VILNIAUS UNIVERSITETAS

EKONOMIKOS IR VERSLO ADMINISTRAVIMO FAKULTETAS

KOKYBĖS VADYBOS MAGISTRO PROGRAMA

Magistranto Karolio Januškos

MAGISTRO BAIGIAMASIS DARBAS

VALSTYBĖS ATSPARUMO HIBRIDINĖMS GRĖSMĖMS VERTINIMO MODELIS	**STATES'S RESILIENCE TO THE HYBRID THREATS EVALUATION MODEL**

Darbo vadovas

asistentas dr. Darius Ruželė

Vilnius, 2024

TURINYS

PAVEIKSLŲ SĄRAŠAS

LENTELIŲ SĄRAŠAS

SUTRUMPINIMAI IR TERMINAI

AOTD – Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos

EIM – Lietuvos Respublikos Ekonomikos ir inovacijų ministerija

FINMIN – Lietuvos Respublikos Finansų ministerija

KAM – Lietuvos Respublikos Krašto apsaugos ministerija

LK – Lietuvos kariuomenė

LRV – Lietuvos Respublikos Vyriausybė

NKSC – Nacionalinis kibernetinio saugumo centras

NVO – Nevyriausybinės organizacijos

NKVC - Nacionalinis krizių valdymo centras prie Lietuvos Respublikos Vyriausybės

SKD – Lietuvos kariuomenės Strateginės komunikacijos departamentas

URM – Lietuvos Respublikos Užsienio reikalų ministerija

VSAT – Valstybės sienos apsaugos tarnyba

VSD – Valstybės saugumo departamentas

NSGK – Lietuvos Respublikos Seimo Nacionalinio saugumo ir gynybos komitetas

ĮGALIOTASIS KARAS – karinis konfliktas, kurio metu viena ar kelios trečiosios šalys tiesiogiai ar netiesiogiai remia vieną ar daugiau valstybinių, ar nevalstybinių kovotojų, siekdamos paveikti konflikto baigtį ir taip įgyvendinti savo strateginius interesus arba pakenkti oponentų interesams.

ĮVADAS

Darbo temos aktualumas. Pastaraisiais metais susiduriama su įvairiomis hibridinėmis grėsmėmis, įskaitant migracijos instrumentalizavimą (angl. weaponization of migration), kibernetines grėsmes, ekonomines poveikio priemones, siekiant vykdyti politinį spaudimą bei informacinio karo operacijas, įskaitant propagandą ir dezinformacijos kampanijas. Politikai, politikos formuotojai ir saugumo analitikai vis dažniau diskutuoja apie tai, kaip elgtis su įvairiomis hibridinėmis grėsmėmis, kurios yra slaptos, galingos ir sunkios atsispirti (Clarke & Jackson, 2019). Hibridinio poveikio tikslai paprastai yra kruopščiai identifikuoti ir parinkti pažeidžiamumai. Tokie pažeidžiamumai varijuoja nuo korumpuotų individų, užimančių reikšmingas pozicijas iki struktūrinių valstybės problemų, tokių kaip etninė atskirtis (Cederberg ir kt., 2017). Naujausių technologijų pažanga ir jų sklaida, kartu su plačiu Vakarų visuomenių skaitmeninimu, įskaitant kritinę infrastruktūrą ir ryšių priemones, sukuria palankias sąlygas hibridinėms grėsmėms. Technologijų plėtra leidžia įvairiems grėsmės subjektams turėti platesnį geografinį pasiekiamumą ir didesnį galimų taikinių pasirinkimą. Be fizinės ir skaitmeninės infrastruktūros, hibridinės įtakos gali būti nukreiptos į mūsų svarbiausias funkcijas ir procesus bei visuomenės kognityvinį lygmenį (Cederberg ir kt., 2017). Pastaraisiais metais pastebimas padidėjęs ribų nykimas tarp strateginių ir ekonominių užsienio veikėjų interesų. Investicijos į atskiras Europos Sąjungos (toliau – ES) valstybes – nares - identifikuojamos kaip galimos politinės įtakos priemonės, keliančios grėsmių nacionaliniam saugumui (Aho ir kt., 2020). Energetikos geopolitika, įskaitant pasaulinės rinkos ir saugumo aplinkybes, tampa vis sudėtingesnė, o tai pabrėžia poreikį analizuoti ir suprasti energetines priklausomybes. Atsižvelgiant į šiuos veiksnius, svarbu integruoti energetinės priklausomybės aspektus į hibridinių grėsmių, rizikų ir atsparumo vertinimus bei strategijas (Verner ir kt., 2019). Kišimasis ir bandymas daryti įtaką rinkimams šiais laikais tapo nuolatiniu reiškiniu – nepriklausomai nuo atakuojamo taikinio atsparumo lygio (Sorensen & Bach Nyemann, 2018). Tiek Ukrainos, tiek Jungtinių Amerikos Valstijų (toliau – JAV) rinkimų atvejai atskleidžia, kad „hibridiniai užpuolikai“ nesukūrė pažeidžiamumų, kuriuos išnaudojo. Ukrainos politinės ir ekonominės aplinkybės padarė ją itin pažeidžiamą Rusijos veiksmams ir giliai poliarizuotas 2016 m. JAV politinis kontekstas buvo tarsi atviras kvietimas rusams įsikišti (Treverton ir kt., 2018). Vystantis socialiniams tinklams, pasikeitė „mūšio lauko“ apibrėžimo

supratimas, išryškinant didėjantį pilietinės visuomenės tapimą „mūšio erdve“ savaime (Falk, 2020). „Kiekviena valstybė turi skirtingų lygių kultūrinius, ekonominius, karinius, politinius pažeidžiamumus, todėl nėra vieno tikslaus modelio, kuris padėtų tinkamai pasiruošti ir operatyviai atsakyti į sparčiai kintančias hibridines grėsmes bei pasitelkiamas įtakos operacijas” (Gecaitė, 2023). Šios grėsmės išryškino sisteminio modelio, kuris galėtų padėti veiksmingai spręsti sudėtingus ir dinamiškus šalies saugumo iššūkius, poreikį. Tai yra tik keletas iš daugelio pavyzdžių, iliustruojančių, kad grėsmės nacionaliniam saugumui kyla skirtingose srityse – ne tik karinėje. Nacionalinis saugumas Enciklopediniame karybos žodyne apibrėžiamas kaip „veikla ir priemonės, kurios sudaro tautos ir valstybės laisvos ir demokratinės raidos sąlygas, užtikrina Lietuvos valstybės nepriklausomybę, jos teritorinį vientisumą ir konstitucinės santvarkos apsaugą ir gynimą“(Čiočys ir kt., 2008).Tai suponuoja išvadą, kad į šias grėsmes reaguoti yra būtina laikantis sisteminio požiūrio į saugumą, integruojant karines, civilines ir visuomenines priemones. Išnaudodama visų suinteresuotųjų šalių, įskaitant vyriausybines įstaigas, privataus sektoriaus subjektus ir pilietinės visuomenės nevyriausybines organizacijas (toliau - NVO), stipriąsias puses, valstybės gali stiprinti atsparumą ir veiksmingai reaguoti į sudėtingus ir besikeičiančius XXI amžiaus saugumo iššūkius.

Analizuojamos temos ištyrimo lygis. Hibridinių grėsmių samprata XXI amžiuje, daugiausia dėmesio skiriant Rusijos hibridiniam karui, kaip aktyviausiam ir įžūliausiam pavyzdžiui, aptariama Švedijos gynybos universiteto publikuotoje studijoje (Treverton ir kt., 2018). Berzinš (2023) tyrė kaip Latvija pritaiko visos visuomenės (angl. Whole-of-Society) požiūrį į nacionalinį saugumą dėl Rusijos „naujos kartos karo“ grėsmės. Aho ir kiti (2020) tyrė hibridinių grėsmių pasireiškimą finansų sistemoje. Verner (2019) analizavo energetinę priklausomybę kaip politinio poveikio priemonę, iš hibridinių grėsmių perspektyvos. Limnell (2018) tyrė viešojo ir privataus sektorių bendradarbiavimo bei veiklos tarpusavio koordinavimą, siekiant padidinti atsparumą hibridinėms grėsmėms. Cederberg ir kiti (2017) nustatė, kad hibridinės grėsmės yra stiprėjanti problema dėl šių grėsmių tarpusavio sąsajų, veikimo per skirtingas dimensijas bei technologinės pažangos suteikiamų informacijos dalijimosi, veiklos koordinavimo bei sintezės galimybių. Kaip atsakas šiam iššūkiui siūlomas visapusiško nacionalinio požiūrio derinimas su informacijos dalijimusi bei koordinavimu tarptautiniame lygmenyje.

Darbo naujumas. Hibridinės grėsmės yra plačiai aprašoma tema, egzistuoja rekomenduotini atsparumo hibridinėms grėsmėms modeliai, tačiau nėra pakankamai mokslinių šaltinių, kuriuose būtų pateiktas praktinis valstybės atsparumo hibridinėms grėsmėms vertinimo modelis. Šiuo darbu bus

siekiama sukurti vertinimo modelį, padėsiantį įvertinti valstybės, kaip sistemos atsparumo hibridinėms grėsmėms vertinimo modelį.

Mokslinė problema: nerasta valstybės atsparumo hibridinėms grėsmėms vertinimo modelio.

Taikomoji problema: kaip pagerinti Lietuvos Respublikos atsparumą hibridinėms grėsmėms?

Magistro baigiamojo darbo tikslas: remiantis išanalizuota moksline ir ekspertine literatūra bei atliktu autoriniu tyrimu, sukurti valstybės atsparumo hibridinėms grėsmėms vertinimo modelį, kurį galima pritaikyti bet kurios valstybės atsparumo hibridinėms grėsmėms įvertinimui.

Magistro baigiamojo darbo uždaviniai:

1. Apžvelgus mokslinę literatūrą, nagrinėjančią hibridines grėsmes, atskleisti hibridinių grėsmių problematiką;
2. Išanalizuoti hibridinių grėsmių valdymo gerąsias praktikas;
3. Ištyrus Lietuvos Respublikos hibridinių grėsmių valdymo sistemą, įvertinti atsparumą hibridinėms grėsmėms;
4. Pasiūlyti rekomendacijas ir strategines gaires Lietuvos Respublikos atsparumo hibridinėms grėsmėms stiprinimui.

Tyrimo objektas: Atsparumo hibridinėms grėsmėms sisteminis vertinimas.

Magistro baigiamąjį darbą sudaro trys dalys. Pirmojoje, remiantis moksline ir ekspertine literatūra – apibrėžiama hibridinių grėsmių sąvoka bei analizuojami hibridinių grėsmių atvejai Lietuvos Respublikoje. Remiantis šia analize, atskleidžiamas hibridinių grėsmių kompleksiškumas. Antrojoje dalyje analizuojami hibridinių grėsmių valdymo atvejai bei išskiriami bendri veiksniai, užtikrinantys efektyvų kompleksinių problemų sprendimą. Trečioji dalis skirta empirinio tyrimo metodikai atskleisti. Darbo pabaigoje pateikiamos išvados ir rekomendacijos bei naudotos literatūros sąrašas.

Raktiniai žodžiai: Hibridinės grėsmės, kompleksiškumas, atsparumo vertinimas

1. LITERATŪROS APIE HIBRIDINES GRĖSMES APŽVALGA

1.1. Hibridinių grėsmių samprata

Europos Komisijos Jungtinio tyrimų centro paskelbtame raporte "Hibridinės grėsmės: visapusiška atsparumo ekosistema" hibridinės grėsmės apibūdinamos kaip *skirtingų priemonių kombinacija, naudojama siekiant nedeklaruotų strateginių tikslų, oficialiai to nedeklaruojant.* Šios priemonės gali būti žinomos ar nežinomos ir netikėtos (Jungwirth ir kt., 2023).

Kai kuriuose šaltiniuose, kalbant apie hibridines grėsmes, minimi hibridinio karo arba hibridinės karybos (angl. Hybrid Warfare) terminai, reiškiantys tą patį tradicinių ir nekonvencinių priemonių panaudojimą, siekiant nedeklaruotų strateginių tikslų. *Hibridinio karo sąvoka reiškia konflikto su smurto taikymu formą, kurioje dalyvauja valstybiniai ir nevalstybiniai veikėjai, naudodami įprastines ir nekonvencines įtakos priemones, neapsiribojant mūšio lauku arba specifine netradicine poveikio priemone, ir/ arba specifine, fizine teritorija*, teigia Banasik, cituodamas pagal Jacobs ir Lascoasnjarias (2017). „Hibridinio karo koncepcija siekia apibrėžti tai, kas yra „per vidurį" konvencinės ir nekonvencinės karybos skirstymo sampratos" (Bajarūnas & Keršanskas, 2018). Šiuo atveju, verta atkreipti dėmesį, kad išskiriami valstybiniai ir nevalstybiniai veikėjai. Tai yra svarbus aspektas bandant identifikuoti galimus grėsmių šaltinius.

Vertinant priemones, taikomas hibridiniame kare, minima, kad *hibridinis karas yra tradicinių kariavimo priemonių panaudojimas su kitomis, asimetrinėmis priemonėmis ar net terorizmu, siekiant politinių tikslų* (Žilinskas, cituodamas Hoffmaną, 2017). Taigi išskiriamas tradicinių karinių priemonių panaudojimas kombinuotai su kitomis, siekiant bendrų politinių tikslų. Taigi, sukeliamas netikrumo jausmas, o sugebėjimas atskirti karą nuo taikos ypatingai svarbus, kai kalbama apie tarptautinę teisę (pavyzdžiui, NATO 5-asis straipsnis) (Marsh & Searle, 2023). Apibendrinant, hibridines grėsmes galima apibūdinti kaip politinių ar strateginių tikslų siekimą, jų nedeklaruojant bei pasitelkiant tradicinių karinių priemonių ir netradicinių, asimetrinių priemonių kombinaciją išnaudojant valstybinius išteklius, ir nevalstybinius veikėjus.

Valstybės bei nevalstybiniai veikėjai nuolat konkuruoja dėl resursų bei įtakos sferų. Karas ir karinė galia yra vienas iš valstybės galios šaltinių, tačiau kalbant apie Nacionalinį saugumą, nereikėtų apsiriboti vien tik pastaraja. Galia gali būti suskirstyta į „kietą galią" ir „minkštąją galią". Minkštoji galia apima daugybę neapčiuopiamų ir sunkiai išmatuojamų savybių, tokias kaip: bendros vertybės, išsilavinimas, žiniasklaida, literatūra, religija ir viešoji politika (Zorri, 2023). Hibridinio karo

fenomenas – tai strateginių tikslų pasiekimas be būtinybės pradėti karinę kovą tradicine prasme. (Banasik, 2017). Tai paaiškina, kad siekdami daryti įtaką ir siekti savo tikslų, valstybiniai ir nevalstybiniai veikėjai pasitelkia įvairius galios instrumentus, tarp jų ir karines priemones, tačiau pastarosios nėra vienintelis būdas šiems tikslams pasiekti.

Labiau specializuotuose, į karines ir žvalgybos organizacijas orientuotuose šaltiniuose yra vartojami terminai „Pilkoji zona“ bei „Pilkosios zonos karyba“ (angl. Gray Zone Warfare) (Morris ir kt., 2019), (Mahmood Azad ir kt., 2023), (Scharlach, 2023). Terminas „pilkas“ atspindi ne tik veiksmų pobūdį tarp taikos ir karo šiuolaikinėse didžiųjų galių varžybose (angl. Great Power Competition), bet ir pirmenybės teikimą dviprasmiškiems veiksmams, už kurių vykdymą negalima priskirti atsakomybės jokiam konkrečiam veikėjui, pilkojoje zonoje. Nesvarbu, ar tai taip vadinami „žalieji žmogeliukai“ ar kitaip vadinami „mandagūs žmonės“, kurie aneksavo Krymą, ar komercinės žvejybos laivynai, bauginantys Ramiojo vandenyno šalis Kinijos komunistų partijos vardu arba kompiuterines sistemas atakuojantys „patriotiniai įsilaužėliai“ – šie veiksmai vyksta pilkojoje zonoje ir šiais laikais jų daugėja. (Marsh & Searle, 2023) Nors pilkosios zonos konfliktai ir įprasti karai turi panašius tikslus, jie pasiekia šiuos tikslus skirtingais būdais ir priemonėmis. Konkrečiau, pilkosios zonos konfliktai dažniausiai naudoja kelis galios instrumentus. Nors tai dažnai pasakytina ir apie tradicinius konfliktus, santykinis karinės galios instrumento, palyginti su diplomatiniu, informaciniu, ekonominiu, finansiniu, žvalgybos ir teisėsaugos (DIMEFIL), svoris yra priešingas, o pastarieji instrumentai naudojami daug plačiau, nei karinis, pilkosios zonos konfliktuose. Pilkosios zonos konfliktai ne tik teikia pirmenybę skirtingiems galios instrumentams, bet ir siekia neperžengti didelio masto tiesioginio karinio konflikto slenksčio. Tai dažnai apima pastangas padidinti dviprasmiškumą ir neaiškų priskyrimą (angl. attribution) (Marsh & Searle, 2023). Pilkosios zonos veikla yra skirta išvengti atsako, apimančio karinę jėgą (Coombs, 2023)

Didžiosios valstybės, tokios, kaip Rusija Federacija (toliau – Rusija) ar Kinijos liaudies respublika (toliau – Kinija), stengiasi išvengti branduolinio konflikto, todėl konkurencija pilkojoje zonoje yra *dernier cri* – naujausia mada, kai valstybės siekia plėtoti ir ginti savo interesus tuo pačiu destabilizuojant, ir trikdant joms priešiškas jėgas, tačiau nesukeliant rimtesnio konflikto grėsmės (Zorri, 2023). „Nors Rusijos valdančiojo režimo atstovai nuolat kalba apie, jų nuomone, neišvengiamai įsitvirtinsiančią naują daugiapolę pasaulio tvarką, vienintelis tokio naratyvo tikslas – suburti antivakarietišką koaliciją, kurią sudarytų visų pirma globaliųjų Pietų valstybės, o Rusija įtvirtintų savo įtaką kaip tokios koalicijos lyderė” (VSD ir AOTD, 2024). Kalbant apie pilkosios zonos taktikas, naudojamas Kinijos, būtina paminėti agresyvų elgesį Pietų Kinijos jūroje. Pasitelkdama savo

žvejybos laivyną, kuris aktyviai užsiima neteisėta, nereglamentuojama ir nedeklaruojama žvejyba regione ir už jo ribų, ji (Kinija) taip pat pila dirbtines salas ir jose dislokuoja ginkluotąsias pajėgas. Nors Pekinas atkakliai neigia („tai tik žvejybos laivynai!“), realybė tokia, kad ši veikla, kurią vykdo Kinijos „jūrinė milicija“, yra tiesiogiai kontroliuojama Kinijos komunistų partijos ir Liaudies išlaisvinimo armijos. Dėl to Kinijai pavyko atitverti ir tada militarizuoti zonas, kurios kažkada buvo laikomos tarptautiniais vandenimis, dislokuojant ten radarus, raketų paleidimo sistemas ir net orlaivius (Marsh & Searle, 2023). Didelės Kinijos įmonės daug investuoja į strateginius sektorius, įskaitant energetiką, bankininkystę, vandenį, sveikatą ir draudimą. „Nacionalinio saugumo įstatymas“ Kinijoje kelia susirūpinimą dėl privačių įmonių dalyvavimo žvalgybos veikloje. Kinijos investicijos apima vidutines įmones, nekilnojamąjį turtą, pramonę, turizmo ir žiniasklaidos grupes, o buvę politikai dažnai įdarbinami ir glaudžiai susiję Kinijos valdomomis ar Kinijos kapitalo įmonėmis (Pathe Duarte, 2020).

Ryškus hibridinių priemonių panaudojimo, siekiant paslėptų strateginių tikslų, pavyzdys yra Rusijos veiksmai Ukrainos atžvilgiu. Galutinis Kremliaus veiksmų Ukrainoje, nuo 2013 m., tikslas buvo įgyti politinę įtaką ir neleisti šaliai priartėti prie Vakarų, bei potencialiai tapti NATO nare. Tai buvo įvykdyta atvirai, Donecke ir Luhanske įkūrus kvazivalstybes bei aneksuodama Krymą – dalį suverenios Ukrainos teritorijos. Lygiagrečiai buvo vykdoma ir paslėpta veikla – kišimasis į Ukrainos rinkimus, organizavimas ir finansavimas kampanijos už „švelnią Ukrainos federalizaciją“ visos šalies mastu, taip siekiant pakeisti šalies konstituciją ir sukurti alternatyvų valdžios centrą, tuo pačiu kuriant plačios paramos šiai veiklai iliuziją. Kremliaus kišimosi į Ukrainos rinkimus ir kampanijos už "švelnią Ukrainos federalizaciją" organizavimo tikslas buvo pakeisti Ukrainos konstituciją ir sukurti alternatyvų valdžios centrą, siekiant padidinti Rusijos įtaką šalyje. Rusijos veiksmai Ukrainoje taip pat buvo skirti sukurti plačios paramos iliuziją kvazivalstybėms ir kitoms hibridinėms veikloms (Shandra & Seely, 2019).

Visapusiška gynyba apibūdinama kaip oficiali vyriausybės strategija, apimanti visos visuomenės integravimą siekiant apsaugoti valstybę nuo galimų grėsmių (NATO Special Operations Headquarters, 2020). Baltijos šalyse, priešinantis agresyvioms Rusijos priemonėms ir hibridiniam karui, taikoma visapusiška gynybos strategija, panaši į taikomą Šiaurės šalyse. Tuo siekiama stiprinti visuomenės atsparumą, stiprinti teisinę valstybę, kovoti su korupcija, integruoti rusakalbes mažumas, didinti energetinę nepriklausomybę ir infrastruktūros ryšius su Vakarų Europa. Akcentuojama, kad norint integruoti etninius rusus ir kovoti su Rusijos dezinformacija, reikia regioninių sąjungininkų ir partnerių pagalbos. Teigiama, kad Baltijos šalys turėtų įtraukti visus savo gyventojus į gynybą, kad

padidintų karinį personalą ir sukurtų įvairius iššūkius potencialiems užpuolikams. Jos taip pat turi kovoti su korupcija transporto sektoriuje ir teikti pirmenybę infrastruktūros projektams, tokiems kaip „Rail Baltica“ ir elektros sistemos sinchronizavimui su Europa (Bankauskaitė ir kt., 2020).

Estijos, Latvijos ir Lietuvos gynybos pastangos nuo 2014 m., yra orientuotos į karinę gynybą ir visuomenės atsparumą. Akcentuojamas pragmatiškas Baltijos šalių grėsmių suvokimas, karinių pajėgumų plėtra ir pilietinio atsparumo stiprinimas. Teigiama, kad nors buvo padaryta pažanga įgyvendinant visapusišką gynybą (angl. comprehensive defence), Estijoje, Latvijoje ir Lietuvoje dar reikia įveikti daugybę iššūkių. Lietuvos atveju minima, kad šalis 2016 metais priėmė karinę strategiją, kurioje pripažįstama įprastinės ginkluotos agresijos grėsmė ir pabrėžiama atgrasymo svarba. Lietuva daugiausia dėmesio skyrė gynybinių pajėgumų, įskaitant teritorinę gynybą, didinimui ir plėtojo visos visuomenės požiūrį į gynybą, įtraukdama švietimo ir mokymo veiklą, skirtą atsparumui ir pasipriešinimo įgūdžiams didinti. Buvo žymiai padidintas gynybos biudžetas, leidžiantis modernizuoti ginkluotąsias pajėgas ir plėtoti rezervo personalą. Šalis taip pat priėmė priemones, skirtas rengti visuomenę gynybai įskaitant aktyvaus pasipriešinimo vadovėlio parengimą ir nacionalinio saugumo ugdymo įtraukimą į mokyklų programas (Śliwa et al. 2021).

Švedijos pastangos, diegiant visapusiškos gynybos modelį apima ir visuotinės gynybos reikalavimų įgyvendinimą privačiame sektoriuje. Pabrėžtina, kad tai reikalauja paprastumo ir tinkamo išlaidų padengimo, kad būtų užtikrinta konkurencinė lygybė. Per didelė įmonių našta be atlygio gali pakenkti jų veikimui, o per didelės kompensacijos gali sutrikdyti laisvąją rinką. Teigiama, kad Švedijos konkurenciją reguliuojanti institucija turėtų užtikrinti, jog rinkos intervencijos būtų vienodos konkurencijos požiūriu. Turėtų būti naudojami viešųjų pirkimų konkursai, nediskriminuojant užsienio įmonių. Teigiama, kad integracija su kitomis valstybėmis ir tarptautinis bendradarbiavimas yra labai svarbūs tarptautiniams srautams ir tarpvalstybiniam bendradarbiavimui, o politinė atsakomybė ir informuotas strateginis vadovavimas yra būtini norint išspręsti sudėtingus iššūkius ir apsaugoti visuomenę nuo grėsmių (Lallerstedt, 2021)

Nagrinėjant civilinių ir karinių santykių vaidmenį tiekimo grandinės valdyme, pasirengimo ekstremaliųjų situacijų valdymui kontekste, ištyrus Švediją, Suomiją ir Lenkiją pabrėžiama civilinių ir karinių santykių svarba, suderinant saugos ir saugumo priemones bei reagavimą į sudėtingas ekstremalias situacijas bei grėsmes išsivysčiusiose šalyse. Veiksmingas civilinis ir karinis koordinavimas yra esminis, prižiūrint ir reguliuojant strategines atsargas bei vykdant ekstremalių situacijų valdymo operacijas. Atkreipiamas dėmesys į nuolatinius politikos pokyčius bei civilinių ir karinių santykių integravimą į pasirengimo ekstremalioms situacijoms planavimą. Be to, pabrėžiama

komunikacijos, valdymo bei koordinavimo civilių ir kariškių santykiuose svarba siekiant efektyvaus ekstremalių situacijų valdymo (Kaneberg, 2017).

Siekiant užkirsti kelią grėsmėms valstybės stabilumui ir suverenitetui - pasirengti joms, reaguoti į jas ir atsistatyti po to, kai šios grėsmės pasireiškė, svarbus visos visuomenės (angl. Whole-of-Society) požiūris ir būtinybė valstybėms integruoti visus nacionalinės galios elementus, įskaitant atskirus piliečius, siekiant veiksmingai atgrasyti arba apsiginti nuo šiuolaikinių grėsmių (NATO Special Operations Headquarters, 2020).

Atsparumo hibridinėms grėsmėms stiprinimui, kaip visapusiška atsparumo ekosistema, siūlomas CORE (angl. A Comprehensive Resilience Ecosystem) modelis. Jį sudaro tarpusavyje susiję elementai, apimantys demokratinius pagrindus, skirtingus domenus (tokius, kaip politinis, teisinis, diplomatinis, gynybos, ekonomikos, kibernetikos, kultūrinis ir t. t.) ir visuomenės sluoksnius. Pabrėžiama, kad ekosistemoje įgyvendinamos atsparumo priemonės gali teigiamai arba neigiamai paveikti kitus elementus dėl jų tarpusavio ryšio. CORE modelis yra pagalbinė strateginio planavimo priemonė, skirta politikos formuotojams nustatyti ir įgyvendinti tinkamas priemones, siekiant kovoti su hibridinių grėsmių poveikiu visuose visuomenės sektoriuose ir lygiuose (Jungwirth ir kt., 2023). Kalbant apie atsparumo hibridinėms grėsmėms sampratą, buvo nustatyta, kad laikui bėgant, literatūroje lankstumo samprata keitėsi. Iš pradžių buvo orientuojamasi į statišką sukrėtimų valdymo perspektyvą, atsispiriant jiems ir grįžtant į pusiausvyros būseną. Tačiau ši samprata išsivystė į labiau dinamišką požiūrį, kuris apima sukrėtimų įveikimą prisitaikant ir pereinant prie naujos stabilios pusiausvyros, artimos pradinei būsenai.

Pabrėžiama, kad kai atsparumo sąvoka verčiama iš kitų kalbų, tai nėra tik žodžių perkėlimo iš vienos kalbos į kitą procesas, tai taip pat yra ir kultūriniai skirtumai. Kiekviena šalis, kolektyvas ir žmonės skirtingai rezonuoja žodžius, todėl literatūra apie atsparumą ir jo supratimą skiriasi. Šie skirtumai taip pat išryškėja lyginant ne vakarietišką atsparumo analizę su Vakarų perspektyva (Jungwirth ir kt., 2023).

