MYKOLO ROMERIO UNIVERSITETAS
VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

ROMUALDAS PETKEVIČIUS
Kibernetinio saugumo valdymas

HIBRIDINIŲ GRĖSMIŲ VALSTYBĖS MASTU E. ERDVĖJE VALDYMO MODELIS IR VERTINIMAS

Magistro baigiamasis darbas

Darbo vadovas –
Prof. dr. Tadas Limba

Vilnius, 2023

MYKOLO ROMERIO UNIVERSITETAS
VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

HIBRIDINIŲ GRĖSMIŲ VALSTYBĖS MASTU E. ERDVĖJE VALDYMO MODELIS IR VERTINIMAS

Kibernetinio saugumo valdymo magistro baigiamasis darbas
Studijų programa KSVvmis22-1

Vadovas
Prof. dr. T. Limba

Atliko
KSVvmis22-1 gr. stud.
Plk. R. Petkevičius

Vilnius, 2023

TURINYS

PAVEIKSLAI IR LENTELĖS

ĮVADAS

Temos aktualumas ir ištirtumas. Mokslinės literatūros ir strateginių dokumentų analizė išryškino, kad tiriant hibridinės grėsmės ir jų keliamas saugumo rizikas dažniausiai koncentruojamasi į tradicines ir nekonvencines karinių veiksmų priemones, propagandą diplomatiją, ekonomines spaudimo priemones, energetinį saugumą. Dažnai tiriamos valstybių, teroristinių ar nusikalstamų grupuočių keliamos hibridinės grėsmės. Tarp hibridinių grėsmių dažnai įvardijamos ir kibernetinės atakos.

Keletas hibridinių kibernetinių atakų pavyzdžių galėtų būti tokios atakos kurios trikdo šalies kritinės infrastruktūros veiklą, galimai elektros energijos tiekimo linijas, oro transporto valdymo sistemą ir tuo pačiu metu vykdoma kinetinė svarbių valstybės kritinės infrastruktūros objektų, bei karinių objektų ataka. (Niglia, 2016, Janicke et al., 2022,)

Vystantis technologijoms, ypač proveržio technologijoms, atsiranda vis daugiau galimybių hibridines atakas vykdyti elektroninėje erdvėje. Elektroninė erdvė tampa nauju kritinės infrastruktūros objektu. (Limba et al., 2020,)Staigus naujų technologijų atsiradimas ir didelė jų skvarba taip pat didina riziką atsirasti naujiems pažeidžiamumams. Pavyzdžiui gausus visada prisijungusių įrenginių (IoT) atsiradimas padidina galimų pažeidžiamumų ir kibernetinės atakos vektorių skaičių (Morfino & Eampone, 2020, Bajarunas & Kersanskas, 2018,). Panašiai dirbtinio intelekto plėtra gali sutikti naujas galimybes manipuliuoti socialinius tinklus ir kitas žiniasklaidos priemones ir taip stiprinti hibridinių atakų keliamą efektą.

Tokio tipo hibridinės atakos yra kompleksinės ir sudėtingos valdyti. Valstybė prieš galėdama valdyti tokias hibridines grėsmes turi sukurti atitinkamą teisinę bazę (LRV, 2018) atlikti grėsmių analizę kad identifikuoti galimas hibridines grėsmes. Stiprinti valstybės atsparumą hibridinių grėsmių poveikiui, turėti gynybos planus, investuoti į kritinės infrastruktūros objektų gynybą ir fizinę apsaugą, ruošti personalą ginti ir greitai šalinti atakos poveikius. Stiprinti kibernetinę gynybą valstybės mastu, segmentuoti tinklus, diegti ugniasienes, stiprinti kibernetinių atakų apsaugos sistemas. (LRV, 2018)

Galiausiai, bendradarbiauti su kitomis šalimis ir tarptautinėmis organizacijomis, dalintis informacija ir koordinuoti atsaką į hibridines kibernetines grėsmes. (Bajarunas, 2020)

Atsiranda poreikis sisteminiam požiūriui į hibridinių grėsmių valdymą. Tradiciniai grėsmių valdymo modeliai ne visada gali būti taikomi siekiant sėkmingai nustatyti, valdyti ir atliepti

hibridines grėsmes. Todėl tyrimu siekiama, remiantis teorinėmis įžvalgomis ir jas empiriškai patikrinus pasiųlyti hibridinių grėsmių valstybės mastu elektroninėje erdvėje valdymo ir vertinimo modelį kuris atliepia nūdienos poreikius ir gali būti praktiškai taikomas rengiant atsako į hibridines grėsmes planus.

