali taškų suma	587.5					
LYDERYSTĖ						
1.Kokiame lygmenyje leidžiamas Kibernetinės gynybos pajėgumų panaudojimas:						
a) Taktiniame lygmenyje (Tactical Level of authorisation for CD capabilities)?	12.5		■			
b) Operaciniame lygmenyje (Operational Level of authorisation for CD capabilities)?	25			■		
c) Strateginiame lygmenyje (Strategical Level of authorisation for CD capabilities)?	50				■	
2. Aiškus nacionalinių incidentų eskalavimo mechanizmas (Clear escalation mechanism for national incidents)	50				■	
3. Kas suteikia leidimą privataus sektoriaus tinklų stebėjimui:						
a) Reikalinga teismo nutartis (Court Order level of authorization required for surveillance of private sectornetworks)	25			■		
b) Valstybės tarnautojo sprendimas (Civil Servant level of authorization required for surveillance of private sector networks)	25			■		
c) Kito lygmens sprendimas (Other level of authorization required for surveillance of private sector networks)		■				
Bendra maksimali taškų suma	187.5					

Pajėgumų Sritis	Vertė	Brandos lygis				
		B1	B2	B3	B4	B5
INFRASTRUKTŪRA						
1.Nacionalinės interaktyvios technologijų aplinkos (pvz. laboratorijos) egzistavimas (Existence of a national range)	25				■	
2.Egzistuoja infrastruktūra kibernetinės gynybos organizavimui (Dedicated physical facility to address CD)	25			■		
3.Egzistuoja infrastruktūra puolamųjų kibernetinių pajėgumų vystymui ir testavimui (Existence of a facility to develop &test offensive capabilities)	12.5				■	
4.Egzistuoja nacionalinio lygmens kriminalistinių tyrimų infrastruktūra (Existence of a national level forensics research facility)	37.5				■	
Bendra maksimali taškų suma	100					
SĄVEIKUMAS						
1.Ar kibernetinio saugumo (gynybos) padalinyje įdiegta Įmonės sąveikos sistema (Enterprise interoperability framework)?	50					
2.Ar Įmonės sąveikos sistema bendra su kitomis valdžios institucijomis (Common with other government departments)	25					
3.Ar pakankamas kibernetinės gynybos sąveikumo vystymas (Sufficient development of CD interoperability)?	12.5		■			
4.Kokiame lygmenyje užtikrinamas sąveikumas:						
a) Taktiniame lygmenyje (Tactical Level of interoperability)	25		■			
b) Operaciniame lygmenyje (Operational Level of interoperability)	12.5			■		
c) Strateginiame lygmenyje (Strategic Level of interoperability)	50				■	
Bendra maksimali taškų suma	175					