Įvairiomis kalbomis atsparumas siejamas su panašiomis sąvokomis, tokiomis kaip lankstumas, judrumas ir naujovės. Manoma, kad šie elementai yra būtini siekiant atsparumo hibridinėms grėsmėms (Jungwirth ir kt., 2023).

Apibendrinant, galima teigti, kad hibridinės grėsmės yra sudėtingos ir daugiasluoksnės, nes jos dažnai apima subtilias bei mažiau akivaizdžias taktikas, kurias galima palyginti su pilkosios zonos arba pilkosios zonos karybos strategijomis. Šios sąvokos apibūdina būdus, kuriuos naudoja priešiški veikėjai, siekdami išnaudoti spragas, susilpninti priešo pozicijas arba sukelia painiavą bei neaiškumą

konflikto zonose. Pilkoji zona yra sąvoka, kuriai būdingas neaiškumas dėl to, kas vyksta, o pilkosios zonos karyba apibūdina taktikas, kuriomis naudojantis priešas stengiasi veikti neakivaizdžiu būdu, neiššaukdamas tiesioginio karinio konflikto, bet kelia grėsmę saugumui ir stabilumui. Todėl, kalbant apie hibridines grėsmes, svarbu suprasti, kad jos neretai apima pilkosios zonos taktikas arba pilkosios zonos karybą. Minėtosios grėsmės gali apimti informacinį karą, ekonominį spaudimą, dezinformaciją ar įvairius netiesioginius veiksmus, kurie gali destabilizuoti politinę aplinką arba sukelti nesusipratimus bei konfliktus, net neprasidėjus tiesioginiams kariniams veiksmams. Į tai reikia atsižvelgti siekiant sukurti efektyvius atsako ir prevencijos mechanizmus. Rusijos veiksmai Ukrainoje nuo 2013 m. parodo, kad valstybės atsparumas hibridinėms grėsmėms yra svarbus, siekiant išvengti politinės įtakos ir prijungimo prie kitų šalių. Ukrainos artėjimas prie Vakarų buvo vertinamas kaip grėsmė Rusijos interesams, todėl Kremlius naudojo hibridinius metodus siekdamas išlaikyti kontrolę. Kremlius įkūrė kvazivalstybes Donecke ir Luhanske, siekdamas destabilizuoti Ukrainos valdžią ir sukurti alternatyvą oficialiam Ukrainos valdžios centrui. Tokios veiklos priešpriešos valstybėje kūrimas stipriai iškreipė Ukrainos politinę, ekonominę ir socialinę struktūrą, todėl valstybės atsparumas yra būtinas siekiant išvengti tokios destabilizacijos. Valstybės atsparumas hibridinėms grėsmėms yra svarbus, kad būtų galima užtikrinti teisingus ir nepriklausomus rinkimus bei apsaugoti demokratiją nuo tokių kišimosi bandymų. Tai parodo, kad valstybės bei piliečių atsparumas dezinformacijai, manipuliacijoms ir kitoms hibridinėms priemonėms yra svarbus atsparumo hibridinėms grėsmėms elementas. Šios priemonės yra orientuotos į trijų Baltijos šalių atsparumo didinimą, sumažinant priklausomybę nuo Rusijos energetikos ir atgrasant nuo agresijos. Visgi, verta pastebėti, kad nėra skiriamas pakankamas dėmesys visos vyriausybės įtraukimui į atsparumo hibridinėms grėsmėms sistemą. Taigi, Švedijoje į hibridinių grėsmių valdymą žvelgiama šiek tiek plačiau, nei Baltijos šalyse, apimant privataus sektoriaus įtraukimą, integraciją su kitomis valstybės institucijomis bei pabrėžiant politinės vadovybės informuotumo svarbą.

1.2. Hibridinės grėsmės Lietuvoje

Lietuvoje pastaruoju metu padaugėjo nelegalių sienos kirtimų ir prieglobsčio prašymų. Šiais žmonių srautais užsienio veikėjai manipuliavo kaip politinio spaudimo ir destabilizavimo įrankiu. Lietuva į tai atsakė stiprindama sienų kontrolę ir bendradarbiaudama su tarptautiniais partneriais, siekdama pašalinti pagrindines migracijos priežastis. 2023 metų balandžio 25-ąją Lietuvos Respublikos Seimas įstatymu įtvirtino neteisėtų migrantų apgręžimo galimybę pasienio ruože. „Migracijos per Baltarusiją maršrutas tapo vienu iš kelių nelegaliai patekti į Europą. Sąlygas

nelegaliai migracijai sudaro ne tik žmonių gabentojai, bet ir Baltarusijos pasienio pareigūnai. Tarp į Lietuvą patenkančių nelegalių migrantų nustatoma ryšių su teroristinėmis organizacijomis turinčių asmenų“(VSD ir AOTD, 2023). „Baltarusijos ir Rusijos režimai naudojasi žmonių gabentojų veikla ir nelegalių migrantų tranzitu per savo teritorijas dėl politinių tikslų. Abiejų šalių režimai siekia nubausti ES ir konkrečias jos nares už jų politinę poziciją, kritiką, sankcijas ir kitus esą priešiškus veiksmus. Labai tikėtina, kad 2023 m. Rusija, pasinaudodama migrantais, darė politinį spaudimą Suomijai, reaguodama į šios politiką Rusijos atžvilgiu: ekonomines sankcijas dėl jos agresijos prieš Ukrainą, visokeriopą paramą Ukrainai, narystę NATO. Kaip ir prieš aštuonerius metus, Rusijos režimas dar kartą pasinaudojo migrantais kaip įrankiu, siekdamas priversti kaimynines valstybes prašyti derybų su Maskva. Labai tikėtina, kad artimoje perspektyvoje Baltarusijos režimas dėl politinių tikslų išliks suinteresuotas nelegalia migracija spausti Latviją, Lietuvą ir Lenkiją. Nelegalios migracijos iš Baltarusijos į ES tendencijos nuolat keičiasi – tiek migrantai, tiek žmonių gabentojai reaguoja į situaciją visame ES pasienyje. Artimiausioje pers- pektyvoje labai tikėtina, kad į ES nelegaliai patekti ketinantys migrantai iš kilmės šalių atvyks į Baltarusiją per Rusijos teritoriją – tai patvirtino ir Suomijos atvejis” (VSD ir AOTD, 2024).

„Rusijos žvalgybų kibernetiniai pajėgumai ne tik patys naudoja dažnai kriminaliniam pasauliui priskiriamus įrankius, bet ir bendradarbiauja su valstybiniam sektoriui nepriklausančiais programišiais. Dalis kriminalinio pasaulio programišių, atsakingų už atakas prieš svarbius ekonominius objektus, teikia užsakomųjų *ransomware* atakų paslaugą: programišiai, naudodami savo turimą infrastruktūrą ir įrankius, automatiškai užšifruoja duomenis. Taip tikrasis atakos užsakovas lieka nežinomas”(Lietuvos Respublikos Krašto apsaugos ministerija, 2021).

„2021 m. ir toliau buvo matomos prieš Lietuvą nukreiptos hibridinės veiklos, kai naudojama įvairių kibernetinių incidentų elementų, tendencijos. Daugiausia fiksuota įsilaužimų į savivaldybių administracijų interneto svetaines, išskirtinai naudojantis lietuviškos įmonės turinio valdymo sistemos spragomis. Kaip ir ankstesniais metais, įvykdžius įsilaužimus, savivaldybių svetainėse buvo skelbiamos melagienos jautriomis Lietuvai temomis. Tiksliniams adresatams buvo siunčiami imituojantys el. laiškai (angl. email spoofing) su melagienomis. Be šių pasikartojančių atvejų, 2021 m. pastebėta nauja tendencija, susijusi su hibridine veikla ir kibernetiniais incidentais, – tai melagingos informacijos platinimas nevykdant kibernetinių įsilaužimų” (Lietuvos Respublikos Krašto apsaugos ministerija, 2021). Už kibernetinį saugumą yra atsakingas Lietuvos kariuomenės Nacionalinis kibernetinio saugumo centras.

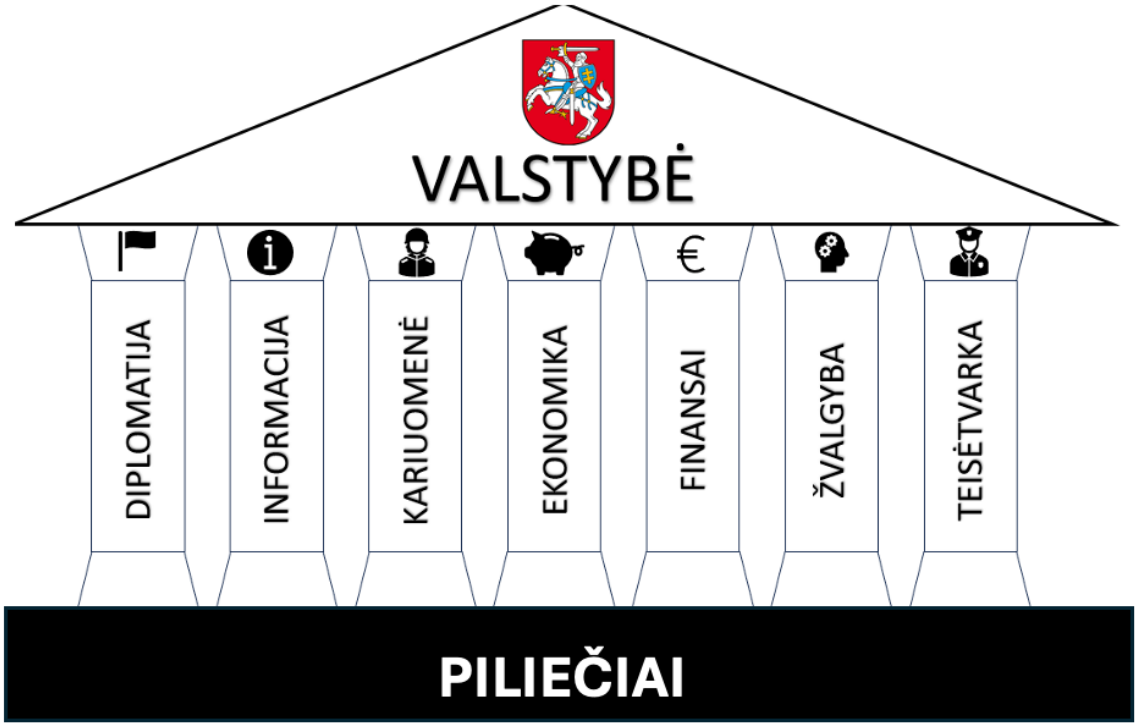
Kinijos ekonominė įtaka iškilo kaip pagrindinis Lietuvos rūpestis, nes šalis siekia subalansuoti savo ekonominius interesus su nacionalinio saugumo prioritetais. Kinijos investicijos į strateginius sektorius, tokius kaip energetika ir telekomunikacijos, sukėlė susirūpinimą dėl galimo šnipinėjimo ir kibernetinių grėsmių. Vilniuje atidarius Taivano atstovybę, Kinija reagavo ekonominiu spaudimu ir ribojimais Lietuvos verslo įmonėms. Lietuva į tai atsakė stiprindama investicijų patikros mechanizmus ir diversikuodama ekonomines partnerystes su kitomis šalimis.

Dar viena, verta paminėti, grėsmė, yra neišprovokuotas Rusijos karas prieš Ukraina, keliantis tiesioginį saugumo iššūkį Lietuvai, kaip šio regiono valstybei. Krymo aneksija ir besitęsiantis konfliktas Rytų Ukrainoje sukėlė susirūpinimą dėl agresyvios Rusijos užsienio politikos ir galimų grėsmių regiono saugumui. Lietuva į tai atsakė didindama investicijas gynybai, stiprindama karinius pajėgumus ir glaudžiai bendradarbiaudama su NATO sąjungininkais, siekdama atgrasyti nuo galimos agresijos.

Lietuva priklauso didžiausiam pasaulyje kariniam aljansui – NATO, taip pat yra Europos Sąjungos nare. Remiantis Strateginių ir tarptautinių studijų centro pateikiama informacija, NATO karinis biudžetas ($1,175 trln.) yra 17,8 karto didesnis, nei Rusijos (CSIS, 2022), todėl, siekiant daryti įtaką valstybėms, kurios yra šio aljanso narės, ieškoma alternatyvių metodų, dažnai pasitelkiant šiuolaikinio pasaulio teikiamų pranašumų silpnąsias vietas. Tai pastebi ir Žilinskas (2017), pabrėždamas, kad dėl visuminių resursų disbalanso, hibridinių priemonių panaudojimo prieš NATO valstybes tikimybė padidėja. Marsh ir Searle (2023) atkreipia dėmesį, kad veikimas pilkojoje zonoje Rusijos Federacijai yra kaštų mažinimo ir rizikų valdymo priemonė.

Roberts (2015) teigia, kad siekiant apsiginti nuo hibridinių grėsmių, būtina suformuoti doktrininį požiūrį, apimantį visos vyriausybės priemones (angl. whole-of-government). Šiame požiūryje turėtų būti naudojami tradiciniai valstybės galios elementai: diplomatinis, informacinis, karinis ir ekonominis. Siekiant sistemiškai įvertinti hibridines grėsmes Lietuvos Respublikai, būtina jas (grėsmes) išanalizuoti iš valstybės galios šaltinių perspektyvos. Tai suteiks galimybę susidaryti išsamesnį vaizdą. Valstybės galios šaltinius yra įprasta skirstyti į diplomatiją, informaciją, karinę galią, ekonomiką, finansus, žvalgybą, teisėtvarka. Tam naudojama abreviatūra DIMEFIL (angl. Diplomatic, Information, Military, Economic, Finance, Intelligence, Law enforcement).

1 paveikslas *Valstybės galios šaltiniai*



Sudaryta autoriaus

Kaip pavaizduota 1 paveiksle, tai yra tarsi ramsčiai, užtikrinantys valstybės stabilumą, kurių pagrindas yra visuomenė arba piliečiai.

Taigi, galima teigti, kad hibridinės grėsmės gali būti apibūdinamos kaip valstybinių ir nevalstybinių veikėjų pastangos siekiant priversti Lietuvą vykdyti jų valią, oficialiai to nedeklaruojant, per visą DIMEFIL spektrą. Šios grėsmės gali būti tiek žinomos, tiek nežinomos ir netikėtos:

Diplomatija: hibridinės grėsmės per diplomatinį valstybės galios šaltinį gali apimti įvairias priemones, pavyzdžiui, dezinformacijos kampanijos, propaganda, netikros vėliavos operacijos (angl. false flag operation). Pastaroji yra šiuo metu pakankamai dažnai vykdoma, sukuriant įspūdį, kad kažkoks veiksmas buvo įvykdytas kitos šalies, nei tikrasis vykdytojas. Visų šių priemonių tikslas yra destabilizuoti vienos valstybės santykius su kitomis valstybėmis arba sukurti įtampą tarp sąjungininkų. Su Lietuva susijusio diplomatinio poveikio pavyzdys yra kai „reaguodamas į Lietuvos suteiktą prieglobstį iš Baltarusijos pasitraukusiai opozicijos lyderei Sviatlanai Cichanouskajai, A. Lukašenka išsiuntė iš Minsko beveik visus Lietuvos diplomatus“ (VSD ir AOTD, 2023).

Informacija: įtaka per informacinį lauką daroma kasdien. Jos tikslas – paveikti viešąją nuomonę arba primest i tam tikrą naratyvą. Tai gali apimti dezinformaciją, duomenų vagystes arba kibernetines atakas, tokias, kaip periodines prieigos trikdymo, arba DDos (angl. distributed denial of service). Informacinė erdvė gali būti pasitelkiama formuoti viešąją nuomonę bei sukurti visuomenės paramos iliuziją. Manipuliavimo viešąja nuomone pavyzdžius galima stebėti ir Lietuvos viešojoje erdvėje, kai kurie iš jų tapo socialinės poliarizacijos visuomenėje priežastimis ir net peraugo į fizinius susidūrimus su policijos pareigūnais. „Informacinis karas yra viena iš Rusijos konfrontacijos su Vakarais sudedamųjų dalių. Jį Rusija vertina kaip nuolatinę veiklą, nukreiptą prieš oponentus, kurių vykdomą politiką traktuoja kaip prieštaraujančią jos strateginiams interesams. Rusija nuolat vykdo kompleksines informacines kampanijas, apimančias psichologines įtakos ar informacines-kibernetines operacijas, kuriomis, siekiant paveikti auditorijų mąstymą, požiūrį ir elgseną, ne tik skleidžiama tikrovės neatitinkanti informacija, tačiau naudojamasi ir kibernetiniu ar kinetiniu elementu” (VSD ir AOTD, 2024). Karinė agresija prieš Sakartvelą buvo viena pirmųjų, kur veiksmai kibernetinėje erdvėje buvo koordinuojami ir vykdomi kartu su kinetinėmis operacijomis (Kilcullen, 2020). Dezinformacija, politinė propaganda ir manipuliavimas suvokimu nėra naujiena, bet technologinės naujovės sumažino konfliktų sąnaudas ir pavertė juos pražūtingais, net nesant tradicinės karinės kampanijos (Arcobasso, 2020).

„Informacinėms operacijoms vykdyti 2022 m. buvo pasitelktos pačios įvairiausios priemonės ir šiuolaikinės technologijos. Kaip įrankiu propagandai skleisti naudotasi Rusijos ir Baltarusijos valstybiniais bei Vakarų auditorijoms skirtais kontroliuojamais informacijos sklaidos kanalais,

kibernetinės atakos vykdytos derinant su melagienų (angl. fake news) sklaida. Dažnu atveju priešiškos ir (ar) nedraugiškos informacinės veiklos skleidėjais 2022 m. tapdavo Rusijos ir Baltarusijos politikai, diplomatai, aukšto rango karininkai ir valstybės institucijų atstovai, taip pat tariami kariniai ar politiniai ekspertai. 2022 m. informaciniai incidentai prieš Lietuvą ir valstybės interesus dažniausiai buvo vykdomi per interneto naujienų portalus bei socialinius tinklus [...] 2022 m. fiksuota daugiausia unikalių informacinių atvejų sausio, gegužės, birželio, liepos, rugpjūčio, spalio mėn. Gynybos temų eskalacija 2022 m. išaugo beveik dvigubai: 2021 m. fiksuoti 26,42 proc. visų unikalių atvejų, o 2022 m. – 47,91 proc. Tai sutapo su reikšmingais užsienio ir šalies vidaus įvykiais, kuriuos Lietuvai nedraugiški informacijos šaltiniai siekė išnaudoti neigiamam šalies įvaizdžiui Vakaruose kurti ir Lietuvos visuomenės auditorijų tarpusavio susipriešinimui skatinti" (Lietuvos Respublikos Krašto apsaugos ministerija, 2022). „Kare prieš Ukrainą Rusija siekia nekonvencinėmis priemonėmis paveikti Vakarų ryžtą remti Kyjivą. Dėl savo nuolatinės paramos Ukrainai, narystės NATO ir strategiškai jautrios geografinės padėties Lietuva atsiduria Rusijos vykdomų kibernetinių operacijų taikinyje" (VSD ir AOTD, 2024). „Nuo 2023 m. fiksuojamas akivaizdus informacinių atakų kiekybinis ir kokybinis pokytis. Prieš Lietuvą, Latviją, Estiją ir Lenkiją įvykdytos savo pobūdžiu ir mastu beprecedentės informacinės operacijos, apimančios ir kinetinius veiksmus, kuriais siekiama konsoliduoti operacijų poveikį. Palyginti su ankstesnėmis atakomis, šios informacinės operacijos pasižymėjo agresyvumu, jomis siekta kelti regiono šalių visuomenių baimę ir paniką, trikdyti valstybės institucijų darbą, skatinti visuomenių nepasitenkinimą valstybės sprendimais ir viešojo saugumo užtikrinimu. 2023 m. atakos prieš Lietuvą, Latviją, Estiją ir Lenkiją sukėlė juntamą poveikį visuomenei, joms suvaldyti reikėjo panaudoti daug valstybės institucijų resursų" (VSD ir AOTD, 2024).

Karinė galia: Pastarųjų kelių dešimtmečių tendencija yra pasitelkti privačias karines ir saugumo kompanijas. Vakarų valstybės taip pat naudoja šias kompanijas, tačiau neįtraukia jų į karinius veiksmus, pasitelkdamos jas karinio mokymo ar apsaugos funkcijoms. Tuo tarpu Rusijos Federacijos veiksmai Artimuosiuose Rytuose atskleidžia kitokias tendencijas, kai šios kompanijos pasitelkiamos aktyviuose kariniuose veiksmuose, suteikiant joms karinius resursus bei kovinę techniką. Lietuvos Valstybės saugumo departamento bei Antrojo operatyvinių tarnybų departamento prie KAM vertinimu, Rusijos privačios karinės ir saugumo tarnybos galėtų būti pasitelktos operacijoms Lietuvoje, atliekant taikinių žvalgybą ir identifikavimą, diversinius veiksmus, sabotažą ar kurstant neramumus visuomenėje (VSD ir AOTD, 2023). Daugelis įgaliotų konfliktų yra nepaskelbti, kaip ir tie, kurie įvyko devintajame XX a. dešimtmetyje Centrinėje Amerikoje ir

Afganistane. Taip pat yra šiandien Ukrainoje, pavyzdžiui, buvimas vadinamųjų „mažųjų žaliųjų žmogeliukų“ – ginkluotų nežinomų Rusijos specialiųjų grupuočių pajėgų, veikiančių šios šalies rytuose (Pathe Duarte, 2020, cituoja pagal Balasevičių). „Baltijos jūros regione Rusija yra priversta naudoti kitus komponentus (oro ir jūrų) ir branduolinio ginklo pajėgumus, kad pademonstruotų savo karinį potencialą ir atgrasymą. Pavyzdžiui, 2023 m. pirmą kartą vyko „Kalibr“ raketų sistemomis ginkluotų kovos laivų kovinė tarnyba Ladogos ežere, tikėtina, siekiant demonstruoti nepasitenkinimą Suomijos naryste NATO. Be to, 2023 m. buvo fiksuoti net penki Rusijos sunkiųjų bombonešių Tu-22M3 skrydžiai virš Baltijos jūros, kai 2022 m. tokių skrydžių nebuvo vykdoma. 2023 m. vasarą V. Putinas ir A. Lukašenka viešai pareiškė apie Rusijos nestrateginio branduolinio ginklo (NSBG) dislokavimą Baltarusijos teritorijoje” (VSD ir AOTD, 2024).

Ekonomika: hibridinės grėsmės šioje srityje gali būti susijusios su energetinio priklausomumo išnaudojimu, ekonominio spaudimo darymu, įtaka per investicijas ar prekybos blokavimu. Ekonomika ir energetika yra plačiai paplitęs įtakos darymo įrankis. Tarp pavydžių verta paminėti Rusijos Federacijos naudojamus energetinės priklausomybės svertus prieš kitas valstybes bei Kinijos liaudies respublikos atsaką į Taivano atstovybės atidarymą Vilniuje, kai buvo blokuotas kiniškų prekių tiekimas Lietuvos verslo įmonėms. „Kinijos režimas siekia užsitikrinti prieigą prie Vakaruose vystomų technologijų ir joms kurti reikalingų žinių, kurios padėtų didinti Kinijos ekonomikos konkurencingumą ir spartintų šalies karinį modernizavimą. Šiam tikslui Kinijos režimas panaudoja tiek tradicinių žvalgybos tarnybų pajėgumus, tiek jų koordinuojamą neformalų rinkikų tinklą. Pavyzdžiui, įgyvendindamas karinio ir civilinio sektoriaus sintezės politiką, KKP (Kinijos komunistų partijos – autoriaus pastaba) režimas naudojasi su Kinijos gynybos sektoriumi siejamais universitetais technologiniam šnipinėjimui ir užmaskuotam technologijų ir žinių perėmimui. Dėl prievolės bendradarbiauti su žvalgybos tarnybomis užsienyje dirbantys ar besistažuojantys Kinijos mokslininkai ir studentai tampa potencialiais Kinijos žvalgybos taikiniais” (VSD ir AOTD, 2024).

“Rusija, prieš imdamasi karinių veiksmų, mažino gamtinių dujų eksportą į Europą, siekdama didinti įtampą energetikos sektoriuje, o pradėjusi karą prieš Ukrainą ėmėsi papildomų manipuliacijų gamtinių dujų tiekimu. Kremliui nurodžius, koncernas „Gazprom“ vienašališkai įpareigojo ES šalių klientus už tiekiamas dujas atsiskaityti tik Rusijos rubliais, o šalims, kurios atsisakė tai daryti, „Gazprom“ nutraukė gamtinių dujų tiekimą. Prieš incidentus, pažeidusius dujotiekių „Nord Stream“ infrastruktūrą, koncernas mažino gamtinių dujų tiekimą ES šalims, nes tai esą lėmė techninės aplinkybės” (VSD ir AOTD, 2023).

„Rusijos ir Baltarusijos subjektai turi interesų įgyti prieigą prie Lietuvai strategiškai svarbios infrastruktūros ar turėti įtakos strategiškai svarbiuose šalies ūkio sektoriuose. Rusija yra itin suinteresuota rinkti informaciją apie pažeidžiamas strateginės infrastruktūros vietas, situaciją strategiškai svarbiuose sektoriuose veikiančiose kompanijose, jų įgyvendinamus projektus. […] Rusija deda daug pastangų tarptautinėms sankcijoms apeiti – kuria naujas sankcijų apėjimo schemas, kuriose dalyvauja ir Rusijos žvalgybos tarnybos, naudojasi ryšiais su ES šalyse veikiančiomis kompanijomis, pasitelkia Rusijos ir Baltarusijos piliečius. Kai kurios Lietuvoje veikiančios įmonės, aiškiai suprasdamos, kad padeda Rusijos subjektams išvengti sankcijų, tęsia bendradarbiavimą su jais ir bando organizuoti įrangos, technologijų ir kitos produkcijos eksportą į Rusiją. [..] Visos Rusijos žvalgybos tarnybos – Rusijos užsienio žvalgybos tarnyba (SVR), Rusijos ginkluotųjų pajėgų Generalinio štabo Vyriausioji valdyba (GRU) ir Rusijos federalinė saugumo tarnyba (FSB) – dalyvauja organizuojant ribojamų prekių importą į Rusiją. […] Artimoje perspektyvoje Rusijai patiriant sunkumų dėl jai taikomų sankcijų, Rusijos žvalgybos tarnybos, labai tikėtina, dar aktyviau ieškos būdų įsigyti ir į Rusiją pristatyti trūkstamus įrenginius, produkciją ar naujas technologijas. Labai tikėtina, kad Rusijos žvalgybos tarnybos, organizuodamos tokios produkcijos patekimą į Rusiją, naudosis Lietuvoje veikiančiomis prekių tiekimo grandinėmis, logistikos infrastruktūra ar iš sankcijų apėjimo schemų pasipelnyti norinčiais asmenimis“ (VSD ir AOTD, 2024).

Žvalgyba: Lietuvos Respublikos Valstybės saugumo departamentas ir Antrasis operatyvinių tarnybų departamentas prie KAM nuolat fiksuoja bei savo ataskaitose pateikia informaciją apie užsienio žvalgybos tarnybų priešišką veiklą Lietuvoje. Tai apima šnipinėjimą, intelektinės nuosavybės vagystes bei asmenų verbavimą, siekiant daryti įtaką politiniams ar socialiniams procesams šalies viduje. VSD ir AOTD (2023) Grėsmių Nacionaliniam saugumui vertinime skelbiama, kad nors Rusijos žvalgybos tarnybų veiklos intensyvumas Lietuvos Respublikoje yra sumažėjęs dėl pajėgumų perkėlimo į Ukrainą, šios grėsmės vis dar yra fiksuojamos. Lietuvoje taip pat veikia ir kitų valstybių žvalgybos tarnybos. „2022 metais iš Lietuvos buvo išsiųsti penki su diplomatine priedanga dirbę Rusijos žvalgybos pareigūnai. Vis dėlto, VSD vertinimu, kitų Rusijos žvalgybos tarnybų veiklos krypčių – informacinių operacijų, radioelektroninės ir kibernetinės žvalgybos – intensyvumas išlieka aukštas […] 2022 metais fiksuota Rusijos, Baltarusijos ir Kinijos ŽST (žvalgybos ir saugumo tarnybų – autoriaus pastaba) žvalgybinė veikla Lietuvoje. Nustatyta keletas atvejų, kai Rusijos, Baltarusijos ar Kinijos žvalgybos ir saugumo tarnybos bandė verbuoti Lietuvos piliečius, tačiau nė vienas iš jų nebuvo sėkmingas” (VSD, 2022).