Temos naujumas. Hibridinių grėsmių perkėlimas į naują elektroninę dimensiją (Limba et al., 2020,), pažangių technologijų pažanga verčia valstybes naujai vertinti technologinę plėtrą, numatyti ir diegti saugiklius, kad išvengti tokių technologijų žalingą panaudojimą. Tai kelia naujus reikalavimus tokioms hibridinėms grėsmėms atpažinti, vertinti ir valdyti. Valstybė turi investuoti į mokslinius tyrimus skatinant naujas technologijas padaryti saugiomis ir atspariomis kibernetinėms atakoms. Atsiranda poreikis naujiems, teisės aktams, standartams ir gairėms, (Europos Sąjunga, 2016) inovatyviems krizių valdymo modeliams.

Mokslinė problema. Mokslo šaltiniuose nepakankamai išanalizuotos hibridinių grėsmių e. erdvėje keliamos grėsmės valstybei. Tuo labiau hibridinių grėsmių e. erdvėje efektyviam valdymui valstybės mastu skiriama dar mažiau dėmesio. Naujų, proveržio technologijų, plėtra elektroninėje erdvėja gali tik dar labiau komplikuoti padėti. Todėl efektyvaus hibridinių grėsmių elektroninėje erdvėje valdymo modelis tampa neišvengiama būtinybe siekiant savalaikiai reaguoti ir koordinuotai atremti valstybei kylančias kibernetines grėsmes.

Tyrimo objektas: Valstybei elektroninėje erdvėje kylančių hibridinių grėsmių valdymas ir vertinimas.

Tyrimo tikslas: Išanalizavus valstybei elektroninėje erdvėje kylančias kibernetines grėsmes ir atlikus jų keliamo poveikio analizę, taip pat įvertinus valstybių parengtį nustatyti, valdyti ir atremti elektroninėje erdvėje kylančias hibridines grėsmes, pasiūlyti hibridinių grėsmių valstybės mastu elektroninėje erdvėje valdymo modelį ir vertinimą.

Uždaviniai:

- išanalizuoti valstybės mastu elektroninėje erdvėje kylančias hibridines grėsmes jų poveikį nacionaliniam saugumui ir ateities tendencijas;
- išnagrinėti galimus atsako į hibridinių grėsmių keliams krizes teoriniu valdymo modelius;
- išanalizuoti Hibridinių grėsmių e. erdvėje valdymo modelį
- sukurti hibridinių grėsmių valstybės mastu elektroninėje valdymo modelį ir atlikti vertinimą.

Tyrimo organizavimo metodika. Magistro baigiamajame darbe buvo atlikta mokslinė literatūros ir strateginių dokumentų hibridinių giesmių keliamų iššūkių valstybei ir jų valdymo tematema kokybinio turinio analizė ir padaryti apibendrinimai. Teorijai empiriškai patikrinti, taikant kiekybinio ir kokybinio tyrimo strategijas buvo buvo atlikti vieno atvejo studija ir adaptuotu DELFI metodu įgalinta ekspertų apklausa. Rezultatai buvo apibendrinti ir iškelta hipotezė. Remiantis teorine ir empirine dalimis buvo sudarytas hibridinių grėsmių e. erdvėje valstybės mastu valdymo modelis.

Darbo struktūra. Darbą sudarys 4 dalys (žr. 1 pav.)