Kalbant apie hibridines grėsmes per **teisėtvarkos** elementą, kaip valstybės galios šaltinį, galima išskirti tarptautinių nusikalstamų organizuotų grupių veiklą, kurios veikia ir kurioms įtaką daro Rusijos žvalgybos tarnybos. Tokios grupuotės gali dalyvauti nelegalioje prekyboje, įskaitant prekybą narkotikais, žmonėmis ir ginklais, pinigų plovimo operacijose, kontrabandoje arba kitose nusikalstamose veiklose. Nors paprastai jų tikslas yra finansinė nauda, tačiau jos gali būti pasitelkiamos destabilizuoti Lietuvos teisėtvarkos institucijas bei sukelti neramumus ir netvarką šalyje. Ryškiausias ir naujausias pavyzdys Lietuvoje yra nelegalių migrantų instrumentalizavimas. „2021 m. vasarą Baltarusijos valdžia pradėjo operacijas, nukreiptas į rytines Europos Sąjungos (ES) šalis. Sienos tarp Baltarusijos ir Lietuvos, Latvijos bei Lenkijos tapo tam tikra ES fronto linija kai tūkstančiai migrantų, daugiausia iš Vidurio Rytų ir Šiaurės Afrikos, per Baltarusiją buvo perkeliami į šias tris ES šalis. Pastarosios itin aktyviai pasisakė prieš Baltarusijos lyderio Aliaksandro Lukašenkos režimą, 2020 m. rugpjūtį suklastotus prezidento rinkimus, šalyje aktyviai pažeidžiamas žmogaus teises. Reaguodama į įvykius Baltarusijoje, ES įvedė ir palaipsniui plėtė sankcijas. Lukašenkos atsakas į tai – dirbtinai sukelta migracijos krizė, migrantų srauto nukreipimas į Rytines ES šalis ir spaudimas prie ES išorės sienos. Organizuojant nelegalią migraciją, dalyvavo tiek Baltarusijos valstybės institucijos, tiek finansine nauda suinteresuotas turizmo sektorius" (Gecaitė, 2023). "Hibridinės atakos naratyvas grindžiamas 2021 m. gegužės 26 d. A. Lukašenkos viešu pasisakymu, kuriuo pagrasinta „užtvindyti Lietuvą ir kitas kaimynines valstybes migrantais ir narkotikais" (Radzevičiūtė, 2023). „Galima manyti, kad Baltarusija veikia kaip Rusijos politikos atstovė (angl. *proxy*), ypač vertinant vykdomą politiką ES atžvilgiu" (Gecaitė, 2023). Veikimas per atstovus yra pagrindinė pilkosios zonos karo priemonė, padedanti pakeisti *status quo* ir išlaikyti neapibrėžtumą. Agresoriai (valstybiniai ir nevalstybiniai veikėjai) išnaudoja esamas visuomenės politines, ekonomines ir etnines lūžių linijas, remdami elementus, kurie turi panašių interesų. (Mahmood Azad et al., 2023, cituoja pagal Wirtz). „Veikimas per atstovus sukuria neaiškumų dėl grėsmių šaltinių ir jų tikslų, o tai, savo ruožtu, pažeidžia besiginančiojo atgrasymo mechanizmus. Atstovų panaudojimas taip pat apsunkina atgrasymo strategijas, nes besiginantysis turi peržiūrėti savo atgrasymo mechanizmus, siekiant apsisaugoti nuo neapibrėžtų veikėjų ir nežinomų jėgų, kurios inicijavo *status quo* pasikeitimą. Pilkosios zonos agresoriai taip pat gali pasitelkti nusikalstamas organizacijas ir tinklus, siekdami įvairių tikslų: formuoti viešąją nuomonę, kurti dviprasmiškumą ir apsirūpinti resursais per kontrabandą ir organizuotą nusikalstamumą" (Mahmood Azad et al., 2023, cituoja pagal Chambers). Sukarintų grupuočių, turinčių ryšių su organizuotu nusikalstamumu ar be jų, rėmimas yra klasikinis *modus operandi*. Pavyzdžiui, Rusijos „Naktinių vilkų" atvejis, kai taip

besivadinantis motociklininkų klubas propaguojantis ekstremistinius bei ultranacionalistinius idealus, tikėtina, yra išnaudojami Kremliaus tikslams paveikti civilius gyventojus, eskaluojant visuomenę skaldančias problemas. Šis klubas dalyvavo Krymo krizėje, ruošiantis Maskvos inicijuotam referendumui. Taip pat yra „Rusijos ortodoksų armijos“, kuri skatina ultranacionalistines nuotaikas ir reiškia pasipiktinimą Vakarų įtaka regione, panaudojimo atvejis. Grupė mokoma atlikti karinius veiksmus pavyzdžiui, žvalgyba, gynyba ir snaiperių operacijos (Pathe Duarte, 2020, cituoja pagal Treverton). „Nustatyta atvejų, kai sankcijų apėjimo schemas organizavo Rusijos piliečiai, Lietuvoje neįsteigę ir nevaldantys kompanijų, tačiau įgiję leidimus gyventi šalyje. Jie dažniausiai atlieka tarpininkų vaidmenį – bando užmegzti ryšius su Lietuvoje veikiančiomis Rusijai reikiama įranga prekiaujančiomis ar ją gaminančiomis įmonėmis. Sankcijų apėjimo schemas organizuoja ir Rusijos piliečiai, palaikantys ryšius su Lietuvos organizuotų nusikalstamų grupuočių nariais, taip pat Lietuvos piliečiai, dalyvaujantys organizuoto nusikalstamumo veikloje, turintys ryšių Rusijoje ir dažnai keliaujantys į šią šalį” (VSD ir AOTD, 2024).

1 lentelė *Valstybės galios šaltiniai ir už juos atsakingos institucijos*

DIPLOMATIJA	URM, Prezidentūra
INFORMACIJA	LRV kanceliarijos Strateginės komunikacijos skyrius, SKD NKSC
KARIUOMENĖ	LK, KAM, VSAT
EKONOMIKA	EIM, FINMIN
FINANSAI	EIM, FINMIN
ŽVALGYBA	VSD, AOTD
TEISĖTVARKA	Lietuvos policija, Prokuratūra, Kriminalinė žvalgyba

Šaltinis: (sudaryta autoriaus, remiantis literatūros analize)

Dėl hibridinių grėsmių pobūdžio, pirmieji, kurie į jas reaguoja, yra taktinio lygmens vadai ar civilinių agentūrų atstovai. Jų reakcija, kuri dažnai nėra pagrįsta strategija, gali neigiamai paveikti nacionalinius ir tarptautinius tikslus. Be to, informacinės aplinkos formavimas pasitelkiant įvairias pastangas – nuo įprastų naujienų iki socialinės žiniasklaidos (Coombs, 2023). Tai veda prie išvados, kad būtina apsvarstyti skirtingus, tikėtinos prievartos mechanizmus, kuriose naudojami visi nacionalinės galios elementai (įskaitant diplomatinę, ekonominę, karinę ir informacinę/technologijas), siekiant įtvirtinti gynybą pilkojoje zonoje. Tai ne perėjimas prie puolamosios mąstysenos, o veikiau atgrasymo stiprinimas, naudojant ribotas galimybes, kurios yra skirtos sustabdyti priešiškus veiksmus dar prieš jų imantis ir atkurti pusiausvyrą, kad būtų galima pradėti derybas iš galios pozicijų (Allem ir kt., 2023).

Sistemų dinamiškumas

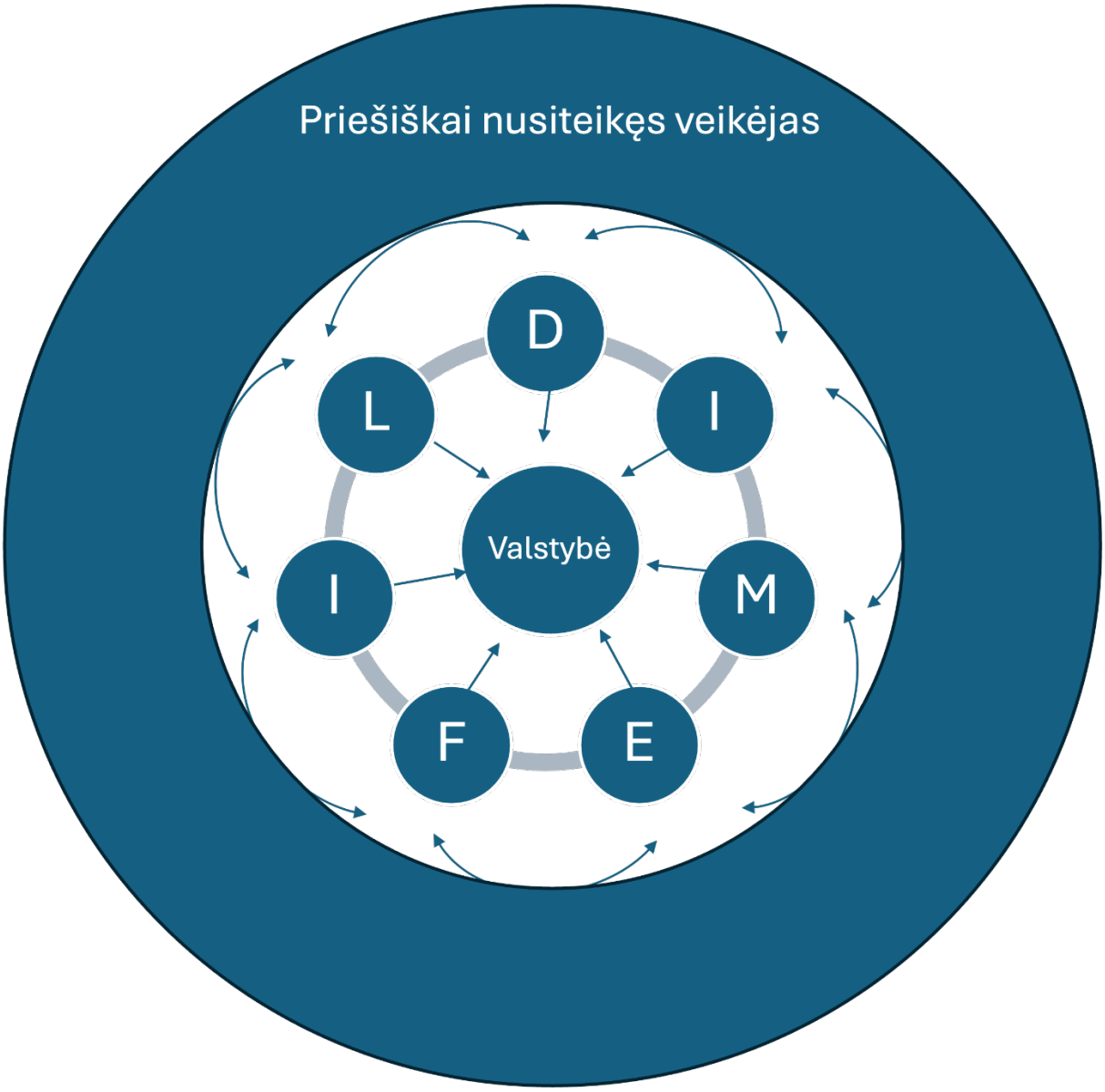
Pastebima, kad hibridinės grėsmės sparčiai keičiasi, plečiasi ir didėja jų sudėtingumo lygis. Atsparumas šioms grėsmėms turėtų būti kuriamas ir įgyvendinamas visais lygiais, atsižvelgiant į atsparumo priemones ne tik iš kelių valstybės galios šaltinių perspektyvos, bet pasitelkiant visapusišką sisteminį požiūrį. Kitaip tariant, stiprinant atsparumą hibridinėms grėsmėms, svarbu ne tik žvelgti į atsparumą atskirose srityse, bet ir atsižvelgti į priklausomybes bei tarpusavio sąveiką tarp skirtingų visuomenės dalių (Jungwirth ir kt., 2023). Sistema, plačiuoju apibrėžimu, susideda iš sąveikaujančių elementų, sukuriančių elgseną visos sistemos mastu. Žmonių visuomenės yra sudėtingos sistemos, atsirandančios dėl asmenų ir institucijų sąveikos. Institucijos apima formalias ir neformalias taisykles, normas ir organizacines struktūras, kurios laikui bėgant vystosi. Kompleksinėse sistemose visuma turi savybių, kurių jos dalyse nėra, pavyzdžiui, visuomenės normos ir struktūros. Perėjimas nuo individų prie bendruomenių atskleidžia tapatybės ir vaidmenų aspektus socialiniame kontekste. Kompleksinėse sistemose yra atsirandančios, savaime organizuotos hierarchijos, kurios prisitaiko prie jų aplinkos. Šių sistemų ribos nėra griežtos, palengvinančios sąveiką su kitomis sistemomis ir aplinka net ir esant fiziniams atstumams, kaip matyti iš sąveikos socialiniuose tinkluose (De Coning, 2021).

De Coning (2021) pateikia kompleksinių, prisitaikančių sistemų teorijos taikymą, siekiant suprasti žmonių visuomenių reakciją į sutrikimus, tokius kaip hibridinės grėsmės. Tai pabrėžia būdingą socialinių sistemų sudėtingumą, kurioms būdingos atsirandančios savybės ir savaime besiorganizuojantis elgesys. Skirtingai nuo sudėtingų sistemų, kompleksinės sistemos negali būti visiškai suprantamos analizuojant atskirus jų komponentus. Sudėtingų sistemų nenuspėjamumas kelia iššūkių planuojant ir valdant atsaką į grėsmes. Taip pat pabrėžiamas intervencijų į kompleksines sistemas ir netiesinės dinamikos vaidmuo, sukeliant nenumatytas pasekmes.

Apibendrinant, verta dar kartą pabrėžti, kad šios grėsmės dažniausiai yra naudojamos kombinuotai. Galima prisiminti nelegalių migrantų atvejį Lietuvoje. Pasitelkiant **informacinį** lauką bei išnaudojant atskirų socialinių grupių nepasitenkinimą valstybės vykdoma politika, buvo sustiprintas visuomenės nepasitenkinimas, išnaudojant šį nepasitenkinimą, buvo surengtas protestas prie Seimo, tarp kurio organizatorių buvo ir asmenų susijusių su neteisėta veika (**teisėtvarka)** bei išprovokuoti neramumai, išsivystę į riaušes. Tuo pačiu metu nelegalių migrantų stovykloje, tikėtina, koordinuojant tarptautinėms nusikalstamoms organizacijoms, užsienio **žvalgybos** tarnybų užsakymu, buvo sukelti neramumai, taip pat išsivystę į riaušes. Tai sukėlė didelį krūvį **teisėtvarkos** pareigūnams bei išskaidė pajėgas. Žvelgiant iš ilgalaikės perspektyvos, būtina atkreipti dėmesį, kad tokie veiksmai turi įtakos politiniams procesams šalies viduje (artėjantys rinkimai) bei tarptautinėje arenoje (vėlesnės

pastangos delegitimizuoti Lietuvos Respublikos pastangas valdant nelegalių migrantų krizę). Poveikis per kitas valstybes ir tarptautines institucijas išryškina, kad valstybė yra ne uždara sistema, bet didesnės išorinės sistemos dalis ir tai yra labai svarbus aspektas planuojant atsaką hibridinėms grėsmėms. Šis pavyzdys iliustruoja, kad poveikis gali būti daromas per skirtingus valstybės galios šaltinius, siekiant destabilizuoti padėtį bei daryti įtaką Lietuvos Respublikos konstitucinei santvarkai. Tai suponuoja išvadą, kad hibridinės grėsmės yra kompleksinė problema, tačiau į jas reaguoja skirtingos valstybės institucijos. Taigi, reikalingas sisteminis modelis, užtikrinantis koordinuotą atsaką į grėsmes, kylančias per skirtingus valstybės galios šaltinius. Atsižvelgiant į jų sudėtingą pobūdį, labai svarbu hibridines grėsmes vertinti kaip sistemą. Tai reiškia, kad reikia suprasti įvairių elementų, kurie prisideda prie bendros grėsmės, tarpusavio ryšį, pavyzdžiui, dalyvaujantys veikėjai, jų ryšiai, tikslai, pajėgumai ir pažeidžiamumas, kuriuo jie naudojasi. Žvelgiant į hibridines grėsmes kaip į sistemą, galima visapusiškiau suprasti grėsmių aplinką, o tai gali padėti politikos formuotojams ir saugumo specialistams sukurti veiksmingas grėsmės mažinimo strategijas. Be to, hibridinių grėsmių sistemos supratimas taip pat gali padėti nustatyti galimas nenumatytas atsakomųjų priemonių pasekmes. Dažnai veiksmai prieš vieną sistemos elementą gali turėti nenumatytų pasekmių kitoms sistemos dalims. Taigi, kuriant atsakomąsias priemones, būtina laikytis holistinio požiūrio ir atsižvelgti į platesnę sistemą.

2 paveikslas *Hibridinių grėsmių sisteminis poveikis*



Sudaryta autoriaus

2 paveiksle schematiškai atvaizduojamas hibridinių grėsmių sisteminis poveikis valstybei. Schemos centre yra valstybė, kurios galios šaltiniai, užtikrinantys nacionalinį saugumą, buvo aptarti aukščiau ir pavaizduoti 1 paveiksle. Valstybę ratu supa skirtingo pobūdžio grėsmės, veikiančios per skirtingus galios šaltinius, pagal DIMEFIL. Išorėje esantis žiedas vaizduoja priešiškai nusiteikusį veikėją, o rodyklės einančios nuo jo link grėsmių, atspindi šių poveikio priemonių sinchronizavimą ir

koordinuotą panaudojimą. Tokiu būdu grėsmės tampa hibridinėmis, o tai padaro šią problemą kompleksiška. Tai suponuoja išvadą, kad, hibridinės grėsmės turi būti vertinamos kaip kompleksinė sistema ir institucijų, reaguojančių į jas, veiksmai – koordinuojami.

2. LITERATŪROS APIE ATSPARUMĄ HIBRIDINĖMS GRĖSMĖMS, APŽVALGA

2.1.Rugsėjo 11-osios atvejis

Nors hibridinės grėsmės konceptualiai negali būti prilyginamos nevalstybiniam terorizmui, tačiau išankstinio įspėjimo aspektu, vis dėlto turi daug panašumų (Cullen, 2018). 2001-ųjų rugsėjo 11-oji (toliau – 9/11) žinoma kaip skaudžia tragedija pažymėta diena Jungtinių Amerikos valstijų istorijoje. Teroristai surengė teroro aktą, užgrobdami civilius orlaivius ir nukreipdami juos į dangoraižius New York‘o centre tokiu būdu sukeldami daugybę civilių žūčių. Praėjus keletui metų po šio įvykio, buvo sudaryta tyrimo komisija šios tragedijos priežastims išsiaiškinti. Komisijos raportas (Žodis raportas reiškia žodinį ar raštišką pavaldinio pranešimą viršininkui tarnybiniais klausimais (Čiočys ir kt., 2008)) yra išsami tyrimo ir analizės ataskaita, kurioje nagrinėjama 2001 m. rugsėjo 11 d. teroristų išpuolių įvykiai Jungtinėse Valstijose (National Commission on Terrorist Atacks, 2004). Šis įvykis, kurio metu teroristai užgrobė keturis lėktuvus ir juos naudojo kaip sprogstamąsias priemones, turėjo didžiulį poveikį visam pasauliui ir labai keitė tarptautinį saugumo ir kovos su terorizmu supratimą.

9/11 komisija buvo sudaryta JAV Kongreso ir Prezidento įsakymu, ir veikė nuo 2002 iki 2004 metų. Jos tikslas buvo atlikti išsamią ir nepriklausomą analizę, siekiant nustatyti, kaip ir kodėl įvyko šie teroristiniai išpuoliai. Komisijos darbas apėmė daugybę tyrimų, susitikimų, interviu ir dokumentų analizės. Komisijos raporte pateikiamos išsami faktų ir įvykių chronologija, o taip pat analizuojami įvairūs aspektai, susiję su teroristų grupės Al-Qaeda organizacija, saugumo priemonės, oro eismo kontrolės sistemos veikimas ir daugelis kitų veiksnių, kurie leido teroristams įgyvendinti savo planą (National Commission on Terrorist Atacks, 2004). Raportas pateikia išvadas ir rekomendacijas, kaip gerinti JAV nacionalinį saugumą, stiprinti terorizmo prevenciją ir reaguoti į tokius masinius teroristinius išpuolius ateityje. Jame taip pat akcentuojama informacijos rinkimo svarba, analizės ir dalijimosi tarp įvairių saugumo agentūrų, taip pat bendradarbiavimas su tarptautiniais partneriais, kovojant prieš terorizmą. 9/11 Komisijos raportas labai svarbus įrankis, padėjęs JAV ir kitoms šalims suprasti įvykių aplinkybes ir pasimokyti iš jų. Jame pateikiamos rekomendacijos buvo įgyvendintos daugelyje saugumo sričių ir lėmė įvairias reformas, siekiant sustiprinti nacionalinį saugumą (Shultz, 2016).

Dokumente buvo identifikuotos kelios organizacinės problemos, kurios prisidėjo prie teroristinių išpuolių įvykdymo ir padidino žalos mastą:

- Informacijos rinkimo ir analizės trūkumai: Buvo pastebėta, kad įvairios žvalgybos ir saugumo agentūros nepakankamai dalijosi informacija ir bendradarbiavo tarpusavyje. Tai ribojo galimybes gauti išsamų ir visapusišką vaizdą apie galimas teroristines grėsmes.
- Biurokratinės kliūtys. Dėl biurokratinių barjerų ir institucinės struktūros suvaržymų informacija dažnai nepasiekdavo tinkamų asmenų ar institucijų. Skirtingos agentūros neturėjo efektyvių mechanizmų dalintis svarbia informacija ar koordinuoti veiksmus.
- Oro eismo kontrolės trūkumai: Teroristai pasinaudojo pažeidžiamumu oro eismo kontrolės sistemoje. Buvo nustatyta, kad buvo spragų, kurios leido teroristams patekti į lėktuvus su draudžiamais objektais ir užgrobti juos.
- Terorizmo prevencijos strategijų trūkumai: Komisija pastebėjo, kad nėra buvę aiškios strategijos terorizmo prevencijai ir išpuolių įvyko, nepaisant gautų įspėjimų. Taip pat aptikta trūkumų bendradarbiavimo su tarptautiniais partneriais, terorizmo prevencijos srityje.
- Išteklių ir įgaliojimų trūkumas: Daugelis institucijų neturėjo pakankamų išteklių, įgaliojimų ir galimybių efektyviai spręsti terorizmo grėsmes. Tai apėmė ir žvalgybos veiklą, ir saugumo priemones (National Commission on Terrorist Atacks, 2004).

Šios organizacinės problemos ir trūkumai buvo pripažinti kaip svarbūs veiksniai, leidę teroristams sėkmingai vykdyti 9/11 išpuolius (National Commission on Terrorist Atacks, 2004). 9/11 Komisijos raporte pateikiamos rekomendacijos siekiant spręsti šias problemas ir stiprinti saugumo priemones terorizmo prevencijai ateityje:

- Informacijos dalijimosi ir bendradarbiavimo gerinimas: Rekomenduota sustiprinti informacijos dalijimąsi tarp žvalgybos ir saugumo agentūrų, taip pat tarp federalinių, valstybinių ir vietos lygmenų. Taip pat pabrėžta tarptautinio bendradarbiavimo svarba terorizmo prevencijos srityje.
- Centralizuota žvalgybos struktūra: Siūloma sukurti naują nacionalinės žvalgybos struktūrą, kurioje būtų integruotos įvairios žvalgybos agentūros. Tai padėtų efektyviau rinkti, analizuoti ir paskirstyti informaciją apie galimus teroristinius grasinimus.
- Biurokratinių kliūčių mažinimas. Rekomenduota skatinti informacijos ir atsakomybės dalijimąsi tarp agentūrų, taip pat peržiūrėti biurokratinius barjerus, kurie gali trukdyti veiksmingam bendradarbiavimui.

- Oro eismo kontrolės stiprinimas: Siūloma įdiegti griežtesnes saugumo priemones oro uostuose ir lėktuvuose, įskaitant keleivių ir bagažo patikrinimus bei keleivių tapatybės tikrinimą. Taip pat rekomenduojama pagerinti oro eismo kontrolės technologijas ir procedūras.
- Terorizmo prevencijos strategijos: Rekomenduojama kurti aiškesnes terorizmo prevencijos strategijas, kurios apimtų svarstymą potencialių teroristinių išpuolių prieš nacionalinį saugumą. Taip pat siūloma didinti investicijas į terorizmo tyrinėjimus ir inovacijas.
- Išteklių ir įgaliojimų stiprinimas: Siūloma didinti finansavimą, personalo skaičių ir technines galimybes žvalgybos, saugumo ir kovos su terorizmu srityse. Taip pat siūloma stiprinti bendradarbiavimą su privačiu sektoriumi ir pilietine visuomene terorizmo prevencijos veikloje.

Šie siūlymai ir rekomendacijos buvo skirti užtikrinti geresnį terorizmo prevencijos ir nacionalinio saugumo lygį JAV (National Commission on Terrorist Atacks, 2004). Po raporto paskelbimo daugelis iš šių siūlymų buvo įgyvendinti ir prisidėjo prie reformų saugumo srityje.

Apibendrinant, informacija iš 9/11 Komisijos raporto gali būti naudinga, taikant sisteminį požiūrį Lietuvos Respublikos atsparumo hibridinėms grėsmėms stiprinimui, nes yra tam tikrų sąsajų tarp terorizmo ir hibridinių grėsmių. Nors kontekstas ir veikėjai gali skirtis, kai kurios organizacinės problemos ir veiksmai, išskirti 9/11 Komisijos raporte, gali turėti bendrą pritaikomumą Lietuvos atvejui. Svarbu užtikrinti efektyvų informacijos rinkimą apie galimas grėsmes ir kritinės infrastruktūros pažeidimus. Tai apima geros kokybės žvalgybą, duomenų analizę ir žinių dalijimąsi tarp atitinkamų institucijų. Svarbu pripažinti, kad kiekvienos šalies saugumo iššūkiai gali skirtis, ir būtina atsižvelgti į specifines Lietuvos sąlygas ir kontekstą. Tačiau 9/11 Komisijos raportas gali suteikti naudingų išvadų ir rekomendacijų, kurios gali būti pritaikytos stiprinant Lietuvos atsparumą hibridinėms grėsmėms ir didinant nacionalinį saugumą. Ypatingai svarbu atkreipti dėmesį į žvalgybos institucijų tarpusavio sąveiką, informacijos dalijimąsi ir įgaliojimus imtis veiksmų.

2.2. Besimokančios organizacijos modelio, kaip atsparumo hibridinėms grėsmėms, instrumento taikymas

Besimokančios organizacijos (angl. Learning organization) sukūrimo sėkmės istorija pateikiamas JAV kovos prieš terorizmą pajėgų, žinomų kaip „Task Force 714“ (toliau – TF 714) atvejo analizė. Iškart po to, kai buvo dislokuota Irake 2003 m., ši didelė ir profesionali organizacija nesugebėjo įvykdyti užduoties – numalšinti sukilimą, kuriame pagrindinį vaidmenį vaidino tarptautinės teroristinės organizacijos Al-Qaeda padalinys Irake (toliau – AQI). Į atsargą išėjęs JAV

generolas Stanley McChrystal, kuris tarnavo TF 714 vadu, pripažino, kad jie pralaiminėjo gerokai silpnesniam ir turinčiam prastesnes technologines galimybes priešui, tačiau niekaip negalėjo identifikuoti šių nesėkmių priežasčių. (McChrystal, 2015, p.19). Verta paminėti, kad šios pajėgos buvo sukurtos 1980-aisiais, t.y. daugiau nei prieš du dešimtmečius bei įgijusios daug kovinės patirties, vykdydamos įvairias kontrteroristines operacijas. TF714 buvo pripažinta geriausiai parengtu padaliniu pasaulyje vykdyti kovą prieš terorizmą, tačiau Irake priešininkas buvo kitoks. AQI pasižymėjo sugebėjimu veikti slapta, nestandartiškai ir svarbiausia – neatitiko jokios tradicinės hierarchinės struktūros, o slaptus tinklus sudarė vidutinio lygio vadai (Shultz, 2016). Taigi priešininko organizacinė struktūra nebuvo hierarchinė, kas jiems padėjo užtikrinti decentralizuotą valdymą bei tuo pačiu apsunkino TF714 pastangas identifikuoti AQI vadovybę ir sprendimų priėmėjus, siekiant neutralizuoti grėsmes. Tai buvo kompleksinė problema, su kuria tradicinė hierarchinė organizacija nesugebėjo susitvarkyti.

Šio tipo (hierarchinės) organizacijos struktūra dažnai yra grindžiama aiškiai apibrėžtais vadovavimo lygiais ir aiškiai nustatytais atsakomybės bei valdymo grandinės elementais. Šioje struktūroje informacija ir sprendimai dažnai juda *iš viršaus į apačią* arba iš vieno lygio į kitą, o *komunikacija vyksta pagal aiškiai apibrėžtus kanalus.* Tokio tipo organizacijos yra labai veiksmingos, siekiant masto ekonomikos, kai reikalingas aukštas standartizacijos laipsnis ar reikia apdoroti didelius duomenų kiekius (Ellis & Black, 2018), tačiau jos taip pat yra labiau linkusios į biurokratiją ir lėtą sprendimų priėmimą. Hierarchinė struktūra gali trukdyti greitam prisitaikymui prie kintančios situacijos bei neapibrėžtumo sąlygomis, nes gali būti sunku greitai reaguoti ir priimti lanksčius sprendimus.

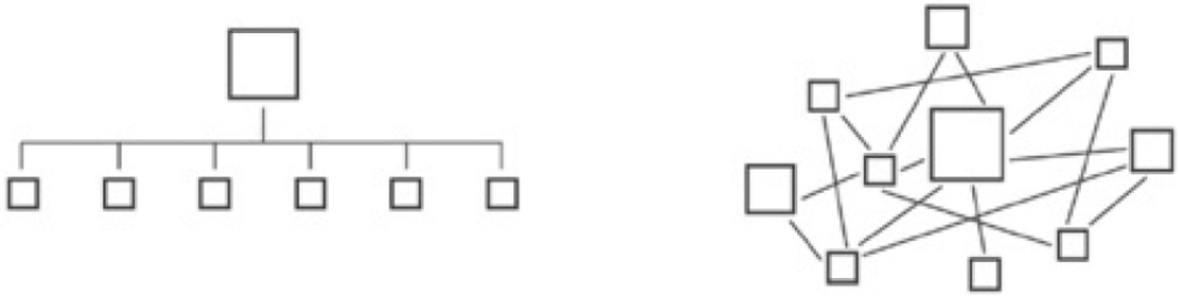
Ši tradicinė struktūra dažnai skatina linijinį valdymą, kurio metu sprendimai priimami ir vykdomi „iš viršaus į apačią“. Tai gali užkirsti kelią kūrybiškumui ir inovacijoms, nes darbuotojams gali trūkti laisvės ar paskatinimo imtis iniciatyvų (Ellis & Black, 2018).

Taigi, nors hierarchinė struktūra turi savo privalumų organizacijos valdyme ir tvarkyme, ji taip pat gali trukdyti efektyviam prisitaikymui prie naujų iššūkių ir sparčiai besikeičiančių sąlygų. Šiandien daugelis organizacijų ieško būdų, kaip derinti hierarchinę struktūrą su lankstesniu, inovatyvesniu ir sparčiau reaguojančiu veikimo modeliu.

Kaip priešingas pavyzdys tradicinei hierarchinei struktūrai yra komanda (grafinis atvaizdavimas pateikiamas 3 paveiksle). Pavyzdžiu pateikiamos JAV jūrų ruonių (angl. US Navy SEAL) komandos, kuriose yra užsimezgę asmeniniai tarpusavio ryšiai. Šie ryšiai pradeda megztis dar bazinio rengimo metu, vadinamu BUD/S (angl. Basic Underwater Demolition/ SEAL). Tai yra

ypatingai sunki 24 savaites trunkanti atranka. Šį etapą įveikia ne patys stipriausi ar raumeningiausi, o tie, kurie geriausiai sugeba dirbti komandoje Kaip teigia McChrystal (2015), BUD/S tikslas nėra gaminti „superkareivius“. Tai yra „superkomandų“ kūrimas. Pirmasis žingsnis yra sukurti tvirtus, pasitikėjimu grįstus santykius. Tai atrodys intuityvu kiekvienam, kuris yra buvęs komandoje, tačiau tai prieštarauja redukcionistinio valdymo esmei. Tradicinėje hierarchinėje organizacijoje vadovas suskaido tikslą į atskiras užduotis ir jas išdalina. Instrukcijų gavėjams nereikia pažinti savo kolegų, jiems tereikia klausyti savo viršininko. Hierarchinėje organizacijoje svarbūs yra vertikalūs ryšiai; Kita vertus, komandos formavimas yra grįstas horizontaliu ryšiu (Shultz, 2016). Asmeniniai ryšiai bei kiekvieno komandos nario pažinimas yra veiksniai, sąlygojantys problemų sprendimo greitį nestandartinėse situacijose.

3 paveikslas *Tradicinės vadovavimo hierarchijos ir komandos palyginimas*



Tradicinė vadovavimo hierarchija

Komanda

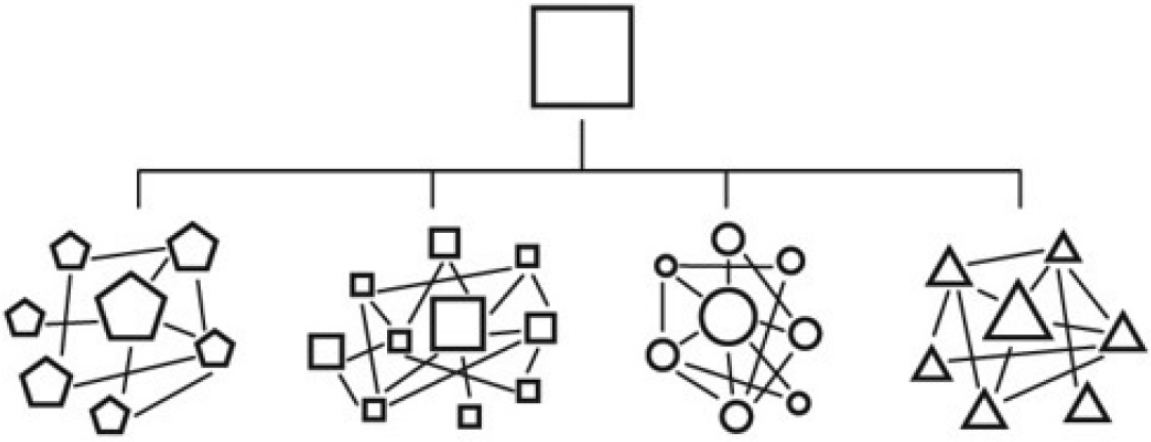
Šaltinis: (McChrystal, 2015)

Komandos dinamika pasižymi asmeniniais tarpusavio ryšiais, kai kiekvienas komandos narys pažįsta kitus komandos narius, žino jų kompetencijas ir stipriąsias bei silpnąsias savybes. Komandai susidūrus su neįprasta situacija ar problema, informacijos dalijimasis komandos viduje yra greitas, ji tiesiogiai pasiekia komandos narius, turinčius kompetencijų, reikalingų tos problemos sprendimui.

Paskirtas vadovauti TF714, generolas McChrystal rado didelę organizaciją, sudarytą iš atskirų komandų (Shultz, 2016). Šios situacijos grafinis atvaizdavimas pateikiamas 4 paveiksle. Kiekvienas operatorius (Specialiųjų operacijų pajėgų karys) stengėsi dėl savo komandos ir kuo geresnio, jiems

iškeltos užduoties įvykdymo rezultato. Nors bet kuris operatorius, kaip ir visas TF714, operacijų planuose ir dokumentuose kovojo tą pačią kovą, iš tikrųjų jie kovojo už savo padalinį. Operatoriai komandose ruošiami, komandiruojami ir dirba kartu. Jie praleidžia keturis mėnesius misijose svetimoje ir priešiškoje aplinkoje ir retai kada užmezga prasmingus, draugiškus santykius su bet kuriuo, nepriklausančiu šiam ratui. Santykiai komandose kardinaliai skiriasi nuo santykių tarp komandų ar kitų karinių vienetų. Jiems nerūpėjo kokių rezultatų pasiekia kitos TF714 komandos ar žvalgybos analitikai štabe, tuo tarpu žvalgybos analitikams rūpėjo tik jų darbo dalis, tačiau jie visiškai nesidomėjo kaip sekasi operatoriams, kaip ir pastarųjų, pagrindinis interesas buvo tik kuo geriau įvykdyti gautą užduotį (McChrystal, 2015). Organizacinių saitų nebuvimas tapo pagrindiniu iššūkiu susidūrus su kompleksine problema - decentralizuota, tinkline priešininko vadovavimo grandine. Tarpusavio ryšiai bei informacijos dalijimasi kiekvienoje atskiroje komandoje vyko kaip aprašyta ankstesniame pavyzdyje, tačiau komandų tarpusavio ryšiai buvo formalūs, informacijos perdavimas vyko pagal griežtai aprašyta taisykles – iš viršaus į apačią ir atgal. Tokia organizacinė strukūra neužtikrino savalaikio dalijimosi informacija, būtino greitam reagavimui į besikeičiančią situaciją (Shultz, 2016).

4 paveikslas *Vadovavimas komandoms*

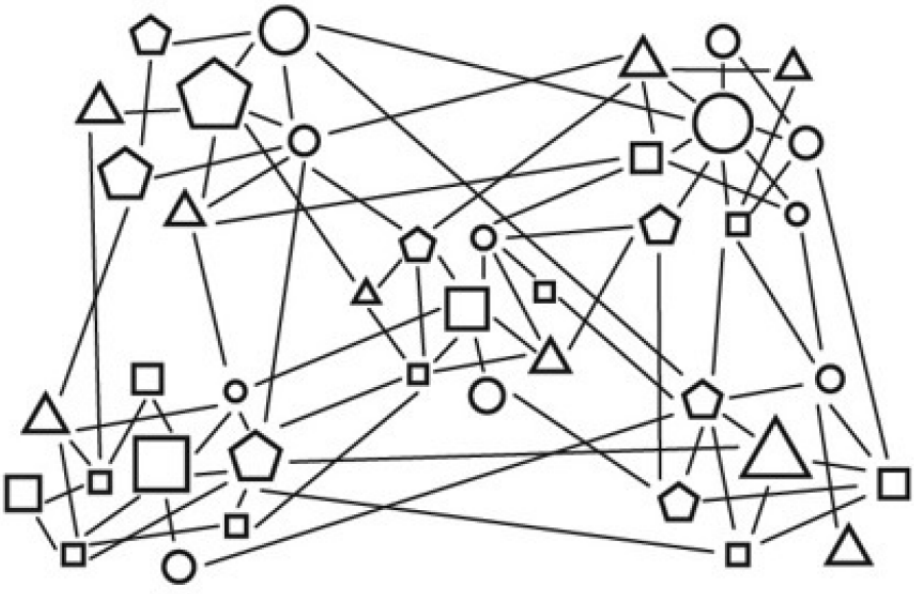


Šaltinis: (McChrystal, 2015)

McChrystal‘as, remdamasis, Harvardo sociologijos profesoriumi Hackman‘u, teigia, kad komandas kurti ir išlaikyti yra daug sudėtingiau, nei atrodo iš pirmo žvilgsnio. Problema yra tame, kad komandų dinamika yra galinga, bet subtili, o plėtra yra patikimas būdas jas išardyti. Klaidinga

prielaida yra, kad didesnės komandos yra efektyvesnės nei mažesnės, nes jos turi daugiau išteklių. Komandai didėjant, atsiranda daugiau tarpusavio ryšių ir santykių tarp jos narių, kuriuos reikia išlaikyti, kol galiausiai tai tampa nebeįmanoma. Taigi, nors komandos yra efektyvios sprendžiant kompleksines problemas, tačiau sukurti komandą iš 7000 žmonių organizacijos, gali tapti keblia užduotimi. Siekdamas išplėsti vienybę ir jungtinumą egzistuojantį komandų viduje per visą TF714, McChrystal‘as sukūrė koncepciją, kurią pavadino „komandų komanda“ (angl. Team of Teams). Komandoje kiekvienas jos narys turi pažinoti kiekvieną kitą narį. Siekiant sukurti pasitikėjimą, jie turi dalintis informacija, kad galėtų siekti bendro tikslo. Komandų komandoje, kiekvienas individas neprivalo pažinoti kiekvieno kito asmens, tačiau, santykiai tarp komandų turi būti panašūs į santykius tarp asmenų tam tikroje komandoje ir kad juos visus sietų bendras tikslas: laimėti karą, o ne pranokti kitą dalinį (McChrystal, 2015). Tai galėtų būti veiksmingai pasiekta **per atstovavimą arba per kariuomenėje taip vadinamus sąveikos karininkus.** Komandų komandos grafinis atvaizdavimas pateikiamas 5 paveiksle.

5 paveikslas *Komandų komanda*



Šaltinis: (McChrystal, 2015)

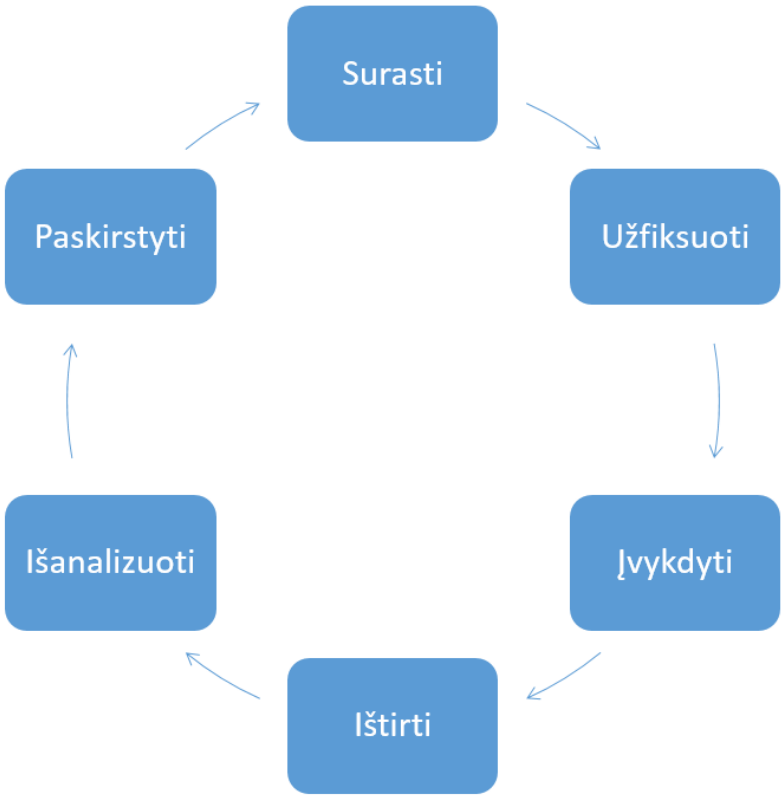
Komandų komandos koncepcija žymi ne struktūrines ar administracines reformas, o *pasikeitimą mąstymo bei organizacinės kultūros lygmenyse*. Svarbiausias šios sistemos variklis yra bendra, visiems organizacijos padaliniams ir kiekvienam jos nariui, vizija. Visiems aiški ir žinoma vizija nurodo organizacijos kryptį, o padalinių tarpusavio ryšių egzistavimas užtikrina suvokimą apie tai, kas už kokią sritį yra atsakingi bei kam kokia informacija gali būti svarbi (Shultz, 2016).

Siekiant įveikti kompleksiškus ir sudėtingus AQI tinklus, TF 714 varančiuoju varikliu tapo žvalgybinė informacija. Specialiųjų operacijų taktinių padalinių veiksmai operacijų rajonuose, buvo sinchronizuoti su tvirtais žvalgybos pajėgumais, kuriuos suteikė Centrinės Žvalgybos agentūros (CIA), Nacionalinės saugumo agentūros (NSA), Federalinio tyrimų biuro (FBI), Gynybos žvalgybos agentūros (DIA), Nacionalinės geografinės žvalgybos agentūros (NGA) ir kitų organizacijų *veiksmų koordinavimas bei duomenų sintezė* (McChrystal, 2015). Tokiam koordinuotam veikimui buvo sukurtas F3EAD (angl. Find – Fix – Finish – Exploit – Analyse - Disseminate) ciklas. Jį sudaro šešios fazės:

- Surasti (angl. Find) surandamas taikinys;
- Užfiksuoti (angl. Fix) toliau taikinys užfiksuojamas – jis yra nuolat stebimas įvairiomis priemonėmis, įskaitant ir nuotoliniu būdu valdomus orlaivius bei pranešama apie taikinio buvimo vietos pasikeitimus;
- Įvykdyti (angl. Finish) taikinys yra sulaikomas ar neutralizuojamas;
- Ištirti (angl. Exploit) operacijos vietoje atliekamas įkalčių surinkimas ir perduodama žvalgybos analitikams, esantiems ne operacijos rajone;
- Išanalizuoti (angl. Analyse) gauta informacija analizuojama, ieškoma sąsajų su jau turimais žvalgybiniais duomenimis.
- Paskirstyti (angl. Disseminate) gauta nauja informacija yra paskirstoma kitoms žvalgybos agentūroms bei operacijas vykdantiems specialiųjų operacijų vienetams (Shultz, 2016).

F3EAD ciklas atvaizduotas 6 paveiksle.

6 paveikslas *F3EAD ciklas*



Sudaryta autoriaus, remiantis Shultz (2016)

Visų pirma, patys TF 714 negalėjo vykdyti F3EAD. Jų struktūroje nebuvo žvalgybos pajėgumų tai padaryti. Tam reikėjo tarpžinybinio bendradarbiavimo. Todėl šiam tikslui pasiekti buvo užmegzti santykiai su žvalgybos agentūromis ir užtikrinta sąveika. Tai buvo būtina norint pasiekti žvalgybos dominavimą. Be jo analizės procesas, panaudojant operacijų metu surinktą žvalgybos informaciją, ir planuojant tolimesnes operacijas būtų buvęs neįmanomu. Tokiu atveju, TF 714 nebūtų galėję pasiekti tokio tempo, kurio reikėjo pogrindinio teroristų tinklo išardymui (degradavimui) (Shultz, 2016).

Šis ciklas padėjo padidinti vykdomų operacijų tempą ir efektyvumą. Remiantis operacijų metu gautais žvalgybiniais duomenimis ir susiejus juos su jau turima informacija duomenų bazėse, galima buvo iškarto planuoti naujas operacijas ir nedelsiant jas vykdyti. Tačiau, kaip teigia Shultz (2016),

Didelė sprendimų priėmimo apimtis ir greitis viršijo net labiausiai įgudusio vadovo galimybes, todėl buvo atsisakyta vadovavimo „iš viršaus į apačią“ ir pritaikytas decentralizuotas vadovavimas bei problemų sprendimas „iš apačios į viršų“. Siekiant aplenkti AQI, problemų sprendimo ir sprendimų priėmimo procesai negalėjo remtis tuo, kad vadovauja vyresnieji vadovai, nes tai užtruktų per daug laiko. F3EAD ciklas iliustruoja žvalgybinės informacijos dalijimosi ir paskirstymo svarbą, sprendžiant kompleksines problemas, tokias, kaip hibridinės grėsmės ar terorizmas. Šio ciklo atsiradimas yra 9/11 komisijos tyrimo identifikuotų pamokų pasekmė ir sėkmingas sprendimas

Asmenys ir komandos, kurie buvo arčiausiai kovinių veiksmų, turėjo geriausias galimybes priimti svarbius sprendimus ir imtis greitų veiksmų. Norint pasiekti sėkmę, labai svarbu suteikti įgaliojimus žemesnėms grandims (Shultz, 2016).

Anot Schulz (2016), atlikusio TF714 atvejo analizę, generolui Mc Chrystal pavyko reorganizuoti TF714 ir sukurti besimokančią organizaciją. Autorius išskiria šias besimokančios organizacijos savybes, nulėmusias TF714 sėkmę:

- Nenumatyti iššūkiai neparalyžiuoja organizacijos;
- Problemų sprendimas yra pagrindinė organizacijos kompetencija;
- Organizacinė praktika yra ginčijama;
- Žinių rinkimo metodai, nustatyti judant sisteminiam mokymuisi;
- Lyderiai kuria aplinką, skatinančią mokymąsi;
- Organizacinė atmintis fiksuoja ir išlaiko naujoves, tačiau išlieka lanksčia.

Sisteminis mąstymas yra galingas kompleksinių problemų sprendimo ir organizacinio mokymosi įrankis. Kompleksiškos problemos negali būti efektyviai išspręstos sutelkiant dėmesį į atskiras dalis ar atskirus veiksmus. Vietoj to, svarbu suprasti ir spręsti pagrindines struktūras, santykius ir modelius, kurie formuoja sistemą. Šis požiūris, žinomas kaip sisteminis mąstymas, leidžia mums pamatyti didesnį vaizdą ir suprasti sistemos tarpusavio priklausomybes ir grįžtamąjį ryšį (Senge, 2006). Daroma prielaida, kad šis mąstymo būdas ir sisteminis požiūris potencialiai yra viena iš hibridinių grėsmių, kaip kompleksiškos problemos sprendimo priemonių. TF714 atvejis taip pat atskleidė besimokančios organizacijos modelio efektyvumą, sprendžiant kompleksines problemas.

Senge (2006) įvardija penkias disciplinas, kurios yra būtinos organizacijoms tapti besimokančiomis organizacijomis, galinčiomis spręsti sudėtingas problemas. Šios disciplinos veikia kartu, kad skatintų holistinį ir sisteminį požiūrį į problemų sprendimą:

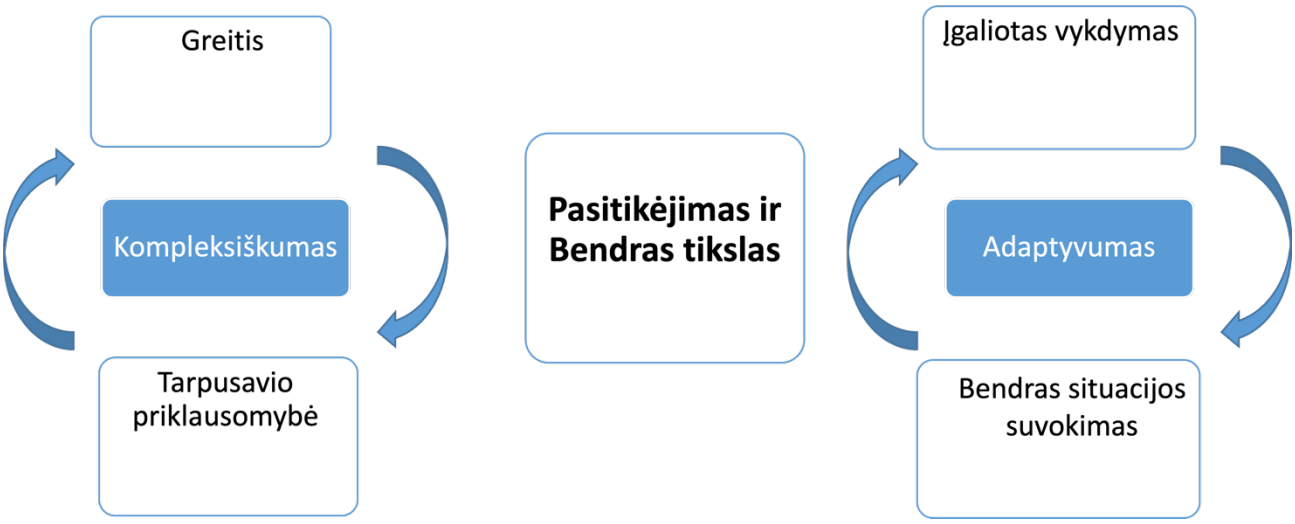
1. Sisteminis mąstymas: ši disciplina yra Senge požiūrio kertinis akmuo. Tai apima įvairių sistemos elementų tarpusavio sąsajų ir tarpusavio priklausomybių

pripažinimą. Sisteminis mąstymas skatina asmenis žvelgti į problemas platesniame kontekste bei apsvarstyti ilgalaikes savo veiksmų pasekmes.

2. Asmeninis meistriškumas: Asmeninis meistriškumas apima asmenis, kurie nuolat stengiasi pagerinti savo asmeninį augimą ir mokymąsi. Tai reikalauja gilaus atsidavimo savęs tobulėjimui, asmeninės vizijos ugdymui ir įgūdžių, reikalingų tai pasiekti, ugdymas. Ugdydami asmeninį meistriškumą, asmenys tampa efektyvesniais problemų sprendėjais ir prisideda prie bendro organizacijos mokymosi.
3. Psichiniai modeliai: psichiniai modeliai yra giliai įsišaknijusios prielaidos, įsitikinimai ir šališkumai, kurie daro įtaką tam, kaip asmenys suvokia ir interpretuoja pasaulį. Senge (2006) pabrėžia, kaip svarbu mesti iššūkius ir plėsti psichikos modelius, siekiant įveikti šališkumą ir skatinti atvirumą.
4. Bendros vizijos kūrimas: Bendra vizija reiškia gebėjimą sukurti ir išlaikyti kolektyvinį tikslo ir krypties jausmą organizacijoje. Tai apima asmeninių asmenų vizijų suderinimą su bendra vizija, kuri įkvepia ir motyvuoja visus. Puoselėdamos bendrą viziją, organizacijos gali sutelkti bendras pastangas ir pasiekti didesnę problemų sprendimo sinergiją.
5. Mokymasis komandoje: Mokymasis komandoje pabrėžia bendrų problemų sprendimo ir bendrų žinių kūrimo svarbą. Tai apima mokymosi kultūros ugdymą komandose, kur asmenys gali atvirai dalytis savo idėjomis, užmegzti dialogą ir bendrai mokytis iš savo patirties. Mokydamosis komandoje, organizacijos gali pasinaudoti kolektyviniu savo narių intelektu ir kūrybiškumu, kad galėtų veiksmingai spręsti sudėtingas problemas.

Integruojant šias penkias disciplinas, galima sukurti „besimokančią organizaciją“, kuri skatina nuolatinio mokymosi, prisitaikymo ir naujovių kultūrą. Šis metodas leidžia veiksmingiau spręsti sudėtingas problemas, nustatant pagrindines priežastis, pasitelkiant kolektyvinį intelektą ir skatinant sisteminius pokyčius.