1 dalis: nagrinėjamos valstybės mastu elektroninėje erdvėje kylančios hibridinės grėsmės jų raidos analizė, keliamas poveikis nacionaliniam saugumui. Įvertinamos naujos, proveržio technologijų pasekoje atsirandančios, hibridinės grėsmės. Analizuojami galimi hibridinių grėsmių atpažinimo ir valdymo metodai. Įvertinamas tarptautinių organizacijų vaidmuo valdant hibridines grėsmes.

2 dalis: empirinis tyrimas. Atliekant kokybinę vieno atvejo studiją tiriama Suomijos geroji patirtis identifikuojant, pasiruošiant ir valdant valstybės mastu kylančias hibridines grėsmės. Toliau, naudojant kombinuoto tyrimo strategiją atliekama ekspertų apklausa. Apklausa įgalinta adaptuotu DELFI metodu, per dvi iteracijas. Naudoti instrumentai:

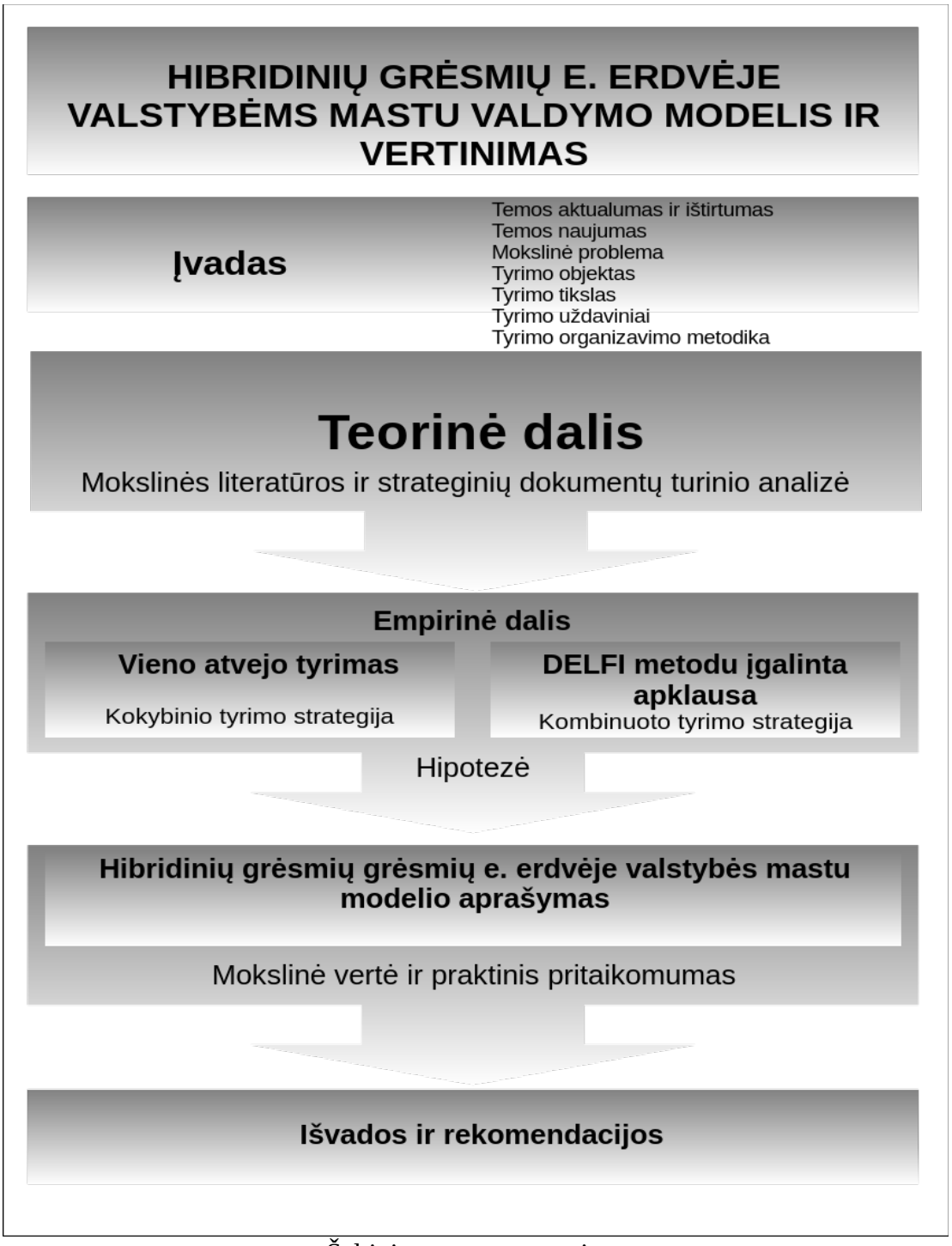
- Pirma iteracija - anketa;
- Antra iteracija - minčių žemėlapis.