7 paveikslas *Besimokančios organizacijos atsakas kompleksiškumui*



Sudaryta autoriaus, remiantis (McChrystal, 2015)

Besimokančios organizacijos atsakas kompleksiškumui pavaizduotas 7 paveiksle:

1) Pirmame šio darbo skyriuje pateikta hibridinių grėsmių apžvalga, jų (hibridinių grėsmių) kompleksiškumą lemia du vienas kitą stiprinantys faktoriai:
   a) Nepaisant poveikio per skirtingus valstybės galios šaltinius (per visą DIMEFIL), grėsmės dažniausiai kyla iš to paties priešiškai nusiteikusio veikėjo arba iš skirtingų veikėjų, kurie yra **tarpusavyje susiję** ir, neretai, derina savo veiksmus.
   b) Šiuolaikinės technologijos ir įvairių ryšio priemonių galimybės bei sparta užtikrina itin greitą **(greitis)** keitimąsi informacija bei galimybes laiku prisitaikyti prie besikeičiančios situacijos (McChrystal, 2015). Naujos technologijos sukuria sąlygas *hipersujungimui* (angl. hyper-conectivity), kuris pats savaime yra įvairiakryptės konkurencijos sudedamoji dalis, kurią skatina pasaulinės įtampos. Be to, klimato kaita, dabartinės pasaulinės tvarkos kaita ir kylantis socialinis nusivylimas bei pandemija, viena baisiausių praėjusio šimtmečio ligų, pavojingai sujaukė tradicines sąvokas, mąstymo būdus ir gebėjimus (Allem ir kt., 2023).
2) Iš kitos pusės, besimokanti organizacija pasižymi **adaptyvumu** kuris leidžia prisitaikyti prie besikeičiančios situacijos ir atitinkamai veikti:

a) **Įgaliotas vykdymas**, dar vadinamas tiksliniu vadovavimu (angl. mission command), reiškia decentralizuotą sistemą, kuria siekiama nustumti sprendimo priėmimo teisę į organizacijos kraštus. Šioje sistemoje sprendimų priėmimo galia paskirstoma asmenims ar komandoms visoje organizacijoje, o ne sutelkta centrinėje institucijoje. Įgaliotas vykdymas reiškia, kad žmonės organizacijoje gali priimti sprendimus ir imtis veiksmų savarankiškai, laikantis nustatytų ribų ir gairių. Šiuo požiūriu siekiama padidinti organizacijos judrumą, reagavimą ir naujoves, leidžiant greitai priimti sprendimus ir imtis veiksmų įvairiais lygmenimis.

b) Kaip matoma visose trijose hibridinių grėsmių valdymo atvejų analizėse, labai svarbi besimokančios organizacijos savybė – **bendras situacijos suvokimas** bei dalijimasis informacija. Bendro situacijos suvokimo klausimas aktualus ir organizacijų viduje. Optimaliam funkcionavimui reikalinga, kad aukščiausio ir vidutinio lygių vadovai bei darbuotojai turėtų tą patį situacijos vaizdą (Larsson ir kt., 2021). Kaip teigia McChrystal, remdamasis Tocqueville (2015), Organizacija turi įgalinti savo narius, bet tik po to, kai yra užtikrintas bendras situacijos suvokimas, priešingu atveju, tai gali sukelti sumaištį. Kita vertus, geras situacijos suvokimas be įgalinimo nebus produktyvus ir galiausiai sukels frustraciją jos nariams, kadangi pastarieji neturės galimybės veikti, remdamiesi savo įžvalgomis. Efektyvus bendras situacijos suvokimas TF 714 atveju buvo įgyvendintas **per atstovavimą arba per kariuomenėje taip vadinamus sąveikos karininkus** bei įdiegus F3EAD ciklą ir ypatingai per šio ciklo paskirstymo fazę. Ellis ir Black (2018), remdamiesi Kahneman žmonių kognityvikos tyrimų rezultatais, pastebi, kad organizacijoms, susiduriant su kompleksiškumu, dažnai problemos, kurias žmonės suvokia, nėra tikrosios priežastys, skatinančios įvykius, tačiau 1 sistemos momentiniai sprendimai juos suklaidina, kad jie žino, kas vyksta. Kita vertus, 2 sistemos mąstymas praverčia tada, kai spontaniškas, intuityvaus sprendimo ieškojimas kartais nepavyksta. Tokiais atvejais dažnai pereiname prie lėtesnės, labiau apgalvotos ir daug pastangų reikalaujančios mąstymo formos.

3) Svarbiausias, jungiantis elementas, užtikrinantis adaptyvios organizacijos atsaką kompleksiškumui yra tarpusavio pasitikėjimas ir bendras tikslas. Analizuojant bendro tikslo perspektyvą Coombs, cituodamas Simpson (2023), pastebi, kad Strateginis pasakojimas (angl. narrative) išreiškia strategiją kaip istoriją, paaiškinančią savo

veiksmus. Jis tarnauja keliems tikslams: nuo savo pajėgumų derinimo ir koordinavimo iki bendro supratimo, ir bendro tikslo kūrimo bei oponentų, ir kitų šalių įtikinimo savo politiniais tarpiniais bei strateginiais tikslais. Be to, strateginis pasakojimas (1) leidžia tiems, kurie yra pirmieji, reaguojantys asmenys, priimti sprendimus, pagrįstus strateginiu pasakojimu, ir (2) užtikrina, kad civiliai gyventojai suprastų strateginius tikslus ir išvengtų priešiškos veiklos poveikio, ypač sukelto veiksmų, kurie yra žemiau smurto ribos. Šis ryšys veikia abipusiai stiprinančiai su organizacijos adaptyvumą lemiančiais faktoriais:

a) Įgaliotas vykdymas negalimas be tarpusavio pasitikėjimo, o pastarasis kyla iš kiekvieno organizacijos nario asmeninio meistriškumo, bei kaip minėta aukščiau, yra tiesiogiai susijęs su bendru situacijos suvokimu.
b) Bendras tikslas taip pat yra labai svarbus, užtikrinant įgaliotą vykdymą, imantis veiksmų savarankiškai, laikantis nustatytų ribų ir gairių.

Literatūros apžvalgos rezultatai suponuoja nuomonę, kad besimokančios organizacijos koncepcija yra potencialiai tinkama, taikant sisteminį požiūrį, siekiant sustiprinti Lietuvos Respublikos atsparumą hibridinėms grėsmėms. Besimokančioje organizacijoje problemų sprendimas yra pagrindinė kompetencija. Šio požiūrio taikymas įgalintų Lietuvos institucijas ir organizacijas sugebėti greitai ir efektyviai reaguoti į hibridines grėsmes. Tai reikštų, kad organizacijos būtų parengtos ir turėtų tinkamą įrangą, protokolus ir kompetencijas atpažinti, analizuoti ir spręsti hibridines grėsmes, siekiant minimalaus poveikio valstybės saugumui ir stabilumui. Besimokančioje organizacijoje yra išlaikoma organizacinė atmintis, tačiau ji išlieka lanksti. Tai taip pat galėtų būti taikoma Lietuvos Respublikai, kur organizacijos turėtų išlaikyti ir perduoti patirtį, gautą iš praeities hibridinių grėsmių atvejų, tačiau tuo pačiu būti lankstesnės ir pasiruošusios prisitaikyti prie naujų grėsmių ir iššūkių.

Apibendrinant. pirma, hibridinės grėsmės yra kompleksiškos dėl dviejų faktorių: skirtingų veikėjų veiklos, kurios dažnai derinamos, ir šiuolaikinių technologijų, kurios užtikrina greitus informacijos mainus. Antra, besimokanti, adaptyvi organizacija geba prisitaikyti prie kintančių sąlygų ir veikti efektyviai. Šios organizacijos pagrindiniai bruožai apima įgaliotą vykdymą, kuris skatina decentralizaciją ir sprendimų priėmimo galios paskirstymą visoje organizacijoje. Taip siekiama padidinti organizacijos judrumą ir reagavimą. Be to, bendras situacijos suvokimas ir informacijos dalijimasis yra būtini, kadangi tai užtikrina, jog sprendimai priimami pagal bendrą supratimą ir realią situaciją. Pagaliau, tarpusavio pasitikėjimas ir bendras tikslas yra esminiai jungiamieji elementai,

kurie stiprina įgaliotą vykdymą ir organizacijos adaptaciją. Tai įrodo, kad bendras tikslas ir pasitikėjimas yra svarbūs, užtikrinant, kad organizacija būtų pajėgi reaguoti į kompleksiškas hibridines grėsmes.

3. VALSTYBĖS ATSPARUMO HIBRIDINĖMS GRĖSMĖMS VERTINIMO MODELIO TYRIMAS

3.1 Empirinio tyrimo metodika

Empirinio tyrimo objektas: Lietuvos Respublikos atsparumas hibridinėms grėsmėms.

Empirinio tyrimo tikslas: Įvertinus atsparumą, sukurti empirinių duomenų analize pagrįstą atsparumo hibridinėms grėsmėms vertinimo modelį.

Empirinio tyrimo uždaviniai:

1. Išnagrinėti hibridinių grėsmių pasireiškimo Lietuvoje atvejus ir identifikuoti jų pagrindines charakteristikas bei veiksnius.
2. Ištirti Lietuvos Respublikos hibridinių grėsmių valdymo strategijas.
3. Ištirti ir įvertinti besimokančios organizacijos modelio taikymo galimybes Lietuvos kontekste.
4. Pagal sudarytą modelį, pasiūlyti rekomendacijas ir strategines gaires Lietuvos Respublikos atsparumo hibridinėms grėsmėms stiprinimui.

Tyrimo metodai: pasirinkta kokybinio tyrimo metodologija - pusiau struktūruotas interviu. „Dėmesio centras – tyrimo dalyvių perspektyvos, subjektyvios sampratos ir patirtys, kasdieniai kontekstai" (Gaižauskaitė ir Valavičienė, 2016). Remiantis literatūros apžvalga bei antrinių šaltinių analize, buvo suformuotas pradinis konceptualus modelis. Remiantis literatūros apžvalgos metu surinktais duomenimis, sudarytu klausimynu, buvo atliktas kokybinis tyrimas, padėjęs patikrinti pradinį modelį ir tyrimo pabaigoje įvertinti Lietuvos respublikos atsparumą hibridinėms grėsmėms.

Klausimyne buvo pateikti klausimai, susiję su hibridinėmis grėsmėmis Lietuvos Respublikai. Klausimynas sudarytas iš kelių dalių, kuriose siekiama nustatyti suvokimą apie hibridines grėsmes, vizijų ir veiksmų suderinamumą, tarpinstitucinę sąveiką ir tarptautinį bendradarbiavimą bei informacijos dalijimosi galimybes ir apribojimus. Sudarant klausimyną, buvo remiamasi besimokančios organizacijos prisitaikymo kompleksinėms (hibridinėms) grėsmėms modeliu. Surinkus empirinius duomenis bei atlikus jų analizę, įvertintas Lietuvos Respublikos atsparumas hibridinėms grėsmėms.

Empirinio tyrimo metodo pagrindimas: Kokybinis tyrimas pasirinktas kaip priemonė įvertinti problemas iš tyrimo dalyvių perspektyvos, stengiantis suprasti jų objektų ir įvykių subjektyvų vertinimą (Hennink ir kt., 2020). Tyrimui atlikti pasirinktas abdukcinis metodas. „Darbas su duomenimis yra daugiasluoksnis: surinkti duomenys apdorojami ir sisteminami (t. y. daromi interviu išrašai, kataloguojama su kiekvienu interviu su- sijusi papildoma medžiaga, pvz., interviu protokolai, tyrėjo pastabos ir kt.), atliekama interviu analizė ir interpretacija (tiek preliminari, po kiekvieno interviu, tiek detali, atlikus visus planuotuosius interviu), jie lyginami tarpusavyje, reikalui esant grįžtama prie duomenų rin- kimo, o tada – vėl prie analizės ir interpretacijos, teorinių teiginių formulavimo, tikslinimo, performulavimo“ (Gaižauskaitė ir Valavičienė, 2016).

Tyrimo filosofija: Tyrimas remiasi ontologine, subjektyvistine filosofija, tiriant informantų pateikiamas prielaidas apie hibridines grėsmes Lietuvoje bei jų organizacijose. Tai padės suvokti organizacijų informuotumą hibridinių grėsmių atžvilgiu, pasiruošimą jas atremti bei įvertinti perspektyvų į šias grėsmes suderinamumą.

Tyrimo imtis ir populiacija: Tyrimui atlikti pasirinkta tikslinė, netikimybinė informantų atranka. Remiantis pirmoje darbo dalyje sudarytu institucijų sąrašu, pasirinkti raktinių institucijų atstovai, užimantys pareigas vadovaujančiuose lygmenyse, kurių pareigos yra tiesiogiai susijusios su institucijos strategijos parengimu, įgyvendinimu ir sąveikos su kitomis institucijomis užtikrinimu. Pasirinktų institucijų sąrašas, kuris sudarytas, remiantis DIMEFIL, pateikiamas 2 lentelėje.

2 lentelė *Tyrimui pasirinktos institucijos bei pasirinkimo pagrindimas*

Pasirinkta institucija	**Pagrindimas**
Vidaus reikalų ministerija	Institucija, kuriai pavaldžios įstaigos yra tiesiogiai atsakingos už tvarkos palaikymą, reagavimą į krizes bei nelaimes ir valstybės funkcijų užtikrinimą.
Lietuvos kariuomenės Strateginės komunikacijos departamentas	Institucija – tiesiogiai atsakinga už informacinės erdvės stebėjimą bei informacinių grėsmių identifikavimą.
Krašto apsaugos ministerija	Institucija – atsakinga už ginkluotą valstybės gynybą.
Valstybės sienos apsaugos tarnyba	Institucija – atsakinga už ginkluotą valstybės sienų apsaugą.
Finansų ministerija	Ministerija, atsakinga už valstybės finansus, kaip vieną iš valstybės galios šaltinių.
KAM Atsako į hibridines grėsmes grupė	Institucija – tiesiogiai atsakinga už hibridinių grėsmių stebėseną ir valdymą.
Valstybės saugumo departamentas	Valstybės institucija, atsakinga už žvalgybinės informacijos rinkimą ir paskirstymą.
Lietuvos šaulių sąjunga	Visuomeninė organizacija, prisidedanti prie Nacionalinio saugumo užtikrinimo.
Lietuvos Respublikos Seimo Nacionalinio saugumo ir gynybos komitetas	LR Seimo komitetas, tiesiogiai atsakingas už Nacionalinio saugumo užtikrinimą teisėkūros srityje.

Šaltinis: (sudaryta autoriaus, remiantis literatūros analize)

Atliekant interviu, remiantis informantų ekspertine nuomone bei rekomendacijomis, buvo apklausti atstovai, atstovaujantys organizacijas iš papildomų sektorių – Nacionalinio krizių valdymo centro prie Lietuvos Respublikos vyriausybės atstovas, kaip valstybinės įstaigos, tiesiogiai atsakingos

už reagavimą į krizes bei hibridinių grėsmių valdymą; visuomenininkas, vadovaujantis nevyriausybinei „Pilietinio atsparumo centras“, užsiimančia kova prieš priešišką propagandą ir dezinformacija; Vilniaus miesto tarybos narys – siekiant išsiaiškinti atsparumo lygį savivaldos lygmeniu ir gebėjimą sąveikauti su valstybinėmis institucijomis. Iš viso buvo atlikta 12 interviu su vadovais ir pareigas vadovaujančiame lygmenyje užimančiais tarnautojais, turinčiais kompetencijų atsakyti į klausimus apie organizacijos veiklą ir sąveiką su kitomis institucijomis. Interviu buvo tęsiami, kol atsakymai pradėjo kartotis ir buvo pasiektas prisotinimo efektas (Gaižauskaitė ir Valavičienė, 2016). Informantų kodavimas, atstovaujamos institucijos ir socialiniai – statistiniai duomenys pateikiami 3 lentelėje. Visi, apklausti, asmenys turi aukštąjį išsilavinimą – nuo magistro iki daktaro mokslinius laipsnius bei yra sukaupę ilgametę profesinę patirtį.

3 lentelė *Informantų socialiniai duomenys*

Kodas	Institucija	Kuruojama sritis	Patirtis	Amžius	Išsilavinimas
A1	Vidaus reikalų ministerija	Hibridinės grėsmės	32 metai valstybės tarnyboje	Nuo 50 iki 59 metų	Aukštasis universitetinis
A2	Lietuvos šaulių sąjunga	Vadovaujančios pareigos	27 metai valstybės tarnyboje	Nuo 50 iki 59 metų	Aukštasis universitetinis
A3	KAM Atsako hibridinėms grėsmėms grupė	Vadovaujančios pareigos	29 metai valstybės tarnyboje	Nuo 50 iki 59 metų	Aukštasis universitetinis
A4	Krašto apsaugos ministerija	Teisė, administracija, korupcijos prevencija, duomenų apsauga ir saugumas	14 metų valstybės tarnyboje	Nuo 30 iki 39 metų	Aukštasis universitetinis
A5	VSAT	Pajėgų valdymas, operatyvus valdymas, krizių ir ekstremalių situacijų valdymas	32 metai valstybės tarnyboje	Nuo 50 iki 59 metų	Aukštasis universitetinis
A6	Finansų ministerija	Vadovaujančios pareigos	24 metai valstybės tarnyboje	Nuo 40 iki 49 metų	Aukštasis universitetinis
A7	NVO „Pilietinio atsparumo centras“	Kova su dezinformacija	10 metų	Nuo 50 iki 59 metų	Aukštasis universitetinis
A8	Lietuvos Respublikos seimo NSGK	Komiteto narys	12 metų valstybės tarnyboje	Nuo 40 iki 49 metų	Aukštasis universitetinis
A9	Vilniaus miesto taryba	Tarybos narys. Aplinkos komitetas ir Kontrolės komitetas.	30 metų valstybės tarnyboje	Nuo 40 iki 49 metų	Aukštasis universitetinis
A10	Lietuvos kariuomenės Strateginės komunikacijos departamentas.	Vadovaujančios pareigos	27 metai valstybės tarnyboje	Nuo 40 iki 49 metų	Aukštasis universitetinis
A11	VSD	Žvalgybos politika	10 metų	Nuo 50 iki 59 metų	Aukštasis universitetinis
A12	Nacionalinis krizių valdymo centras.	Vadovaujančios pareigos	25 metai valstybės tarnyboje	Nuo 50 iki 59 metų	Aukštasis universitetinis

Šaltinis: (sudaryta autoriaus, remiantis empirinio tyrimo duomenimis)

Tyrimo instrumentas: Tyrimo instrumento klausimai sudaryti remiantis literatūros apžvalgos dalių išvadomis. Tyrimo instrumento struktūra pateikiama 4 lentelėje

4 lentelė *Tyrimo instrumento struktūra*

Struktūrinis elementas	Klausimas	Pagrindimas
1. Hibridinių grėsmių suvokimas ir valdymas	1. Hibridinės grėsmės apibūdinamos kaip skirtingų priemonių kombinacija, naudojama siekiant nedeklaruotų strateginių tikslų. Jos pasireiškia per skirtingus valstybės galios šaltinius. Su kokiomis hibridinėmis grėsmėmis tenka susidurti jūsų organizacijoje?	Klausimas skirtas nustatyti kaip organizacijos supranta grėsmes ir ar yra bendras situacijos suvokimas tarp valstybinių institucijų.
	2. Kokių, standartinėse procedūrose neišreikštų, iššūkių tai sukelia?	
2. Įgaliotas vykdymas	3. Kokiu būdu jūsų organizacijoje užtikrinamas vizijos suderinamumo su veiksmais principas (t.y. ar kiekvienas darbuotojas savo veikloje vadovaujasi valstybės, organizacijos vizijomis ir tikslais)?	Bendros vizijos kūrimas: Bendra vizija reiškia gebėjimą sukurti ir išlaikyti kolektyvinį tikslo ir krypties jausmą organizacijoje. Tai yra viena iš sąlygų įgaliotam vykdymui.
	4. Kaip jūsų organizacijoje veikia sprendimų priėmimo delegavimo principas, esant neatidėliotinoms situacijoms?	Įgaliotas vykdymas.
3. Tarpinstitucinė sąveika ir tarptautinis bendradarbiavimas	5. Kaip, kilus nenumatytų situacijų arba grėsmių, koordinuojate veiksmus su kitomis institucijomis? 6. Ar tai yra reglamentuota? 7. Ar yra taikoma praktika keistis sąveikos pareigūnais su kitomis institucijomis (pasitikėjimo ir bendro situacijos suvokimo užtikrinimas)? 8. Kokios kuriamos tarpinstitucinės komandos grėsmėms identifikuoti ir suvaldyti?	Poveikis per kitas valstybes ir tarptautines institucijas išryškina, kad valstybė yra ne uždara sistema, bet didesnės išorinės sistemos dalis ir tai yra labai svarbus aspektas planuojant atsaką hibridinėms grėsmėms. Tai suponuoja išvadą, kad hibridinės grėsmės yra kompleksinė problema, tačiau į jas reaguoja skirtingos valstybės institucijos. Taigi, reikalingas sisteminis modelis, užtikrinantis koordinuotą atsaką į grėsmes, kylančias per skirtingus valstybės galios šaltinius.
	9. Kokie yra numatyti bendradarbiavimo veiksmai ir procedūros su užsienio partneriais, valdant hibridines grėsmes?	

4 lentelės tęsinys Tyrimo instrumento struktūra

Struktūrinis elementas	Klausimas	Pagrindimas
4. Informacijos dalijimasis	10. Kaip veikia informacijos dalijimasis tarp LR Žvalgybos įstatymo subjektų? 11. Ar, jūsų nuomone, jis yra efektyvus? 12. Ką reikėtų pakeisti? 13. Kokių yra biurokratinių kliūčių savalaikiai ir efektyviai dalintis žvalgybine informacija su ne LR Žvalgybos įstatymo subjektais, esant neatidėliotinai būtinybei? 14. Kaip vertinate F3EAD ciklo taikymo perspektyvą, hibridinių grėsmių užkardymui (klausimas žvalgybos ir jėgos struktūrų atstovams)?	Biurokratinės kliūtys. Dėl biurokratinių barjerų ir institucinės struktūros suvaržymų informacija dažnai nepasiekdavo tinkamų asmenų ar institucijų. Skirtingos agentūros neturėjo efektyvių mechanizmų dalintis svarbia informacija ar koordinuoti veiksmus. Rekomenduota sustiprinti informacijos dalijimąsi tarp žvalgybos ir saugumo agentūrų, taip pat tarp federalinių, valstybinių ir vietos lygmenų. Taip pat pabrėžta tarptautinio bendradarbiavimo svarba terorizmo prevencijos srityje.
5. Besimokančios organizacijos modelio taikymas	15. Kaip kaupiama informacija, susijusi su hibridinių grėsmių valdymu? 16. Kaip keičiama hibridinių grėsmių valdymo sistema, remiantis sukaupta informacija?	Klausimų grupė, skirta identifikuoti valstybės, kaip besimokančios organizacijos potencialą bei gebėjimą prisitaikyti, reaguojant į hibridines grėsmes.
6. Papildomi klausimai	17. Kokiais klausimais, jūsų manymu, vertėtų papildyti šį klausimyną? 18. Galbūt galėtumėte rekomenduoti su kuo dar vertėtų pasikalbėti šia tema?	

Šaltinis: (sudaryta autoriaus, remiantis literatūros analize)

Tyrimo instrumentas yra sudarytas iš šešių kategorijų, kurias iš viso sudaro aštuoniolika klausimų. 1 grupės klausimai skirti išsiaiškinti hibridinių grėsmių suvokimo lygį ir valdymo strategijas bei atsakyti į tyrimo klausimus Nr. 1 ir Nr. 2. Įgaliotas vykdymas, kaip viena iš besimokančios adaptyvios organizacijos savybių yra analizuojamas 2 klausimų grupėje. Pasitikėjimo ir bendro tikslo aspektui įvertinti yra skirta 3 klausimų grupė. 4 klausimų grupė skirta išsiaiškinti informacijos dalijimosi efektyvumą bei identifikuoti potencialias reglamentavimo spragas, panašias į tas, kurios sudarė sąlygas 2001-ųjų rugsėjo 11-osios teroristiniam aktui Jungtinėse Amerikos valstijose. 5 klausimų grupė skirta išsiaiškinti, kaip valstybė sugeba įgyvendinti identifikuotų ir išmoktų pamokų ciklą, remdamasi išankstine gaunama informacija bei atlikus analizę, hibridinėms grėsmėms tapus realiais išpuoliais. 6 klausimų grupės paskirtis – išplėsti tyrimo ribas, siekiant

prisotinimo efekto. Klausimynas buvo naudojamas kaip pagalbinis instrumentas, atliekant interviu – klausimai buvo užduodami, atsižvelgiant į organizacijos kontekstą, informantų ekspertinę sritį bei pokalbio eigą.

Empirinio tyrimo vykdymas: tyrimas buvo vykdomas 2024 m. balandžio 15 – gegužės 8 d. Vidutinė vieno interviu trukmė buvo 37 minutės ir priklausė nuo organizacijos konteksto. Susitikimai buvo vykdomi gyvai, su Lietuvos Respublikos seimo NSGK nariu interviu vyko naudojantis *„MS Teams“* programa. Garso įrašai atlikti naudojantis programa *„iPhone Voice Memos“*. Transkribuota, naudojantis svetainės www.semantika.lt transkribavimo funkcija.

Tyrimo ribotumas: kalbant temomis, susijusiomis su nacionaliniu saugumu, labai svarbu išlaikyti diskretiškumą. Kadangi apklausiami buvo vadovaujančio lygmens asmenys, kertinėse valstybinėse institucijose, kilo sunkumų susiderinti susitikimų laikus, juos nekartą teko keisti. Kai kurie susitikimai vyko viešosiose vietose, esant aplinkinių triukšmų, todėl transkribavimo programa sunkiai atpažino garso įrašus ir teko transkribuoti rankiniu būdu.

Tyrimo etika: vykdant tyrimą buvo laikomasi geranoriškumo principo, o siekiant išlaikyti konfidencialumą, informantų duomenys yra nuasmeninti, o pareigos pristatomos apibendrintai.

3.2. Empirinio tyrimo duomenų analizė

Empirinio tyrimo duomenų analizės tikslas – atsakyti į tyrimo klausimus. „Kokybinio interviu tyrimo ataskaitos struktūra atitinka įprastas socialinių tyrimų ataskaitas. Tačiau ji skiriasi rezultatų pateikimo būdu. Interviu metu duomenys surenkami teksto forma, o analizė nėra pagrįsta skaičiavimais. Todėl interviu tyrimo ataskaitoje rezultatai pristatomi pasitelkiant procesų schemas, lenteles (su temomis, kategorijomis, klasifikacijomis, bet ne skaičiais)“ (Gaižauskaitė ir Valavičienė, 2016). Duomenys bus pateikiami lentelėse, pagal klausimyno kategorijas.

Empirinio tyrimo metu buvo siekiama išsiaiškint hibridinių grėsmių suvokimo ir vertinimo lygį skirtingose valstybės institucijose. Hibridinių grėsmių suvokimas bei atvejai Lietuvoje pateikiama 5 – 7 lentelėse.

5 lentelė *Hibridinių grėsmių suvokimas*

Skirtinga terminologija kelia iššūkių	„[...] visos, šalys Vakaruose, įskaitant tiek NATO, tiek Europos Sąjungą, sutinka, kad tos hibridinės grėsmės yra problema, bet niekas to nesupranta - kokia, Kita-, kad nėra bendro supratimo vieningo, tai trukdo duoti atsaką joms“ (A1) „Pagrindinis iššūkis yra dabar, kadangi tai santykinai nauja sąvoka [...] kas yra hibridas ir kaip hibridas veikia, ir tai dar ne visi sutariame. [...] didžiausias iššūkis – naudoti vieną terminologiją, ją išsigryninti ir apsibrėžti, kas yra hibridinės grėsmės kad visi mes vienodai suvoktumėm jas“ (A3) „vieni žmonės vertina tai kaip tokią paradigmą, kuria galima remtis tiek vertinant grėsmes valstybei, tiek formuojant tam tikras mūsų gynybos priemones ir atgrasymo priemones. Ir kiti žmonės mano, kad tai yra [...] toksai neaiškus konceptas, kuris yra sunkiai vertintinas ir sunkiai apibrėžiamas.“ (A8). „common understanding (liet. Bendras supratimas – autoriaus pastaba) – mums šito trūksta. Mes turime kalbėti vienoda kalba, vienoda terminologija, kad mes suprastumėme. Tada sekantis dalykas, aišku, yra atpažinimas ir dekonstrukcija - informacinių karų, arba jeigu tu matai, kažkoks energetinis šantažas… Ta prasme, ir viešumas - čia labai svarbu ir viešumas yra“ (A1).

Šaltinis: (sudaryta autoriaus, remiantis empirinio tyrimo duomenimis)

Apibendrinant 5 lentelėje pateiktus empirinio tyrimo duomenis, daromos išvados, kad Vakarų šalys, įskaitant NATO ir Europos Sąjungos valstybes, sutinka, jog hibridinės grėsmės yra rimta problema, tačiau trūksta bendro supratimo ir vieningos terminologijos apibrėžiant šią sąvoką. Svarbiausias iššūkis yra nustatyti, kas iš tikrųjų yra hibridinės grėsmės ir kaip jos veikia, siekiant užtikrinti vienodą supratimą apie jų pobūdį ir iššūkius. Skirtingi požiūriai į šias grėsmes rodo, kad vieni vertina jas kaip naują paradigmą, kuria galima remtis vertinant valstybės grėsmes ir formuojant gynybos priemones, o kiti laiko jas neaiškiu ir sunkiai vertinamu konceptu.

6 lentelė *Hibridinių išpuolių atvejai Lietuvoje per informacinę erdvę*

Informacinės atakos	„Daugiausiai su informacinėmis atakomis su ta netikra informacija, o daugiausia kova, kova su ja vyksta žiniasklaidoje. Tai per socialinius tinklus, per žiniasklaidą“ (A4). „Dezinformacija, su kitom netenka“ (A7). „Pagrindinės grėsmės Vilniaus miesto savivaldybei, kaip ir Lietuvai, turbūt yra informacinės“ (A9). „Nuo 2014 metų vienaip ar kitaip kovojame su rusų dezinformacija ir dabar jau prasideda po truputėlį kinų rodymasis“ (A7). „Pagrindinė grėsmė - tai yra informacinis spaudimas, informacinės atakos, psichologinės operacijos prieš Lietuvą“ (A10). „Tai gali būti nuo paprasčiausių dalykų, tos pačios artilerijos sviedinių gamykla, paminklo pastatymas – visur stengiamasi įnešti sumaištį“ (A7).
Poveikis per kultūrą	„konkrečiai, visą tai, kas yra susiję su mūsų istorine atmintimi, istorinės atminties įamžinimu“ (A9). „Prie DIMEFIL gali drąsiai pridėti C – Culture, nes jie neidėję, Culture, ir mes, NATO visada badydavom nosį – pridėkit kultūrą, nes ją rusai naudoja kaip ginklą – labai rimtai išnaudoja – pridėkit kultūrą“ (A1). „istorija yra tarp kultūros ir socialinės dimensijų [...] yra formuojamas žmonių suvokimas [...] kultūra irgi yra svarbu ir ką mes matome: Tie visi dainininkai, ne tik rusų, bet čia paskutinis įvykis su italų dainininkų, kuris nuvažiavo, padainavo Putinui, pašventė kartu su juo Kremliuje, ir paskui jis atvažiuoja pas mus į Šiaulius koncertuoti. [...] Jeigu tai būtų neišnaudojama paskui, nebūtų problemos“ (A3). „ką dabar pasakoja baltarusių disidentai arba opozicionieriai, kaip jie savinasi Lietuvos istoriją [...] Ir tai šneka rimti profesoriai, kurie skaito pranešimus Amerikoje, Lenkijoje, Olandijoje. [...], vidinei auditorijai, kai tu pasakoji, kad Vilnius - tai yra tavo protėviai [...] dėl to, kad ten yra fašistinis režimas, supuvę Vakarai, negali aplankyti savo senelių, tėvelių, prosenelių kapų. [...] tada yra išorinė auditorija. [...] vaikas kuriam 15 metų, iš kur jam žinot, kad tas profesorius, oficialiai pripažintas Vakarų universitetų, ir jisai pasakoja šitą tiesą. Ateis kita karta, ir jai jau bus kitokia istorija diegiama, tai va čia yra ta ilgalaikė perspektyva“ (A3). „nėra sisteminio požiūrio dėl to, kad nėra sisteminio požiūrio valstybėje. ta prasme, ką jau minėjau: desovietizaciją – nevyksta, liustracija – nebuvo iki galo padaryta“ (A9).

Šaltinis: (sudaryta autoriaus, remiantis empirinio tyrimo duomenimis)

Empirinio tyrimo duomenys, pateikti 6 lentelėje, išryškina informacines atakas ir jų poveikį, kaip vieną iš hibridinių grėsmių šaltinių.

Daugiausiai informacinių atakų vyksta per netikros informacijos platinimą ir svarbų vaidmenį čia vaidina žiniasklaida, įskaitant socialinius tinklus. Taip pat pastebima, kad šalia rusų dezinformacijos, jau atsiranda ir kinų informacinio poveikio atvejų.

Taip pat atskleidžiamas kultūros, kaip informacinio poveikio priemonės aspektas. Kultūra yra naudojama kaip ginklas, ir tai gali turėti rimtų padarinių, nes ji veikia žmonių suvokimą ir istorinę atmintį. Be to, nėra sistemingo požiūrio į desovietizaciją ir liustraciją, kas daro valstybę pažeidžiamą.

7 lentelė *Hibridinių grėsmių atvejai Lietuvoje per ekonomikos sritį*

Ekonominės poveikio priemonės	„taip pat yra turbūt sankcijos, kurios kartais yra oficialios. Kartais jos yra neoficialios kaip kad Kinijos Respublika pritaikė neoficialias sankcijas. Nieko oficialiai nepaskelbė, bet, pritaikius poveikio priemones per savo poveikio kanalus valstybėje, Lietuvos verslui ir rezultatams, kuriuos gauna Lietuvos eksportuotojai, buvo padarytas poveikis [...] galimos ir oficialios sankcijos. Dabar jos vykdomos iš mūsų pusės kitoms valstybėms“ (A6).
	„Kinija ir yra ta pagrindinė priežastis, dėl savo veikimo visame pasaulyje, kuris tapo labai rimtu spėjimu, kas gali nutikti, jeigu tu nesukontroliuosi [...] baisiausias pavyzdys yra Afrika, kur kai kuriose Afrikos valstybėse […] pagrindiniai valstybės resursai nebėra prieinami vyriausybei ir tarša, pavyzdžiui, kuri yra sukeliaman, nesilaikant aplinkosauginių reikalavimų, vykdant, pavyzdžiui, kasybos darbus, yra tai, kas kainuoja tiesiog masiškai žmonių sveikatą ir gyvybes“ (A8).

Šaltinis: (sudaryta autoriaus, remiantis empirinio tyrimo duomenimis)

7 lentelėje pateikti empirinio tyrimo duomenys parodo, kad ekonominės poveikio priemonės, ypač tokios kaip sankcijos, ir užsienio investicijos, turi plačias ir daugialypes pasekmes tiek vietiniu, tiek globaliu mastu. Tai reikalauja atidžiai vertinti ir nuolat stebėti situaciją, siekiant minimalizuoti neigiamą poveikį.

8 lentelė *Kitos hibridinės grėsmės*

Instrumentalizuota migracija	„Na, visų pirma, tai nauja sąvoka, kuri atsirado būtent pastarųjų keleto metų laikotarpiu. Tai ta instrumentalizuota migracija, tai, apie ką anksčiau išvis nebuvo šnekėta, kai valstybė, kaimynė, kaip viena iš poveikio priemonių, pasinaudojo tais nelegaliais migrantais“ (A5).
Kibernetika	„dalis turbūt grėsmių yra tokių tiesioginių, tame tarpe matyti, kad ir užsienio tarnybų žvalgybos institucijos kartais domisi duomenimis, kurie yra susiję su finansais, ir natūralu, kad duomenys, kurie susiję su finansais, turi savyje daug kitos informacijos. Tai yra bandymų įsilaužti į informacines sistemas, pasižiūrėti kas kokius finansus naudoja, kokiomis programomis naudojasi. [...] tam, kad būtų galima ateityje turėti poveikio“ (A6).
Politinis poveikis	„Hibridinių grėsmių šaltinių pagrindinis tikslas yra padaryti poveikį politikams, politiniams sprendimams ir santvarkai Lietuvoje, valstybėje, [...] destabilizuoti padėtį, kad paveikti politinius sprendimus, kad politikai priimtų, tam šaltiniui, iš kurio kyla grėsmė, reikalingus politinius sprendimus“ (A3). „Tikslas vienas visada – destabilizuoti šalį, tai yra senas […] *modus operandi* – ieškoti bet kokios progos visuomenėje įnešti sumaištį” (A7). „kai kalbame apie Lietuvą, tai nuo informacinių incidentų, kuomet yra, paskleidžiama tam tikra klaidinanti informacija ir bandoma visuomenėje paskleisti tam tikras neteisingas žinias ir sukiršinti žmones iki tokios situacijos, kada […] mes kalbame apie patį rinkimų proceso organizavimą, (bandoma – autoriaus pastaba) daryti poveikį, siekiant iškelti tam tikras jėgas, kurios yra kaip tik prorusiškos, prokremliškos ir palankios mums grėsmę keliančioms valstybėms“ (A8). „vadinamasis įstatyminis kariavimas – *Lawfare*, ką tikrai kiniečiai labai gerai sugeba daryti tai daryti tam tikrą spaudimą, priimti sau palankius įstatymų projektus ir kitus teisės aktus, kurie leistų jiems iš esmės perimti tam tikros valstybės resursų valdymą ir ypatingai jie yra orientuoti į kritinės infrastruktūros valdymą. Labai džiaugiuosi, kad mes sugebėjome tam atsispirti. Nuo, pavyzdžiui, 5G tinklo plėtroje „Huawei“ dalyvavimo iki Klaipėdos uosto apsaugos nuo patekimo į daug nemalonesnę situaciją, negu galėtų būti“ (A8). „prašė manęs užduoti klausimą toje diskusijoje Kinijos užsienio reikalų ministrui kodėl Lietuvos piliečiams neišduodamos vizos. […] buvo visiškai sustojęs procesas […] keletą mėnesių net nebuvo jokio normalaus paaiškinimo – techninės kliūtys – negali išduoti vizų Lietuvos piliečiams keliauti į Kiniją“ (A8).

Šaltinis: (sudaryta autoriaus, remiantis empirinio tyrimo duomenimis)

Iš 8 lentelėje pateiktų empirinio tyrimo duomenų matyti, kad hibridinės grėsmės apima įvairius veiksnius, įskaitant migraciją, kibernetinį saugumą ir įtaką politiniams sprendimams, dažnai, siekiant daryti įtaką politinei sistemai ir destabilizuoti valstybės santvarką. Šios grėsmės dažnai veikia subtilesniais būdais, tokiais, kaip manipuliacija informacija ar darymu įtakos teisės aktų pakeitimams, kurie galiausiai gali kelti pavojų nacionaliniam saugumui ir stabilumui. Tai parodo, kad būtina suprasti ir atidžiai stebėti įvairias grėsmių formas, siekiant efektyviai reaguoti ir apsaugoti valstybės interesus.

9 lentelė *Kombinuotų hibridinių išpuolių atvejai Lietuvoje, veikiant kelis sektorius*

Poveikis finansų sektoriui per informacinę erdvę	„galimos poveikio priemonės, su kurioms iki šiol Lietuva buvo susidūrusi labiau praeityje, tai pačios finansų sistemos stabilumas ir bandymas paveikti informacinį lauką, kai yra diskredituojamas vienas kitas didelis finansų rinkos žaidėjas, ir natūralu, kad tai gali daryti poveikį žmonių pasitikėjimui. O finansų sistemai pasitikėjimas yra viskas. Jeigu nėra pasitikėjimo vienų ar kitų rinkos žaidėjų, žmonės linkę atitraukti pinigus iš jo, ir natūralu, kad stabilumas galėtų susvyruoti“ (A6).
Poveikis kombinuotai per kibernetinę ir informacinę erdves	„Hibridinės grėsmės eina kompleksiškai. Jos neveikia vieną sektorių“ (A3). „Mūsų organizacija susiduria su visom šitom apraiškom, Rusijos žvalgybos tarnybų veikimas eina tiek per diplomatinę liniją [...] yra bandoma ekonominį saugumą paveikti, finansus. [...] kinetinės, netgi operacijos su paminklų išniekinimu su gadinimu transporto priemonių [...] Volkovo *case'as* (atvejis – autoriaus pastaba). Esmė yra ne to žmogaus sumušime, bet bauginime“ (A11). „buvo paskelbtas sankcijų paketas ir buvo padaryta kibernetinė ataka prieš Lietuvos geležinkelius. [...] Tame kontekste automatiškai išstojo rusų remiami *hakeriai* ir pasakė: mes padarėme įspėjimą. Daromas politinis spaudimas. automatiškai politikai įstojo, kad jeigu jūs toliau taip sankcijas taikysite, mes paralyžiuosime jūsų geležinkelius. Mes sutrukdysime jūsų tiekimą. [...] Paskui pasirodo žinutės, kad visi vagonai Lietuvos geležinkelių yra registruoti bendroje sistemoje, kurią valdo Maskva, ir jie žino kiekvieną vagoną, kur jis važiuoja ir t. t. [...] paaiškėja, galų gale, kad ta registracija vagonų yra niekinė. Vis viena automatinė elektroninė valdymo sistema yra valdoma Lietuvoje, yra autonominė, tiktai kad vagonų, su kuriais vykdomas tranzitas, registracijos numeriai suteikti Maskvoje“ (A3).
Poveikis kombinuotai per diplomatinį ir ekonominį spaudimą	„mes buvome tiesiogiai įtraukti į visus tuos pakankamai sudėtingus procesus, kai būtent naudodami diplomatines priemones, spaudimą, diplomatines, ekonomines priemones, buvo daromas didžiulis spaudimas mums nevystyti santykių su Taivanu“ (A8).

Šaltinis: (sudaryta autoriaus, remiantis empirinio tyrimo duomenimis)

Apibendrinant 9 lentelėje pateiktus empirinio tyrimo duomenis, daromos išvados, kad hibridinės grėsmės veikia kompleksiškai ir neapima vieno sektoriaus. Jos apima įvairias sritis, įskaitant finansų sistemą, informacinį lauką, diplomatinius santykius ir netgi fizines operacijas. Tai reikalauja integruoto požiūrio ir įvairių strategijų taikymo, siekiant užtikrinti valstybės saugumą ir stabilumą.

10 lentelė *Įgalioto vykdymo atvejai Lietuvos institucijose*

Atsakomybės prisiėmimas	„stebėsenos įgalinimas, institucijų atsakomybės turėjimas. Nelaukit, kol situacija bus tokia, kad jūs jos negalėsit suvaldyti ir tada prašysit kažko kitų, kad ateitų į pagalbą, bet būkit atsakingi už tą sritį ir šitoje vietoj veikite kuo greičiau. Prisiimkite atsakomybę. Turėkit įrankius, turėkit kompetencijos ir turėkit pajėgumus“ (A12).
Pamatuota veiksmų laisvė	„Šaulių sąjunga, nors ir yra sukarinta visuomeninė organizacija, nors mums yra taikomi subordinacijos, hierarchijos, pavaldumo principai, bet mūsų viena iš stiprybių yra pamatuota veiksmų laisvė ir iniciatyva“ (A2).
Kompetencijų pasitelkimas	„gal labiau ne veikti ir reaguoti į krizę, bet labiau padėti identifikuoti galimą potencialią riziką, nes kartais žmonės savo darbe susiduria su situacija, kuomet matai, kad įvykis yra netipinis, nestandartinius, tame tarpe, pavyzdžiui, muitinė arba pati mokesčių inspekcija, kai tu turi tam tikrus duomenis, jie tau kelia klausimų, galėtum šiaip nereaguoti, bet jeigu matai bendrą valstybės tikslą, bendrą savo organizacijos tikslą, matyt, gali identifikuoti, kad tai yra nauja rizika, nauja grėsmė, kurią galbūt ir tavo vadovai, ir aukštesni pareigūnai, turėtų įvertinti ir tiesiog praneši per savo kanalus apie galimas rizikas aukščiau ir tie kiti žmonės priima sprendimus, kurie padėtų sistemiškai pasižiūrėti į kylančias rizikas. [...] Matyt, žmonės gali pastebėti tokius dalykus, kurių tu iš anksto negali visų modelių įvertinti, bet žmonės iš apačios tai gali tiesiog identifikuoti, kad tai yra spręstina problema“ (A6).

Šaltinis: (sudaryta autoriaus, remiantis empirinio tyrimo duomenimis)

10 lentelėje pateikti empirinio tyrimo duomenys atskleidžia, kad įgaliotas vykdymas yra esminė besimokančios, adaptyvios organizacijos savybė, kuri užtikrina jos gebėjimą operatyviai reaguoti į nenumatytas ir nestandartines situacijas. Ši savybė apima gebėjimą deleguoti galias ir atsakomybes bei suteikti darbuotojams ar komandoms laisvę priimti sprendimus ir veikti, kadangi jie yra labiausiai kompetentingi spręsti tam tikras problemas. Pamatuota veiksmų laisvė ir iniciatyva gali būti stiprybė, net jei organizacija veikia pagal subordinacijos ir hierarchijos principus. Tokios savybės leidžia greitai prisitaikyti prie kintančių situacijų ir veikti efektyviai net sudėtingose sąlygose. Svarbu ne tik reaguoti į krizes, bet ir padėti identifikuoti potencialias rizikas. Darbuotojai gali pastebėti netipinius arba nestandartinius įvykius savo darbe. Pranešdami apie šias rizikas, jie padeda organizacijai ir jos vadovams sistemingai įvertinti pavojus ir imtis prevencinių veiksmų. Šis žinių srautas iš apačios gali būti nepakeičiamas, siekiant užtikrinti organizacijos veiklos stabilumą ir saugumą. Empirinio tyrimo duomenys parodo, kad įgalioto vykdymo praktika Lietuvos institucijose ir organizacijose ne tik egzistuoja, bet ir yra skatintina.

11 lentelė *Tarpinstitucinė sąveika ir tarptautinis bendradarbiavimas*

Bendras supratimas	„pirmas žingsnis yra common understanding (bendras supratimas – aut. Pastaba) - tiek kariuomenė, tiek VRM'as turi pradėti kalbėti viena kalba ir sutarti“ (A1). „noriu pabrėžti, kad atsakas į hibridinę grėsmę taip pat turi būti sinchronizuotas su kitom ministerijom, su kitom institucijom“ (A10). „kalbėjimas apie hibridą, apie „žalius žmogeliukus“ suteikia galimybę sakyti, kad čia yra rusų būdas veikti ir jie tą daro“ (A11). „Todėl, kad tu turi, kai pats jau susigaudai struktūroje, tada turi būti trim kryptim darbas: dalinamasi su kolegom, raportuojama vadovybei ir edukuojama visuomenė - tokie trys srautai“ (A1). „Pastaruoju metu, kadangi daug tų grėsmių buvo, tai išties kyla daugiau tokių atvejų, kuomet yra tarpinstituciniai pasikalbėjimai ir bandymas išspręsti problemas kartu susėdus“ (A6).
Tarpinstitucinis bendradarbiavimas	„Yra numatyta turėti ir planus, ir vykdyti intensyvią sąveiką su valstybės savivaldos institucijomis, karo komendantūromis, turėti bendras pratybas“ (A2). „Mūsų veikimo principas yra toks, kad mes, turint konkrečią situaciją, galime pasitelkti iš bet kokios valstybinės institucijos ekspertų. Tie ekspertai pas mus atvyksta, ir mes sprendžiame vieną ar kitą klausimą ir ekspertai grįžta atgal į savo institucijas, taip neprarasdami kvalifikacijos, įgūdžių, tinklo ekspertų ir pan. [...] mūsų centras toks daugiau yra apjungiantis, koordinuojantis ir tuo pačiu stebintis situaciją ir, reikalui esant, mes aktyvuojam tuos nusistovėjusius ekspertų formatus, kurie yra reikalingi vienai ar kitai situacijai spręsti“ (A12 „labai svarbu, kad tiek kariuomenė, tiek Krašto apsaugos ministerija, dažnai Vidaus reikalų ministeriją arba „kibernetikai“ kitos institucijos, taip pat veiktų, sinchronizuotai“ (A10). „Tai teoriškai turėtumėme turėti kontaktą su Vyriausybės krizių valdymo centru. Patirties, dirbant su šituo centru, jau turime per NATO viršūnių susitikimą, kai parėmėme Krizių valdymo centrą savo ekspertize“ (A2). „Istoriniai pavyzdžiai - turbūt migrantų krizė yra geriausia. Čia daugiausiai koordinavo Vidaus reikalų ministerija – Pasienis“ (A10). „įstatymas numato galimybę Vyriausybei paskirti, visų pirma pripažinti, kad reikalinga konkreti operacija vienai ar kitai situacijai spręsti, ir tada Vyriausybės sprendimu yra priimamas sprendimas, kas bus tos operacijos vadovas, ir su šituo sprendimu ateina ir atsakomybė, bet ateina tuo pačiu, ir įgalina tą vadovą priimti nurodomuosius sprendimus, kurie tampa privalomi kitom institucijom“ (A12). „migrantų krizė parodė, kad tiek pasieniečiai, tiek muitinė, tiek policija gali dirbti bendrai, bet kartais to koordinavimosi reikia šiek tiek daugiau“ (A6). „Covid'o atvejis, kur taip pat vyko tam tikra koordinacija“ (A10). „Tai va čia, šitoje vietoj tas lankstumas, kuomet, jeigu mes turime daugiafunkcinę krizę, kur daug yra sektorių vienu metu įtraukta, vienas ministras negali spręsti, tarkim, kitų sferų, nes tai yra ne jo atsakomybės zona. Tai mes turime tokią sistemą, kuomet Vyriausybė deleguoja tokią funkciją - būti operacijos vadovu, kad ir krizių valdymo centro vadovą“ (A12). „kadangi pastaruoju metu tikrai daug buvo vienas po kito sekančių tokių įvykių, kur reikia tarpinstitucinio bendradarbiavimo, tai sakyčiau, kad ta kultūra yra linkusi augti, bendradarbiavimo tarpusavyje“ (A6). „Taip. Nebūtinai tie pareigūnai yra pastovūs. Jie yra numatyti tam tikroms situacijoms. Per migrantų krizę mes ne tik turėjome savo sąveikos pareigūnus, bet ir dalį savo ryšio sistemos“ (A11).
Tarptautinis bendradarbiavimas	„visų pirma, tai nauja sąvoka, kuri atsirado būtent pastarųjų keleto metų laikotarpiu. Tai ta instrumentalizuota migracija, tai, apie ką anksčiau išvis nebuvo šnekėta, kai valstybė, kaimynė, kaip viena iš poveikio priemonių, pasinaudojo tais nelegaliais migrantais, tai dabar šiek tiek ta situacija yra suvaldyta ir ne be Europos Komisijos pagalbos, nes mūsų, pavyzdžiui, diplomatija būtų šitoje vietoje per silpna. [...] kai buvo organizuoti tiesioginiai skrydžiai į Minską, tai ne Lietuvos diplomatai, o būtent Europos mastu diplomatai šnekėjosi su tų trečių šalių oro uostais, su kompanijom, su perspėjimais dėl galimų sankcijų ir t. t. Kas iš tikrųjų prisidėjo, nes tie skrydžiai, kaip ir tokie, nustojo“ (A5). „krizių valdymo centro sustiprėjimas ir jų vystymasis tai yra didžiulis žingsnis į priekį, koordinuojant veiksmus tarp institucijų“ (A10). „buvo kalbama ir Europos mastu, nes dar vienas spaudimas, kurį mes gavome, tai tos visos nevyriausybinės organizacijos“ (A5).

Šaltinis: (sudaryta autoriaus, remiantis empirinio tyrimo duomenimis)

Apibendrinant 11 lentelėje pateiktus empirinio tyrimo duomenis, galima daryti išvadą, kad pasitikėjimas ir bendras tikslas yra esminiai veiksniai, kurie, susidūrus su hibridinėmis grėsmėmis, užtikrina sklandų tarpinstitucinį ir tarptautinį bendradarbiavimą. Šie veiksniai leidžia suinteresuotoms šalims veikti kartu ir koordinuotai, siekiant bendrų tikslų. Siekiant efektyvaus bendradarbiavimo, bendras situacijos suvokimas yra esminė sąlyga. Pasitikėjimas, bendras tikslas ir bendras situacijos suvokimas - sukuria tvirtą pagrindą tarpinstituciniam ir tarptautiniam bendradarbiavimui, kuris yra būtinas norint veiksmingai įveikti hibridines grėsmes. Tai leidžia suinteresuotoms šalims veikti kartu kaip vieninga ir koordinuota jėga, susidūrus su kompleksiniais iššūkiais.

Analizuojant empirinio tyrimo duomenis, aiškiai matyti, kad tarpinstitucinis ir tarptautinis bendradarbiavimas yra svarbūs veiksniai, leidžiantys efektyviai reaguoti, susidūrus su kompleksinėmis problemomis, tokiomis, kaip hibridiniai išpuoliai. Šie duomenys pateikia įvairius aspektus, kurie yra esminiai vertinant iš atsparumo hibridinėms grėsmėms perspektyvos:

Tarpinstitucinis bendradarbiavimas prasideda nuo vieningo supratimo ir kalbėjimo vienodais terminais apie grėsmes bei jų pobūdį. Institucijos turi kalbėti viena kalba (terminologija) ir sutarti dėl bendrų veiksmų Komunikacija ir sinchronizacija su kitomis institucijomis yra būtina, siekiant efektyviai reaguoti į grėsmes. Edukacija ir visuomenės švietimas taip pat yra svarbūs aspektai, kad būtų užtikrintas bendras supratimas ir reagavimas.

12 lentelė *Hibridinių grėsmių valdymas per informacijos dalijimąsi*

Informacijos valdymas per operacijų centrus	„jeigu tai susiję su kitomis ministerijomis, kas dažnai būna, su Vidaus reikalų, tada koordinuojame per Nacionalinį krizių valdymo centrą. Ten yra ir budėtojai, ten yra atsakingi žmonės, ir ten priimami sprendimai, kaip reaguojame ir kas reaguoja, tai ta koordinacija yra gerai išvystyta“ (A10). „Tai yra standartinės procedūros – yra *SITCEN‘as* (Situacijų stebėjimo centras – autoriaus pastaba), kuris veikia 24/7 [...], gauna visą informaciją, veikia tarptautiniu ryšiu. Jei partneriai vidury nakties perduoda kažkokią informaciją, kuri yra labai svarbi, tai SITCEN‘as žino ką turi daryti, kam skambinti, pagal procedūras. Tai yra ne tik *pradrill‘inta* (išbandyta pratybų metu – autoriaus pastaba), bet ir veikia“(A11).
Techniniai informacijos valdymo būdai	„Krašto apsaugos ministerija, jeigu perduoda informaciją, tais biurokratiniais kanalais [...] tai nekyla problemų“ (A4). „Aš manau jau esame šiek tiek kitoje eroje. Informacijos dalinimasis vyksta tokiu įprastu būdu, kad ten kažkokie raštai keliauja, ar tai ten pažymos, ar dar kažkas. Tai mūsų dabar yra pagrindinis tikslas, kad mes tuos informacinius resursus, juos skaitmenizuotume ir kad tas skaitmenizavimas vyktų natūraliai, realiu laiku, apjungiant informacines sistemas į vieną bendrą duomenų ežerą. Ir iš tų duomenų ežero institucijos ima jiems reikalingą informaciją, tada vertina. Mes esame šitam kelyje, šitoje koncepcijoje ir būtent šitą metodą naudojam“ (A12). „Aišku, yra išimčių tam tikrų. Tarkim, žvalgybinė informacija, kuri yra klasifikuota, kuri negali eiti į tą bendrą *pool‘a* informacijos, nes ji yra gauta jautriais metodais ir naudojant žvalgybinius įrankius. Tai ta informacija šiek tiek yra atskirta, bet vėlgi tas apsijungimas duomenų į vieną; ir mūsų centras tą funkciją ir atliekame mes integruojame tiek klasifikuotą informaciją, tiek viešą informaciją ir tada pagal tos informacijos turinį matome bendrą paveikslą“ (A12).

Šaltinis: (sudaryta autoriaus, remiantis empirinio tyrimo duomenimis)

12 lentelėje pateikti empiriniai duomenys parodo, kad valstybės krizių valdymo sistema veikia koordinuotai, o dalijimasis informacija yra efektyvus. Valstybės institucijos, reaguodamos į krizes, aktyviai bendradarbiauja per Nacionalinį krizių valdymo centrą. Tai rodo gerai išvystytą koordinaciją ir komunikaciją tarp skirtingų institucijų, kas yra būtina efektyviam krizių valdymui.