Empirinio tyrimo rezultatai apibendrinti ir iškeliama hipotezė kurios validumas tikrinamas konstruojant hibridinių grėsmių e. erdvėje valstybės mastu grėsmių valdymo modelį ir vertinimą.

3 dalis: remiantis teorine analize ir kombinuoto tyrimo rezultatais, siūlomas hibridinių grėsmių valstybės mastu elektroninėje erdvėje valdymo modelis ir vertinimas.

4 dalis: išvados ir rekomendacijos.

Darbo praktinis reikšmingumas. Magistrinio darbo tyrimo rezultatai gali būti pritaikyti siekiant tobulinti Lietuvos pasirengimą laiku reaguojant ir sėkmingai valdant elektroninėje erdvėje kylančias hibridines grėsmes. Praktinis pritaikomumas gali būti siejamas su siūlomo hibridinių grėsmių elektroninėje erdvėje valdymo modeliu ir vertinimo pritaikymo lankstumu įskaitant galimybę pritaikyti atskiriems valstybės veiklos sektoriams. Taip pat ekspertinės apklausos rezultatai gali būti pritaikyti tobulinant krizių valdymą valstybės mastu.



Šaltinis: parengta autoriaus

1 pav. Magistro baigiamojo darbo struktūros loginė schema

1. HIBRIDINIŲ GRĖSMIŲ TEORIJA

1.1 Hibridinių grėsmių atsiradimas ir evoliucija

Hibridinės grėsmės vis labiau vyrauja pasaulinėje saugumo srityje. Šis terminas reiškia įvairių, įprastinių ir netradicinių grėsmių derinį, kuris dažniausiai yra integruotas ir pasireiškia koordinuotai. Šios grėsmės gali kilti iš valstybinių ir nevalstybinių veikėjų (The European Centre of Excellence for Countering Hybrid Threats, 2022, Smith et al., 2021,) ir gali būti nukreiptos pasiekti įvairius politinius, karinius, ekonominius ir visuomeninius tikslus. Hibridinis šių grėsmių pobūdis apsunkina tokių grėsmių identifikavimą, sekimą ir atsaką. Tai kelia didelių iššūkių vyriausybėms ir organizacijoms visame pasaulyje. (Carlson, 2019, 60-84, Europos Sąjunga, 2016, Ruhle & Roberts, 2021, Simon, 2017, 23-26)

Hibridinės grėsmės gali būti įvairių formų, įskaitant kibernetines atakas, dezinformacijos kampanijas, terorizmą, ekonominę prievartą ir politinį perversmą. Pavyzdžiui, valstybės veikėjas gali panaudoti kibernetinių atakų ir dezinformacijos kampanijų derinį, kad sužlugdytų rinkimus kitoje šalyje, o nevalstybinis veikėjas tam tikram tikslui pasiekti gali panaudoti terorizmo ir ekonominės prievartos derinį.

Hibridinių grėsmių augimą paskatino daugybė veiksnių, įskaitant technologijų pažangą, pasaulinį tarpusavio ryšį ir nevalstybinių veikėjų gausėjimą. Šios grėsmės dažnai yra skirtos išnaudoti visuomenės, vyriausybių ir organizacijų pažeidžiamumą, įskaitant dalijimosi informacija spragas, silpną kibernetinę gynybą ir koordinavimo tarp įvairių veikėjų trūkumą.