Svarbu pastebėti, kad keitimasis informacija ir sisteminis prieigų suderinimas yra esminis efektyvaus krizių valdymo aspektas. Tai padeda užtikrinti, kad reikalinga informacija būtų prieinama visiems atsakingiems subjektams realiu laiku, leidžiant jiems efektyviai reaguoti į kintančią situaciją.

Šiuolaikinės technologijos leidžia valstybei efektyviau tvarkyti informaciją ir padaryti ją prieinamą visoms suinteresuotosioms pusėms. Tyrimo dalyviai išryškina būtinybę skaitmenizuoti informacijos resursus ir integruoti informacines sistemas į vieną bendrą duomenų bazę. Tai padeda institucijoms greičiau gauti ir analizuoti reikalingą informaciją, reaguojant į įvairias grėsmes.

Nors dauguma informacijos skaitmenizuojama ir prieinama realiu laiku, klasifikuota ar jautri informacija, tokia kaip žvalgybinė informacija, turi būti tvarkoma atskirai. Tačiau siekiant bendro situacijos supratimo, ši klasifikuota informacija taip pat turi būti integruojama į bendrą duomenų apsikeitimo sistemą, kad būtų galima sukurti išsamų situacijos vaizdą.

Visi šie aspektai parodo, kad valstybė aktyviai tobulina savo krizių valdymo sistemą, siekdama greitai reaguoti į įvairias grėsmes ir užtikrinti visuomenės saugumą bei gerovę. Integravimas, ryšių sistemų suderinimas ir skaitmeninis informacijos valdymas yra pagrindiniai veiksniai, kurie leidžia valstybei veikti kaip adaptyviai organizacijai, prisitaikanti prie kompleksinių grėsmių ir besikeičiančios situacijos.

13 lentelė *Hibridinių grėsmių valdymas per organizacijos mokymąsi*

Besimokančios organizacijos principų įgyvendinimas	„Mūsų centras pradėjo funkcionuoti, pradėjo veikti nuo praeitų metų sausio pirmos dienos, priėmus Krizių valdymo ir civilinės saugos įstatymą. Centras funkcionuoja tokiu principu, kad mes turime tris pagrindinius padalinius: situacijų centrą, analizę ir planavimo biurą. Trys padaliniai fokusuojamės į situacijos stebėjimą, situacijos vertinimą ir tam tikrų rekomendacijų ar teisinių kažkokių permainų inicijavimą, kad būtų galima kitą kartą suvaldyti krizę, geriau“ (A12). „Todėl, kad tu turi, kai pats jau susigaudai struktūroje, tada turi būti trim kryptim darbas: dalinamasi su kolegom, raportuojama vadovybei ir edukuojama visuomenė - tokie trys srautai“ (A1).
Teisėkūros pritaikymas, reaguojant į hibridinius išpuolius	„Na, sakykime, jeigu mes paimtumėm dabar hibridinę grėsmę, kuri įvyko 2022-ųjų metų vasarą, su imigrantams, tai iš tiesų buvo kliūčių daug, kurios buvo įveiktos. Kariuomenės pasitelkimas, buvimui pasienyje, kartu su vidaus tarnybos institucijomis. Buvo kliūčių dėl jėgos naudojimo statuto, nes negalėjo naudoti jėgos, negalėjo sulaikyti, negali apžiūrėti mašinų kariuomenė. Tai iš esmės buvo kliūčių daug ne tik kad biurokratinių, bet ir teisinių kliūčių. Tam buvo keisti teisės aktai. Tai buvo padaryta labai greitai, nes grėsmės akivaizdoje reikėjo veikti labai greitai ir visa tai buvo padaroma, bet šitoje vietoj sakyčiau, kad tai buvo teisinės, ne biurokratinės kliūtys“ (A4). „iš vienos ekstremalios situacijos palaipsniui peršokome prie kitos, buvo momentas, kai ir abi žaidėme. Tiek Užsieniečių teisinės padėties įstatymas buvo dažnai keičiamas, ko nebūdavo anksčiau, tiek netgi ir mūsų sienos ir jos apsaugos įstatymas buvo keičiamas pakankamai dažnai. Atsirado tas neįleidimo įteisinimas, nes pačioje pirminėje stadijoje, sakykime, sprendimas, kuriuo mes vadovavomės, buvo tiktai ekstremaliųjų situacijų operacijos vadovo [...] sprendimas. Mes vadovavomės tik tuo sprendimu po to tai buvo įtvirtinta įstatyme“ (A5). „Europos Sąjungos lygiu įtvirtinome migracijos instrumentalizacijos termino naudojimą, ir dabartinės migracijos paketas įtraukia nemažai praktikų, kurios yra paremtos Lietuvos patirtimi dėl grąžinimo, dėl neįleidimo į teritoriją, dėl pagreitintų procedūrų ir kitų procesų“ (A8). „priimant sprendimus dėl investicinių projektų, strateginės reikšmės projektų, ypatingai, susijusių su mūsų energetikos infrastruktūra, buvome prieš keletą metų […] įvertinę, kad grėsmių nacionaliniam saugumui vertinimo komisija prie Vyriausybės labai atsargiai kai kuriuos procesus vertina ir kad teismuose yra pakankamai daug bylinėjimosi ir norėjome sustiprinti tą teisinį reguliavimą, kuris leistų griežčiau uždėti apsauginius filtrus, nes čia, šiuo atveju, yra per daug grėsmės keliantys dalykai“ (A8). „Mes turime tikrai labai atidžiai stebėti, ar nėra teikiami kokie nors įstatymų projektai, matant iš kitų užsienio šalių pavyzdžių, kurie siektų perimti, pavyzdžiui, kritinės infrastruktūros, svarbių objektų valdymą arba daryti įtaką priimant sprendimus dėl jų valdymo […] Viena vertus, mes stebime, ar nėra tokių iniciatyvų ir, kita vertus, patys imamės aktyvių priemonių užkardyti tam tikrą poveikį“ (A8).

13 lentelės tęsinys

Valstybės finansų pritaikymas, reaguojant į hibridinius išpuolius	„pradėkime nuo to, kad fizinis barjeras buvo įdiegtas už biudžetines lėšas ir buvo netgi priimtas atskiras įstatymas“ (A5). „tų poveikio priemonių, jų buvo kelios. Viena buvo kai prasidėjo Lukašenkos imigrantų demaršas iš Baltarusijos, irgi reikėjo rengti staigų paketą priemonių, kuris buvo ir savivaldybėm parama finansinė, priimti tuos žmones, įrengti, kur jie turi gyventi. Reikėjo pastatyti tvorą, fizinį barjerą. Reikėjo apsaugos kamerų, reikėjo naujų pareigūnų, kurie budi prie sienos. Vienas paramos paketas, kitas paramos paketas, prasidėjo, energetikos krizė rengti reikėjo bent du paramos paketus. Kadangi, matyt, buvo tikėtasi, kad greičiau situacija išsispręs, matėsi, kad daro poveikį ne tik gyventojams, bet ir verslui – reikėjo rengti dar vieną paramos paketą, kuriame buvo jau ir priemonės verslui, tęstiniai reakciniai veiksmai, bet jie buvo nesuplanuoti, o labiau reakcija į krizę, bandant išspręsti situaciją“ (A6). „buvo parengtas ir valstybės biudžeto įstatymo pakeitimas, kas turbūt yra pagrindinis valstybės dokumentas ir jam ir parengti, ir pakeisti reikia sutelkti Seime palaikymą pakankamai didelį, kas yra pakankamai sudėtinga. Tai tiek biudžetas, tiek ir buvo energetikos įstatymų įvairių keitimas tam, kad būtų galima pritaikyti paramos priemones ir kainų reguliavimo, prie iššūkių, kurie nutiko“(A6).
Identifikuotos ir išmoktos pamokos	„Nežinojo žmonės kur būriuotis, bet ne mes išmokome pamokas, išmokome, kad mums reikia daryti pratybas. Buvo daromos pratybos. Visi žinojo, ką daryti. Visi žinojo modelį. Žinojo vadovai savo vaidmenį, kaip reikia elgtis, kur rinktis, kam pranešti, kad susirinko. [...] tokia pamoka, kurią taip pat išmokome [...] kad tas saugumas pastato yra svarbus, saugantis nuo tų hibridinių grėsmių“ (A4). „apie informacines ir priešišką informacinę veiklą, tai savo atsakomybės ribose, [...] mes kaupiame savo duomenų bazę. Duomenų bazė yra SKD, ten yra fiksuotas kiekvienas unikalus atvejis yra išsaugoma data, taip pat šaltinis, kita informacija ir remiantis šita statistika darome analizę. Kasmet lyginame tendencijas“(A10). „Pranešta apie sprogmenį. Manęs nėra. Aš esu Vyriausybėje ir esu Vyriausybės slaptame susitikime be telefono. Ir va čia turbūt parodė, kaip veikia sprendimų priėmimas. Jis tuo metu šiek tiek buvo paralyžiuotas. Aš nemačiau (kad skambina – autoriaus pastaba) gal pusvalandį, kol aš pamačiau daugybę žinučių, daugybę skambučių. Na, kažkuriuo metu buvo priimtas sprendimas evakuotis. Iš esmės, tas sprendimas buvo delsiamas, nes buvo laukiama manęs, ir tik aš neatrašiau kažkurį laiką, suprato, kad reikia priimti sprendimą. Tie, kurie yra atsakingi už saugumą, žmonės priėmė sprendimą evakuoti pastatą. Čia buvo pamoka, kurią mes išmokome dabar tas sprendimas jau yra vistik „nuleistas, bet čia vėlgi buvo iš to neturėjimo tokių situacijų“(A4).

Šaltinis: (sudaryta autoriaus, remiantis empirinio tyrimo duomenimis)

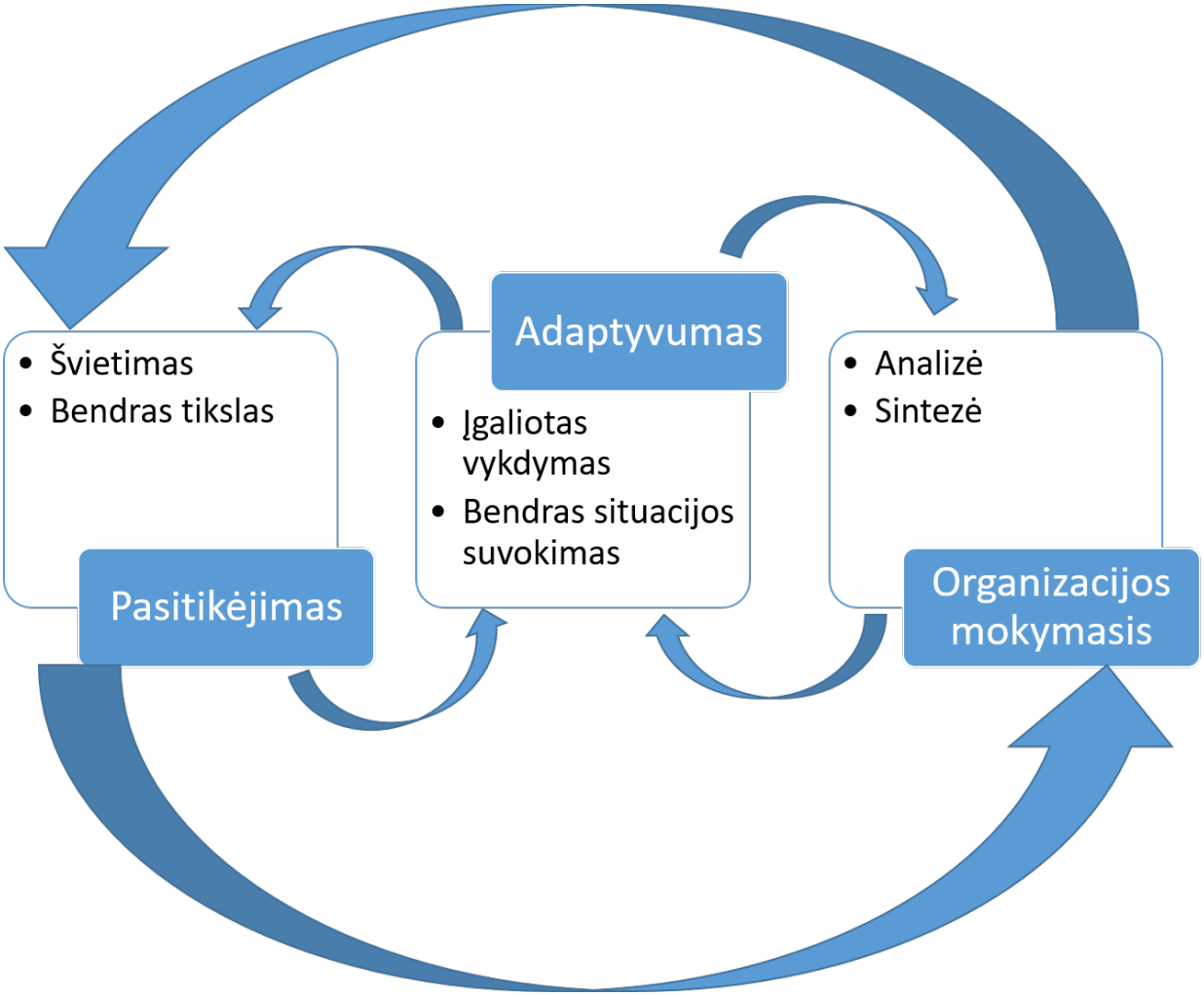
13 lentelėje pateikti empiriniai tyrimo duomenys atskleidžia valstybę kaip adaptyvią ir besimokančią organizaciją, kuri reaguoja į hibridines grėsmes, kaip kompleksines problemas. Nacionalinis krizių valdymo centras, veikiantis pagal Krizių valdymo ir civilinės saugos įstatymą, yra struktūrizuotas taip, kad galėtų veiksmingai stebėti situaciją, vertinti ją ir inicijuoti reikiamas procedūrų bei teisinius pokyčius.

Įvykus hibridiniam išpuoliui, tokiam kaip imigrantų krizė, valstybė reaguoja greitai ir lanksčiai. Pirmiausia, įvykus krizei, buvo svarbu nedelsiant keisti teisės aktus, kad būtų galima veikti efektyviau. Tai parodo, kad valstybė mokosi iš patirties ir prisitaiko prie naujų iššūkių, formaliai įtvirtindama veiksmus, kuriuos jau buvo pradėjusi vykdyti praktikoje. LR Seimo NSGK stengiasi sustiprinti teisinį reguliavimą, siekdami apsaugoti nacionalinį saugumą. Tai atspindi pastangas įvesti

griežtesnius saugumo filtrus ir procedūras, ypač susijusias su investiciniais projektas ir energetikos infrastruktūros saugumu. Tyrimo dalyviai išskiria svarbą reguliarių pratybų ir saugumo kultūros vystymo. Tai padeda visiems susitelkti ir žinoti, kaip reaguoti į krizines situacijas, taip pat įgyti supratimą apie svarbiausias saugumo priemones.

Taip pat pažymėtinas lankstumas valstybės finansų valdymo srityje Tai iliustruoja fizinio barjero įdiegimas, finansinė parama savivaldybėms, parama gyventojams ir kitos reikalingos priemonės, kurių finansavimas buvo užtikrintas keičiant biudžetą ir skirstant finansavimą. Taip pat pastebima valstybės gebėjimas reaguoti į situacijos kintamumą, parengiant ir įgyvendinant skirtingus paramos paketus atsižvelgiant į besikeičiančias aplinkybes. Akcentuojama informacijos rinkimo ir analizės svarba krizių valdyme. Tai leidžia vykdyti sistemingą analizę ir sekti grėsmių tendencijas, kas yra esminis veiksnys veiksmingam reagavimui į hibridines grėsmes.

8 paveikslas *Valstybės atsparumo hibridinėms grėsmėms vertinimo modelis*



Sudaryta autoriaus, remiantis literatūros analize ir empirinio tyrimo duomenimis

7 paveiksle pavaizduotas valstybės atsparumo hibridinėms grėsmėms vertinimo modelis, kuris apima pasitikėjimą, adaptyvumą ir organizacijos mokymąsi, yra subalansuota sistema, kuri leidžia valstybei efektyviai atsakyti į įvairias kompleksines grėsmes ir iššūkius. Šis modelis susideda iš trijų pagrindinių elementų:

1. **Pasitikėjimas**: Šis elementas apima švietimą ir bendrą tikslą. Švietimas ir bendras tikslas sukuria aplinką, kurioje personalas gali augti, tobulėti ir dirbti kaip vientisas kolektyvas. Pasitikėjimas tarp valstybės institucijų, gyventojų ir visuomenės yra esminis veiksnys, užtikrinantis greitą ir efektyvų reagavimą į hibridines grėsmes. „Pagrindinis iššūkis yra dabar, kadangi tai santykinai nauja sąvoka [...] kas yra hibridas ir kaip hibridas veikia, ir

tai dar ne visi sutariame. [...] didžiausias iššūkis – naudoti vieną terminologiją, ją išsigryninti ir apsibrėžti, kas yra hibridinės grėsmės kad visi mes vienodai suvoktumėm jas“ (A3). „Common understanding (liet. Bendras supratimas – autoriaus pastaba) – mums šito trūksta. Mes turime kalbėti vienoda kalba, vienoda terminologija, kad mes suprastumėme. Tada sekantis dalykas, aišku, yra atpažinimas ir dekonstrukcija - informacinių karų, arba jeigu tu matai, kažkoks energetinis šantažas… Ta prasme, ir viešumas - čia labai svarbu ir viešumas yra“ (A1). „Hibridinės grėsmės eina kompleksiškai. Jos neveikia vieną sektorių“ (A3). „Stebėsenos įgalinimas, institucijų atsakomybės turėjimas. Nelaukit, kol situacija bus tokia, kad jūs jos negalėsit suvaldyti ir tada prašysit kažko kitų, kad ateitų į pagalbą, bet būkit atsakingi už tą sritį ir šitoje vietoj veikite kuo greičiau. Prisiimkite atsakomybę. Turėkit įrankius, turėkit kompetencijos ir turėkit pajėgumus“ (A12). „Gal labiau ne veikti ir reaguoti į krizę, bet labiau padėti identifikuoti galimą potencialią riziką, nes kartais žmonės savo darbe susiduria su situacija, kuomet matai, kad įvykis yra netipinis, nestandartinius, tame tarpe, pavyzdžiui, muitinė arba pati mokesčių inspekcija, kai tu turi tam tikrus duomenis, jie tau kelia klausimų, galėtum šiaip nereaguoti, bet jeigu matai bendrą valstybės tikslą, bendrą savo organizacijos tikslą, matyt, gali identifikuoti, kad tai yra nauja rizika, nauja grėsmė, kurią galbūt ir tavo vadovai, ir aukštesni pareigūnai, turėtų įvertinti ir tiesiog praneši per savo kanalus apie galimas rizikas aukščiau ir tie kiti žmonės priima sprendimus, kurie padėtų sistemiškai pasižiūrėti į kylančias rizikas. [...] Matyt, žmonės gali pastebėti tokius dalykus, kurių tu iš anksto negali visų modelių įvertinti, bet žmonės iš apačios tai gali tiesiog identifikuoti, kad tai yra spręstina problema“ (A6). „Mūsų veikimo principas yra toks, kad mes, turint konkrečią situaciją, galime pasitelkti iš bet kokios valstybinės institucijos ekspertų. Tie ekspertai pas mus atvyksta, ir mes sprendžiame vieną ar kitą klausimą ir ekspertai grįžta atgal į savo institucijas, taip neprarasdami kvalifikacijos, įgūdžių, tinklo ekspertų ir pan. [...] mūsų centras toks daugiau yra apjungiantis, koordinuojantis ir tuo pačiu stebintis situaciją ir, reikalui esant, mes aktyvuojam tuos nusistovėjusius ekspertų formatus, kurie yra reikalingi vienai ar kitai situacijai spręsti“ (A12). „labai svarbu, kad tiek kariuomenė, tiek Krašto apsaugos ministerija, dažnai Vidaus reikalų ministeriją arba „kibernetikai“ kitos institucijos, taip pat veiktų, sinchronizuotai“ (A10). „kadangi pastaruoju metu tikrai daug buvo vienas po kito sekančių tokių įvykių, kur reikia tarpinstitucinio bendradarbiavimo, tai sakyčiau, kad ta kultūra yra linkusi augti, bendradarbiavimo tarpusavyje“ (A6).

2. **Adaptyvumas**: Įgaliotas vadovavimas ir bendras situacijos suvokimas yra pagrindiniai adaptyvumo elementai. Įgaliotas vadovavimas leidžia greitai ir veiksmingai priimti sprendimus ir imtis veiksmų, kai susiduriama su naujomis ar nežinomomis situacijomis. Bendras situacijos suvokimas reiškia, kad valstybės vadovai ir institucijos bei kiekvienas darbuotojas yra gebantys suprasti hibridines grėsmes, analizuoti jų poveikį ir numatyti būsimus veiksmus. „pirmas žingsnis yra common understanding (bendras supratimas – aut. Pastaba) - tiek kariuomenė, tiek VRM'as turi pradėti kalbėti viena kalba ir sutarti" (A1). „noriu pabrėžti, kad atsakas į hibridinę grėsmę taip pat turi būti sinchronizuotas su kitom ministerijom, su kitom institucijom" (A10). „kalbėjimas apie hibridą, apie „žalius žmogeliukus" suteikia galimybę sakyti, kad čia yra rusų būdas veikti ir jie tą daro" (A11). „Todėl, kad tu turi, kai pats jau susigaudai struktūroje, tada turi būti trim kryptim darbas: dalinamasi su kolegom, raportuojama vadovybei ir edukuojama visuomenė - tokie trys srautai" (A1). „Pastaruoju metu, kadangi daug tų grėsmių buvo, tai išties kyla daugiau tokių atvejų, kuomet yra tarpinstituciniai pasikalbėjimai ir bandymas išspręsti problemas kartu susėdus" (A6). „Yra numatyta turėti ir planus, ir vykdyti intensyvią sąveiką su valstybės savivaldos institucijomis, karo komendantūromis, turėti bendras pratybas" (A2). „Mūsų veikimo principas yra toks, kad mes, turint konkrečią situaciją, galime pasitelkti iš bet kokios valstybinės institucijos ekspertų. Tie ekspertai pas mus atvyksta, ir mes sprendžiame vieną ar kitą klausimą ir ekspertai grįžta atgal į savo institucijas, taip neprarasdami kvalifikacijos, įgūdžių, tinklo ekspertų ir pan. [...] mūsų centras toks daugiau yra apjungiantis, koordinuojantis ir tuo pačiu stebintis situaciją ir, reikalui esant, mes aktyvuojam tuos nusistovėjusius ekspertų formatus, kurie yra reikalingi vienai ar kitai situacijai spręsti" (A12 „labai svarbu, kad tiek kariuomenė, tiek Krašto apsaugos ministerija, dažnai Vidaus reikalų ministeriją arba „kibernetikai" kitos institucijos, taip pat veiktų, sinchronizuotai" (A10). „Istoriniai pavyzdžiai - turbūt migrantų krizė yra geriausia. Čia daugiausiai koordinavo Vidaus reikalų ministerija – Pasienis" (A10). „įstatymas numato galimybę Vyriausybei paskirti, visų pirma pripažinti, kad reikalinga konkreti operacija vienai ar kitai situacijai spręsti, ir tada Vyriausybės sprendimu yra priimamas sprendimas, kas bus tos operacijos vadovas, ir su šituo sprendimu ateina ir atsakomybė, bet ateina tuo pačiu, ir įgalina tą vadovą priimti nurodomuosius sprendimus, kurie tampa privalomi kitom institucijom" (A12). „migrantų krizė parodė, kad tiek pasieniečiai, tiek muitinė, tiek policija gali dirbti bendrai, bet kartais to koordinavimosi reikia šiek tiek daugiau" (A6). „Covid'o atvejis, kur taip pat vyko tam tikra

koordinacija“ (A10). „kadangi pastaruoju metu tikrai daug buvo vienas po kito sekančių tokių įvykių, kur reikia tarpinstitucinio bendradarbiavimo, tai sakyčiau, kad ta kultūra yra linkusi augti, bendradarbiavimo tarpusavyje“ (A6). „Taip. Nebūtinai tie pareigūnai yra pastovūs. Jie yra numatyti tam tikroms situacijoms. Per migrantų krizę mes ne tik turėjome savo sąveikos pareigūnus, bet ir dalį savo ryšio sistemos“ (A11). „krizių valdymo centro sustiprėjimas ir jų vystymasis tai yra didžiulis žingsnis į priekį, koordinuojant veiksmus tarp institucijų“ (A10). „jeigu tai susiję su kitomis ministerijomis, kas dažnai būna, su Vidaus reikalų, tada koordinuojame per Nacionalinį krizių valdymo centrą. Ten yra ir budėtojai, ten yra atsakingi žmonės, ir ten priimami sprendimai, kaip reaguojame ir kas reaguoja, tai ta koordinacija yra gerai išvystyta“ (A10). „Tai yra standartinės procedūros – yra SITCEN‘as (Situacijų stebėjimo centras – autoriaus pastaba), kuris veikia 24/7 [...], gauna visą informaciją, veikia tarptautiniu ryšiu. Jei partneriai vidury nakties perduoda kažkokią informaciją, kuri yra labai svarbi, tai SITCEN‘as žino ką turi daryti, kam skambinti, pagal procedūras. Tai yra ne tik pradrill‘inta (išbandyta pratybų metu – autoriaus pastaba), bet ir veikia“(A11). „Aš manau jau esame šiek tiek kitoje eroje. Informacijos dalinimasis vyksta tokiu įprastu būdu, kad ten kažkokie raštai keliauja, ar tai ten pažymos, ar dar kažkas. Tai mūsų dabar yra pagrindinis tikslas, kad mes tuos informacinius resursus, juos skaitmenizuotume ir kad tas skaitmenizavimas vyktų natūraliai, realiu laiku, apjungiant informacines sistemas į vieną bendrą duomenų ežerą. Ir iš tų duomenų ežero institucijos ima jiems reikalingą informaciją, tada vertina. Mes esame šitam kelyje, šitoje koncepcijoje ir būtent šitą metodą naudojam“ (A12).