Hibridinės grėsmės yra sudėtingas ir besivystantis reiškinys, keliantis didelių iššūkių pasauliniam saugumui. Todėl labai svarbu, kad viso pasaulio vyriausybės ir organizacijos imtųsi veiksmų, siekdamos geriau suprasti šias grėsmes ir jas atremti, kad užtikrintų savo piliečių saugumą ir gerovę bei jų interesus.

2014 m. Rusijos Federacijos įvykdyta Krymo aneksija gali būti laikoma hibridinio karo pradžia – karo forma, derinanti konvencines ir nekonvencines taktikas siekiant politinių tikslų. Aneksija pasižymėjo karinės jėgos panaudojimu, dezinformacijos kampanijomis ir kitomis nekarinėmis priemonėmis siekiant destabilizuoti regioną ir susilpninti Ukrainos vyriausybę. Rusijos Federacija neigė savo dalyvavimą aneksijoje, tačiau hibridinės taktikos taikymas buvo akivaizdus operacijos vykdymo būdu.

Krymo aneksija ir kiti panašūs nekonvencinio konflikto pavyzdziai parodė hibridinio karo veiksmingumą siekiant politinių tikslų, tuo pačiu sumažinant eskalavimo riziką. Nekarinių priemonių, tokių kaip kibernetinės atakos ir propaganda, naudojimas gali sukelti painiavą ir pasėti nesantaiką tikslinėje populiacijoje, susilpnindamas vyriausybės gebėjimą priešintis. Karinės jėgos panaudojimas gali apsiriboti konkretiems taikiniams ar tikslams, išvengiant plataus masto konflikto su kitomis šalimis. (Bachmann, & Gunneriusson, 2015, SØRENSEN & NYEMANN, 2018)

Po Krymo aneksijos hibridinio karo naudojimas tapo vis dažnesnis, o šalys ir nevalstybiniai veikėjai savo tikslams pasiekti taiko taktikų derinį. Tai sukėlė didelį iššūkį vyriausybėms ir organizacijoms visame pasaulyje, nes dažnai sunku aptikti ir atremti šią taktiką. (DeBenedictis, 2021, 27-48) (Hill, n.d., 321-342, Leonhard, n.d., 77-108)

Tačiau Ukrainai priklausančio Krymo pusiasalio aneksija nebuvo pirmas kartas kai buvo naudojami netradiciniai konflikto pradžios, eskalavimo ir vykdymo metodai. Stuxnet 2010 - kompiuterinis kirminas, nukreiptas į Irano branduolinę programą, sukėlė centrifugų veikimo sutrikimus. Buvo plačiai manoma, kad tai buvo bendros JAV ir Izraelio kibernetinės operacijos rezultatas, ir tai pažymėjo reikšmingą kibernetinių atakų kaip karo ginklo naudojimo eskalaciją. (Sanger, 2012)