3. **Organizacijos mokymasis**: Analizė ir sintezė yra pagrindiniai organizacijos mokymosi komponentai. Analizė leidžia išnagrinėti praeities patirtį, išsiaiškinti stiprybes ir silpnybes bei daryti išvadas, kaip gerinti atsparumą hibridinėms grėsmėms. Sintezė leidžia apjungti gautus rezultatus ir sukurti strategijas bei veiksmų planus ateities grėsmėms įveikti. „Mūsų centras pradėjo funkcionuoti, pradėjo veikti nuo praeitų metų sausio pirmos dienos, priėmus Krizių valdymo ir civilinės saugos įstatymą. Centras funkcionuoja tokiu principu, kad mes turime tris pagrindinius padalinius: situacijų centrą, analizę ir planavimo biurą. Trys padaliniai fokusuojamės į situacijos stebėjimą, situacijos vertinimą ir tam tikrų rekomendacijų ar teisinių kažkokių permainų inicijavimą, kad būtų galima kitą kartą suvaldyti krizę, geriau“ (A12). „Todėl, kad tu turi, kai pats jau susigaudai struktūroje, tada turi būti trim kryptim darbas: dalinamasi su kolegom, raportuojama vadovybei ir edukuojama visuomenė - tokie trys srautai“ (A1). „Na, sakykime, jeigu mes paimtumėm dabar hibridinę grėsmę, kuri įvyko 2022-

ųjų metų vasarą, su imigrantams, tai iš tiesų buvo kliūčių daug, kurios buvo įveiktos. Kariuomenės pasitelkimas, buvimui pasienyje, kartu su vidaus tarnybos institucijomis. Buvo kliūčių dėl jėgos naudojimo statuto, nes negalėjo naudoti jėgos, negalėjo sulaikyti, negali apžiūrėti mašinų kariuomenė. Tai iš esmės buvo kliūčių daug ne tik kad biurokratinių, bet ir teisinių kliūčių. Tam buvo keisti teisės aktai. Tai buvo padaryta labai greitai, nes grėsmės akivaizdoje reikėjo veikti labai greitai ir visa tai buvo padaroma, bet šitoje vietoj sakyčiau, kad tai buvo teisinės, ne biurokratinės kliūtys“ (A4). „iš vienos ekstremalios situacijos palaipsniui peršokome prie kitos, buvo momentas, kai ir abi žaidėme. Tiek Užsieniečių teisinės padėties įstatymas buvo dažnai keičiamas, ko nebūdavo anksčiau, tiek netgi ir mūsų sienos ir jos apsaugos įstatymas buvo keičiamas pakankamai dažnai. Atsirado tas neįleidimo įteisinimas, nes pačioje pirminėje stadijoje, sakykime, sprendimas, kuriuo mes vadovavomės, buvo tiktai ekstremaliųjų situacijų operacijos vadovo [...] sprendimas. Mes vadovavomės tik tuo sprendimu po to tai buvo įtvirtinta įstatyme“ (A5). „Europos Sąjungos lygiu įtvirtinome migracijos instrumentalizacijos termino naudojimą, ir dabartinės migracijos paketas įtraukia nemažai praktikų, kurios yra paremtos Lietuvos patirtimi dėl grąžinimo, dėl neįleidimo į teritoriją, dėl pagreitintų procedūrų ir kitų procesų“ (A8). „pradėkime nuo to, kad fizinis barjeras buvo įdiegtas už biudžetines lėšas ir buvo netgi priimtas atskiras įstatymas“ (A5). „tų poveikio priemonių, jų buvo kelios. Viena buvo kai prasidėjo Lukašenkos imigrantų demaršas iš Baltarusijos, irgi reikėjo rengti staigų paketą priemonių, kuris buvo ir savivaldybėm parama finansinė, priimti tuos žmones, įrengti, kur jie turi gyventi. Reikėjo pastatyti tvorą, fizinį barjerą. Reikėjo apsaugos kamerų, reikėjo naujų pareigūnų, kurie budi prie sienos. Vienas paramos paketas, kitas paramos paketas, prasidėjo, energetikos krizė rengti reikėjo bent du paramos paketus. Kadangi, matyt, buvo tikėtasi, kad greičiau situacija išsispręs, matėsi, kad daro poveikį ne tik gyventojams, bet ir verslui – reikėjo rengti dar vieną paramos paketą, kuriame buvo jau ir priemonės verslui, tęstiniai reakciniai veiksmai, bet jie buvo nesuplanuoti, o labiau reakcija į krizę, bandant išspręsti situaciją“ (A6). „buvo parengtas ir valstybės biudžeto įstatymo pakeitimas, kas turbūt yra pagrindinis valstybės dokumentas ir jam ir parengti, ir pakeisti reikia sutelkti Seime palaikymą pakankamai didelį, kas yra pakankamai sudėtinga. Tai tiek biudžetas, tiek ir buvo energetikos įstatymų įvairių keitimas tam, kad būtų galima pritaikyti paramos priemones ir kainų reguliavimo, prie iššūkių, kurie nutiko“(A6). „Nežinojo žmonės kur būriuotis, bet ne mes išmokome pamokas, išmokome, kad mums reikia daryti pratybas. Buvo daromos pratybos. Visi žinojo, ką daryti. Visi žinojo modelį. Žinojo

vadovai savo vaidmenį, kaip reikia elgtis, kur rinktis, kam pranešti, kad susirinko. [...] tokia pamoka, kurią taip pat išmokome [...] kad tas saugumas pastato yra svarbus, saugantis nuo tų hibridinių grėsmių“ (A4). „apie informacines ir priešišką informacinę veiklą, tai savo atsakomybės ribose, [...] mes kaupiame savo duomenų bazę. Duomenų bazė yra SKD, ten yra fiksuotas kiekvienas unikalus atvejis yra išsaugoma data, taip pat šaltinis, kita informacija ir remiantis šita statistika darome analizę. Kasmet lyginame tendencijas“(A10).

Modelyje organizacijos mokymosi aspektas yra esminis, nes jis padeda užtikrinti, kad pasiektas įgūdžių ir žinių lygis būtų nuolat tobulinamas ir pritaikomas naujoms grėsmėms. Be to, organizacijos mokymasis yra dinaminis procesas, kuris veda atgal prie personalo švietimo, užtikrinant, kad visi darbuotojai ir piliečiai būtų nuolat mokomi, o institucijos būtų pasiruošusios įveikti bet kokias hibridines grėsmes.

IŠVADOS

1. Remiantis išanalizuota literatūra, hibridinės grėsmės yra skirtingų priemonių kombinacija, naudojama siekiant nedeklaruotų strateginių tikslų, oficialiai to nedeklaruojant, dalyvaujant valstybiniams ir nevalstybiniams veikėjams, naudojant įprastines ir nekonvencines įtakos priemones. Darytina išvada, kad reikia stiprinti sugebėjimą pastebėti ir atpažinti šias grėsmes.
2. Išanalizavus hibridinių grėsmių atvejus, nustatyta, kad poveikis gali būti daromas per skirtingus valstybės galios šaltinius, siekiant destabilizuoti padėtį bei daryti įtaką Lietuvos respublikos konstitucinei santvarkai. Tai daro šias grėsmes kompleksine problema tačiau į jas reaguoja skirtingos valstybės institucijos. Tuo remiantis, galima daryti išvadą, kad valstybės atsparumui reikalingas sisteminis požiūris.
3. Empirinio tyrimo duomenys parodo, kad Vakarų šalyse, įskaitant NATO ir Europos Sąjungos valstybes, trūksta bendro supratimo ir vieningos terminologijos apibrėžiant hibridines grėsmes. Tai yra svarbus iššūkis, kurį reikia spręsti, siekiant užtikrinti vienodą supratimą apie šių grėsmių pobūdį ir iššūkius. Tuo remiantis galima daryti išvadą, kad reikalinga standartizuota terminologija.
4. Hibridinės grėsmės veikia įvairias sritis, neapsiribodamos vienu sektoriumi. Jos apima finansų sistemą, informacinį lauką, diplomatinius santykius ir netgi kinetines operacijas. Tai reikalauja integruoto požiūrio ir įvairių strategijų taikymo, siekiant užtikrinti valstybės saugumą ir stabilumą. Tuo remiantis galima daryti išvadą, kad reikalinga vieninga hibridinių grėsmių identifikavimo mokymo programa.
5. Įgaliotas vykdymas ir gebėjimas prisitaikyti yra esminės organizacijų savybės, kurios leidžia operatyviai reaguoti į nenumatytas ir nestandartines situacijas. Tai apima gebėjimą deleguoti galias ir atsakomybes, suteikti darbuotojams ar komandoms laisvę priimti sprendimus ir veikti, kadangi jie yra labiausiai kompetentingi spręsti tam tikras problemas. Galima daryti išvadą, kad reikalingas organizacijų ir jų lyderių mokymas, skatinant tarpusavio pasitikėjimą ir mokant decentralizuoto vykdymo praktikų.
6. Pasitikėjimas ir bendras tikslas yra esminiai veiksniai, kurie užtikrina sklandų tarpinstitucinį ir tarptautinį bendradarbiavimą. Siekiant efektyvaus bendradarbiavimo, bendras situacijos suvokimas yra būtina sąlyga. Tuo remiantis galima daryti išvadą, kad yra reikalingas valstybės lygmens ryšių tinklas su visiems prieinama duomenų baze.

7. Atlikus empirinį tyrimą, nustatyta, kad Lietuvos Respublikos atsparumas hibridinėms grėsmėms vertintinas teigiamai. Šį atsparumą sustiprino priimtas Krizių valdymo įstatymas bei įsteigtas Nacionalinis krizių valdymo centras. Šios iniciatyvos leido efektyviai organizuoti valstybės atsaką į įvairias krizines situacijas ir hibridines grėsmes, įgalinant tarpinstitucinę sąveiką, koordinavimą bei informacijos dalijimąsi. Krizių valdymo centras, veikiantis pagal įstatymą, tapo struktūra, kuri stebi situaciją, vertina ją, analizuoja ir inicijuoja būtinas procedūras bei teisinius pokyčius. Daroma išvada, kad Lietuva įgyvendina veiksmingą priemonių rinkinį, siekdama užtikrinti valstybės saugumą ir stabilumą, atsakydama į kintančias grėsmes ir iššūkius.

REKOMENDACIJOS

1. Remiantis atliktu empiriniu tyrimu, Europos atsparumo hibridinėms grėsmėms kompetencijos centrui siūloma standartizuoti supratimą ir vieningą terminologiją apibrėžiant hibridines grėsmes. Tai leistų efektyviau identifikuoti šių grėsmių pobūdį ir iššūkius bei parengti tinkamas strategijas joms atremti.
2. Remiantis empiriniais duomenimis ir besimokančios organizacijos modeliu, skirtingų valstybės institucijų tarpusavio sąveika, reaguojant į hibridines grėsmes turėtų būti nuolat tobulinama. Mobilizacijos ir pilietinio pasipriešinimo departamentui prie Lietuvos Respublikos krašto apsaugos ministerijos organizuoti reguliarius valstybės institucijų mokymus pagal standartizuotas mokymo programas ir įgytą praktiką, reguliarių pratybų metu.
3. Skaitmeninės technologijos leidžia efektyviau tvarkyti informaciją apie hibridines grėsmes, ją sisteminti ir analizuoti. Valstybės duomenų agentūrai siūloma nusistatyti tvarkas, kurios įgalintų nuolat tobulinti informacinių sistemų saugumą, plėsti duomenų apsikeitimo galimybes ir skatinti skaitmeninį informacijos valdymą.
4. Reaguojant į hibridines grėsmes, labai svarbu visuomenės gebėjimas jas atpažinti ir suprasti. Nacionaliniam krizių valdymo centrui, Lietuvos šaulių sąjungai ir Mobilizacijos ir pilietinio pasipriešinimo departamentui prie Lietuvos Respublikos krašto apsaugos ministerijos rekomenduojama stiprinti mokymo programas ir informacijos sklaidą visuomenei apie hibridines grėsmes, jų pobūdį ir poveikį. Tai padėtų didinti visuomenės sąmoningumą ir gebėjimą atpažinti bei reaguoti į galimas grėsmes.
5. Bendram situacijos suvokimui ir veikimui bendram labui labai svarbus yra nacionalinis naratyvas ir vieningos valstybės istorijos žinios. Nacionaliniam krizių valdymo centrui, pasitelkiant Lietuvos kariuomenės Strateginės komunikacijos departamento ekspertizę, institucionalizuoti nacionalinio lygmens strateginę komunikaciją ir suformuoti valstybinę kultūros politiką, kuri apimtų nacionalinį naratyvą, ateities tikslus, švietimo gaires ir istorinės atminties politiką. Tai svarbu siekiant kurti vieningą ir stiprų nacionalinį identitetą bei sąmoningumą visuomenėje, kad ši taptų atsparesnė hibridinėms grėsmėms. Nacionalinis naratyvas turėtų atspindėti Lietuvos vertybes, istoriją, kultūrą ir ateities viziją, o švietimo gairės turėtų skatinti kritinį mąstymą, demokratinius principus ir visuomenės atsparumą

propagandai bei dezinformacijai. Be to, reikia užtikrinti, kad istorinės atminties politika būtų grindžiama objektyviais istorijos faktais ir skatintų nacionalinį susitelkimą bei vienybę, o ne padalijimą ir nesantaiką.

LITERATŪROS SĄRAŠAS

Aho, A., Midoes, C., & Šnore, A. (2020). *Hybrid threats in the financial system*.

Allem, T., Longley, J., McMichael, R., & Miron, W. (2023). Canadian Special Operations Forces Theory of Gray Zone Conflict. *Operating on the margins: SOF in the gray zone Special Operations Forces and Great Power Competition* (p. 31–46). CANSOFCOM Education & Research Centre.

Arcobasso, A. (2020). Rethinking political warfare in Italy: a bottom-up approach. *Journal of Financial Crime*, *30*(2), 437–452. https://doi.org/10.1108/JFC-11-2019-0139

Bajarūnas, E., Keršanskas, V. (2018). Hibridinės grėsmės: turinio, keliamų iššūkių ir priemonių įveikti jas analizė. *Strateginė metinė apžvalga*, *16*(1). https://doi.org/https://doi.org/10.47459/lmsa.2018.16.5

Banasik, M. (2017). Challenges and Threats for the International Security as the Consequence of the Russian Federation Hybrid War. *Science & Military*, *1*.

Bankauskaitė, D., Berzins, J., Lawrence, T., Šlekys, D., Swaney, B., & Hammex, T. X. (2020). Baltics Left of Bang: Comprehensive Defense in the Baltic States. *Institute for National Startegic Studies*. https://doi.org/10.1080/03071847.2016.1253367

Berzinš, J. (2023). Latvia From Total Defense to Comprehensive Defense. *PRISM*, *10*(2). Žiūrėta 2024-01-17. Prieiga internetu: https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3323892/latvia-from-total-defense-to-comprehensive-defense/

Cederberg, A., Eronen, P., & Mustonen, J. (2017). *Regional Cooperation to Support National Hybrid Defence Efforts*.

Clarke, R., & Jackson, O. (2019). *Building Resilience: Hybrid's Weakness?*

Coombs, H. (2023). Re-Framing NATO Perspectives of 21st Century Conflict and Special Operations Implications. *Operating on the margins: SOF in the gray zone Special Operations Forces and Great Power Competition* (p. 24–31). Žiūrėta 2024-04-11. Prieiga internetu: https://jsou.edu/Press/PublicationDashboard/228

Cullen, P. (2018). *Hybrid threats as a new „wicked problem" for early warning*.

Čiočys, P., Janukevičius, J., Jasiulionis, E., Kisinas, E., Kopūstas, R., Lapinskas, R., Norgėla, J., Venckus, A., ir Žarys, P. (2008). *Enciklopedinis karybos žodynas*. Generolo Jono Žemaičio Lietuvos karo akademija.

De Coning, C. (2021). *Hybrid CoE Strengthening the resilience and adaptive capacity of societies at risk from hybrid threats Hybrid CoE Working Paper 9*.

Ellis, D. C., & Black, C. N. (2018). Complexity, Organizational Blinders, and the SOCOM Design Way. *Joint Special Operations University Report* (T. 18, Numeris 3). Žiūrėta 2024-04-11. Prieiga internetu: https://jsou.edu/Press/Publications

Falk, B. J. (2020). *Hybrid CoE Strategic citizens: Civil society as a battlespace in the era of hybrid threats Hybrid CoE Strategic Analysis / 25*.

Gaižauskaitė, I., Valavičienė, N. (2016). *Socialinių tyrimų metodai: Kokybinis interviu*. Mykolo Romerio universitetas. Žiūrėta 2024-04-11. Prieiga internetu: https://cris.mruni.eu/server/api/core/bitstreams/6bc9b0c7-425b-4420-a2cd-e6ec2d12736a/content

Gecaitė, E. (2023). *Baltarusijos režimo instrumentalizuotos migracijos poveikis Lietuvai* [Magistro darbas, Vilniaus universitetas]. Žiūrėta 2024-05-03. Prieiga internetu: https://epublications.vu.lt/object/elaba:192830019/

Hennink, M., Hutter, I., & Bailey, A. (2020). *Qualitative research methods*.

Jungwirth, R., Smith, H., Willkomm, E., Savolainen, J., Alonso Villota, M., Lebrun, M., Aho, A., & Giannopoulos, G. (2023). *Hybrid Threats. A Comprehensive Resilience Ecosystem*. https://doi.org/10.2760/867072

Kaneberg, E. (2017). Managing military involvement in emergency preparedness in developed countries. *Journal of Humanitarian Logistics and Supply Chain Management*, *7*(3), 350–374. https://doi.org/10.1108/JHLSCM-04-2017-0014

Kilcullen, D. (2020). *The Dragons and the Snakes. How the Rest Learned to Fight the West*. C. Hurst & Co. (Publishers) Ltd.

Lallerstedt, K. (2021). Rebuilding Total Defense in a Globalized Deregulated Economy The Case of Sweden. *PRISM*, *9*(3), 90–104. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2846418/rebuilding-total-defense-in-a-globalized-deregulated-economy-the-case-of-sweden/

Larsson, G., Alvinius, A., Bakken, B., & Hœrem, T. (2021). Social psychological aspects of inter-organizational collaboration in a total defense context: a literature review. *International Journal of Organizational Analysis*, *31*(3), 693–709. https://doi.org/10.1108/IJOA-02-2021-2626

Lietuvos respublikos Krašto apsaugos ministerija. (2021). *Nacionalinė kibernetinio saugumo būklės ataskaita*. Žiūrėta 2024-04-04. Prieiga internetu: https://kam.lt/wp-content/uploads/2022/08/Nacionaline-kibernetinio-saugumo-ataskaita-2021.pdf

Lietuvos respublikos Krašto apsaugos ministerija. (2022). *Nacionalinė kibernetinio saugumo būklės ataskaita*. Žiūrėta 2024-04-04. Prieiga internetu: https://kam.lt/wp-content/uploads/2023/05/Nacionalinekibernetiniosaugumobuklesataskaita2022.pdf

Limnell, J. (2018). *Countering Hybrid Threats: Role of Private Sector Increasingly Important. Shared Responsibility Needed*.

Mahmood Azad, T., Waqas Haider, M., & Sadiq, M. (2023). Understanding Gray Zone Warfare from Multiple Perspectives. *World Affairs*, *186*(1), 81–104. https://doi.org/https://doi.org/10.1177/00438200221141101

Marsh, C., & Searle, T. (2023). Campaigning in the Gray Zone. *Operating on the margins: SOF in the gray zone Special Operations Forces and Great Power Competition* (p. 1–10). Žiūrėta 2023-12-23. Prieiga internetu: https://jsou.edu/Press/PublicationDashboard/228

McChrystal, S. (2015). *Team of Teams. New rules of engagement for a complex world*.

Morris, L., Mazarr, M., Hornung, J., Pezard, S., Binnendijk, A., & Kepe, M. (2019). *Gaining Competitive Advantage in the Gray Zone Response Options for Coercive Aggression Below the Threshold of Major War*.

National Commission on Terrorist Atacks. (2004). *The 9/ 11 Commission Report*. Žiūrėta 2024-05-13. Prieiga internetu: https://www.govinfo.gov/features/911-commission-report

NATO Special Operations Headquarters. (2020). *Comprehensive Defence Handbook* (T. 1). NATO Special Operations Headquarters. Žiūrėta 2023-11-11. Prieiga internetu: https://www.nshq.nato.int/library?org=nshq

Pathe Duarte, F. (2020). Non-kinetic hybrid threats in Europe – the Portuguese case study (2017-18). *Transforming Government: People, Process and Policy*, *14*(3), 433–451. https://doi.org/10.1108/TG-01-2020-0011

Radzevičiūtė, M. (2023). *Vilniaus Universitetas Filosofijos fakultetas Sociologijos ir socialinio darbo institutas Migracijos krizės valdymo atvejo analizė: nevyriausybinių organizacijų perspektyva*. Žiūrėta 2024-04-02. Prieiga internetu: https://epublications.vu.lt/object/elaba:157854438/

Roberts, J. , Q. (2015). Maskirovka 2.0: Hybrid Threat, Hybrid Response. *JSOU Press Occasional Paper*. Žiūrėta 2024-05-12. Prieiga internetu: https://jsou.edu/Press/Publications

Scharlach, T. (2023). Special Operations Forces Collective Training for the Gray Zone. *Operating on the margins: SOF in the gray zone Special Operations Forces and Great Power Competition* (p. 47–54).

Senge, P. (2006). *The Fifth Discipline. The Art & Practice of the Learning Organization*. Crown Publishing Group.

Shandra, A., & Seely, R. (2019). The Surkov Leaks. The inner workings of Russia's Hybrid wars in Ukraine. *Royal United Services Institute for Defence and Security Studies*. Žiūrėta 2024-01-15. Prieiga internetu: https://rusi.org/explore-our-research/publications/occasional-papers/surkov-leaks-inner-workings-russias-hybrid-war-ukraine

Shultz, R. (2016). Military Innovation in War: It Takes a Learning Organization A Case Study of Task Force 714 in Iraq. *Joint Special Operations University Report* (T. 16, Numeris 6). Žiūrėta 2023-08-17. Prieiga internetu: https://jsou.edu/Press/Publications

Śliwa, Z., Kalinowski, R., & Petraitis, D. (2021). Toward Comprehensive Defense: The Case of the Baltic States since 2014. *Safety & Dafense*, *3*. https://doi.org/10.37105/sd.169

Sorensen, H., & Bach Nyemann, D. (2018). *Going Beyond Resilience A revitalized approach to countering hybrid threats*.

Treverton, G. F., Thvedt, A., Chen, A. R., Lee, K., & Mccue, M. (2018). *Addressing Hybrid Threats*.

Verner, D., Grigas, A., & Peet, F. (2019). *Assessing Energy Dependency in the Age of Hybrid Threats*.

VSD. (2022). *Veiklos ataskaita*. Žiūrėta 2024-04-01. Prieiga internetu: https://www.vsd.lt/wp-content/uploads/2023/04/VSD_Ataskaita_2023_04_19.pdf

VSD, ir AOTD. (2023). *Gresmių nacionaliniam saugumui vertinimas*. Žiūrėta 2024-04-04. Prieiga internetu: https://www.vsd.lt/wp-content/uploads/2023/03/Gresmiu-nacionaliniam-saugumui-vertinimas-2023_LT.pdf

VSD, ir AOTD. (2024). *Gresmių nacionaliniam saugumui vertinimas*. Žiūrėta 2024-04-04. Prieiga internetu: https://www.vsd.lt/wp-content/uploads/2024/03/GR-2024-02-15-LT-1-1.pdf

Zorri, D. (2023). Great Power Competition and the Gray Zone. *Operating on the margins: SOF in the gray zone Special Operations Forces and Great Power Competition* (p. 11–22). Žiūrėta 2024-02-12. Prieiga internetu: https://jsou.edu/Press/PublicationDashboard/228

Žilinskas, R. (2017). Valstybės atsparumas išorinėms hibridinio pobūdžio grėsmėms: Hipotetinis modelis. *Politologija*, *3*(87), 45–87. https://doi.org/10.15388/Polit.2017.3.10856

VALSTYBĖS ATSPARUMO HIBRIDINĖMS GRĖSMĖMS VERTINIMO MODELIS

Karolis JANUŠKA

Magistro baigiamasis darbas

Kokybės vadybos studijų programa

Vilniaus universitetas, Ekonomikos ir verslo administravimo fakultetas

Darbo vadovas – asistentas dr. D. Ruželė

Vilnius, 2024

SANTRAUKA

82 puslapiai, 8 paveikslai, 13 lentelių 48 literatūros šaltiniai.

Pagrindinis šio magistro darbo tikslas – sukurti valstybės atsparumo hibridinėms grėsmėms vertinimo modelį

Darbą sudaro trys dalys: literatūros analizė, tyrimas ir jo rezultatai, pabaigoje pateikiamos išvados ir rekomendacijos.

Literatūros analizėje apžvelgiami skirtingi hibridinių grėsmių pasireiškimo aspektai, atskleidžiamas jų kompleksiškumas. Antroje darbo dalyje apžvelgiami atsparumo hibridinėms grėsmėms atvejai ir sudaromas pradinis valstybės atsparumo hibridinėms grėsmėms modelis, remiantis besimokančios organizacijos konceptu.

Atlikęs literatūros analizę, autorius atliko tyrimą, siekdamas įvertinti Lietuvos Respublikos atsparumą hibridinėms grėsmėms. atliktas kokybinis tyrimas - pusiau struktūruotas interviu.. Remiantis literatūros apžvalga bei antrinių šaltinių analize, buvo suformuotas pradinis konceptualus modelis. Remiantis literatūros apžvalgos metu surinktais duomenimis, sudarytu klausimynu, buvo atliktas kokybinis tyrimas, padėjęs patikrinti pradinį modelį ir tyrimo pabaigoje įvertinti Lietuvos respublikos atsparumą hibridinėms grėsmėms. Tyrimui atlikti pasirinktas abdukcinis metodas, remtasi ontologine, subjektyvistine filosofija, tiriant informantų pateikiamas prielaidas apie hibridines grėsmes Lietuvoje bei jų organizacijose.

Tyrimui atlikti pasirinkta tikslinė, netikimybinė informantų atranka. Remiantis pirmoje darbo dalyje sudarytu institucijų sąrašu, pasirinkti raktinių institucijų atstovai, užimantys pareigas vadovaujančiuose lygmenyse, kurių pareigos yra tiesiogiai susijusios su institucijos strategijos parengimu, įgyvendinimu ir sąveikos su kitomis institucijomis užtikrinimu. Pasirinktų

institucijų sąrašas, kuris sudarytas, remiantis DIMEFIL. Buvo atlikta 12 interviu su vadovais ir pareigas vadovaujančiame lygmenyje užimančiais tarnautojais, turinčiais kompetencijų atsakyti į klausimus apie organizacijos veiklą ir sąveiką su kitomis institucijomis.

Atliktas tyrimas atskleidė, kad reikia stiprinti sugebėjimą pastebėti ir atpažinti hibridines grėsmes. Valstybės atsparumui reikalingas sisteminis požiūris. Geriasniam bendram hibridinių grėsmių suvokimui reikalinga standartizuota terminologija. Siekiant užtikrinti valstybės saugumą ir stabilumą ir integruojant skirtingas institucijas, reikalinga vieninga hibridinių grėsmių identifikavimo mokymo programa. Reikalingas organizacijų ir jų lyderių mokymas, skatinant tarpusavio pasitikėjimą ir mokant decentralizuoto vykdymo praktikų. Siekiant efektyvaus bendradarbiavimo, bendras situacijos suvokimas yra būtina sąlyga todėl yra reikalingas valstybės lygmens ryšių tinklas su visiems prieinama duomenų baze. Lietuva įgyvendina veiksmingą priemonių rinkinį, siekdama užtikrinti valstybės saugumą ir stabilumą, atsakydama į kintančias grėsmes ir iššūkius.

STATES‘S RESILIENCE TO THE HYBRID THREATS EVALUATION MODEL

Karolis JANUŠKA

Master's thesis

Quality management study program

Vilnius University, Faculty of Economics and Business Administration

Supervisor - assistant dr. D. Ruželė

Vilnius, 2024

SUMMARY

82 pages, 8 figures, 13 tables, 48 literature sources.

The main goal of this master's thesis is to create a model for assessing the state's resilience to hybrid threats.

This work consists of three parts; first a literature analysis has been conducted to provide context to this thesis, research and its results are then presented. Finally, the conclusion and subsequent recommendations are provided.

The literature analysis reviews different aspects of the manifestation of hybrid threats and reveals their complexity. The second part of the work reviews cases of resilience to hybrid threats and creates an initial model of the state's resilience to hybrid threats, based on the concept of a learning organization.

After analysing the literature, the author conducted a study to assess the resilience of the Republic of Lithuania to hybrid threats. A qualitative study was conducted - a semi-structured interview. Based on the literature review and the analysis of secondary sources, an initial conceptual model was formed. As a result of the data collected during the literature review and the questionnaire, a qualitative study was conducted, which helped to verify the initial model and at the end of the study to assess the resilience of the Republic of Lithuania to hybrid threats. The abductive method was chosen for the research based on an ontological, subjectivist philosophy while investigating the assumptions made by the informants about hybrid threats in Lithuania and their organizations.

A targeted, non-probable selection of informants was chosen for the research. In accordance the list of institutions compiled in the first part of the work, representatives of key

institutions occupying positions at management levels, whose duties are directly related to the preparation and implementation of the institution's strategy and ensuring interaction with other institutions, were selected. The list of selected institutions is based on DIMEFIL. 12 interviews were conducted with managers and employees at the management level who have competences to answer questions about the organization's activities and interaction with other institutions.

The study revealed that there is a need to strengthen the ability to detect and recognize hybrid threats. State resilience requires a systemic approach. A better common understanding of hybrid threats requires standardized terminology. With the aim to ensure the security and stability of the state and the integration of different institutions, a unified hybrid threat identification training program is needed. Training of organizations and their leaders is required, which will enable the fostering of mutual trust and the development of decentralized enforcement practices and better organizational learning. To achieve effective cooperation, common understanding of the situation is a necessary condition, therefore a state-level communication network with a database accessible to all would support information sharing and better flow of knowledge. Lithuania implements an effective set of measures in order to ensure the security and stability of the state, responding to changing threats and challenges.