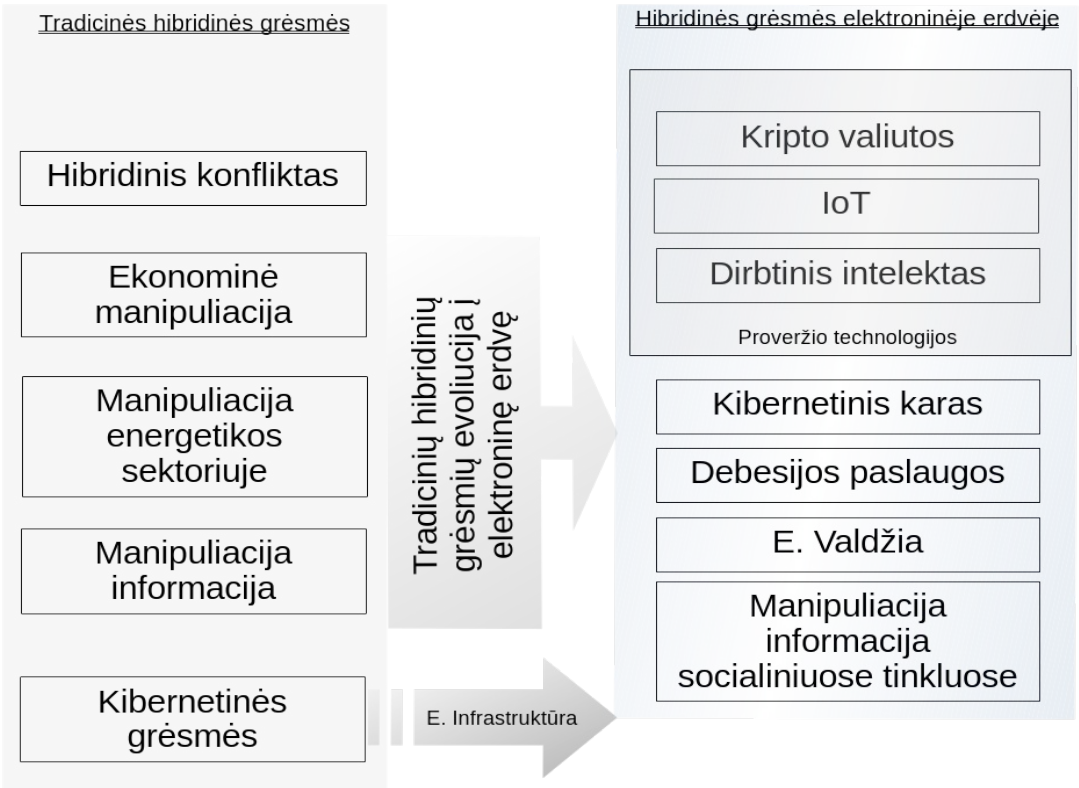
Operacija „Orchard“ (2007 m.) buvo Izraelio ataka prieš Sirijos branduolinį reaktorių, kuris, kaip manoma, buvo statomas. Ataką lydėjo dezinformacijos kampanija, apimanti melagingus pranešimus apie susišaudymą ir Sirijos oro gynybos atsaką. (Gross, 2018)

Rusijos ir Gruzijos karas (2008 m.). Karo metu Rusijos karinės pajėgos savo tikslams pasiekti naudojo įprastines karines taktikas ir kibernetines atakas. Rusijos kibernetinės atakos buvo nukreiptos į Gruzijos vyriausybės svetaines, finansines institucijas ir žiniasklaidos priemones, o Rusijos kariai užėmė Gruzijos teritoriją. (Bumbarner, n.d., 89-114)

Grėsmės, daugiausiai geopolitinės, energetinių resursų gavybos, tranzito ir prekybos sistemoje taip pat dažnai klasifikuojamos kaip hibridinės grėsmės. Tokios tarptautinės organizacijos kaip NATO ir Europos sąjunga yra parengusios eilę dokumentų kuriuose pateikia hibridinių grėsmių klasifikaciją. (Europos Sąjunga, 2016) (NATO, 2017, all, Gudmundsson, n.d., #36-44)

Galiausiai kibernetinės atakos, nukreiptos daryti žalingą poveikį valstybės kritinei infrastruktūrai tokiai kaip elektros energijos perdavimo linijos, transporto valdymo sistema, energetinio išteklių perdirbimo ar saugojimo insfrastruktūra yra priskiriamos prie hibridinių grėsmių. (European Union Agency for Cybersecurity, 2020, Dupuy, 2021) Tokios kibernetinės atakos nukreiptos prieš valstybės kritinius resursus gali būti kombinuojamos su kintetinėmis atakomis darant fizinę žalą kritinės infrastruktūros objektas ar karinei infrastruktūrai.

Hibridinių grėsmių charakteris keičiasi. Nuo hibridinių grėsmių kurios įgalino netradicinius konflikto vykdymo metodus, geopolitines manipuliacijas energetikos sektoriuje ir visą eilę iššūkių kibernetiniam saugumui, dabar vis daugiau kibernetinių grėsmių keliasi į naują, elektroninę, erdvę. Elektroninėje erdvėje hibridinės grėsmės turi vis labiau juntamą poveikį nacionaliniam saugumui. Tokių hibridinių grėsmių valdymui reikalingi nauji jų valdymo ir atliepimo metodai. Kibernetinių grėsmių evoliuciją galima atvaizduoti sękančiai.



Šaltinis: parengta autoriaus

2 pav. Hibridinių grėsmių evoliucija

Apibendrintai galima teigti, kad hibridinės grėsmės yra įvairių, įprastinių ir netradicinių grėsmių derinys, kuris dažniausiai yra integruotas ir pasireiškia koordinuotai. Tokios grėsmės gali būti nukreiptos įvairius politinius, karinius, ekonominius ir visuomeninius tikslus ir gali kilti iš valstybinių ir nevalstybinių veikėjų. Šių grėsmių pobūdis apsunkina jų identifikavimą, sekimą ir atsaką, ir tai kelia didelių iššūkių vyriausybėms ir organizacijoms visame pasaulyje.

Hibridinės grėsmės yra sudėtingas ir besivystantis reiškinys, kuris kelia didelių iššūkių pasauliniam saugumui. Todėl labai svarbu, kad viso pasaulio vyriausybės ir organizacijos imtųsi veiksmų, siekdamos geriau suprasti šias grėsmes ir jas atremti, kad užtikrintų savo piliečių saugumą ir gerovę bei jų interesus.

1.2 Hibridinių grėsmių evoliucija elektroninėje erdvėje

Sparčiau plečiantis elektroninės infrastruktūros sklaidai vis daugiau hibridinių grėsmių ir jas įgalinančių negatyvaus poveikio priemonių valstybei persikelia į elektroninę erdvę. Elektroninės erdvės įgimta charakteristika - visuotinis apjungimas ir visuotinė skvarba, sudaro sąlygas vykdyti hibridinio tipo kibernetines atakas kuris turi tiesioginį ir išvestinį poveikį keletai valstybės kritinės infrastruktūros elementų.(Weaver, n.d., 13-19) Elektroninė infrastruktūra pati tampa atskira valstybės kritinės infrastruktūros dalimi. (Limba et al., 2020, 138-158)

Naujų, proveržio technologijų, plėtra taip pat įgalina hibridinių grėsmių propagavimą elektroninėje erdvėje. Dirbtinis intelektas ar jo pagrindų grindžiamos naujos technologijos gali būti išnaudojamos kuriant naujus kibernetinių atakų vektorius. Dirbtinio intelekto pagalba galima manipuliuoti socialiniuose tinkluose ir žiniasklaidoje skleidžiama informacija. Dirbtinio intelekto pagrindu sukurti įrankiai gali būti naudojami žvalgybos informacijos rinkimui ir apdorojimui.

Tuo pačiu naujų technologijų plėtra sudaro prielaidas atsirasti pažeidžiamumas, kuriuo gali išnaudoti priešiškai nusiteikę veikėjai. Didelė visada prisijungusių įrenginių sklaida, Internet of Things (IoT) ženkliai padidino kibernetinių atakų įeigos taškų ir vektorių skaičių. Ypač didelį pavojų kelia visada prijungti įrenginiai kurių paskirtis yra kritinės infrastruktūros objektų operacinių procesų valdymas. Tokių įrenginių pažeidžiamumas gali turėti ypač neigiamas pasekmes (Vailshery, 2022).

Kriptovaliutos, nors tiesiogiai negalėtų būti vadinamos hibridine grėsme, gali būti naudojamas kaip įrankis hibridinėms grėsmėms įgalinti. (Demaertzis & Wolff, n.d., Limba et al., 2020,)

Debesijos infrastruktūros ir joje teikiamų paslaugų plėtra tap pat didina hibridinių atakų tikimybę. Išnaudojant debesijos paslaugų infrastruktūra piktavaliai gali gauti papildomą prieigą prie valstybės kritinės infrastruktūros valdymo elementų, vidinių tinklų, valstybės teikiamų e. valdžios paslaugų, jautrių valstybės ar jos piliečių duomenų. Debesijos infrastruktūra gali buti išnaudojma vykdtyi plataus masto kibernetines atakas.

E. valdžia reiškia elektroninių priemonių naudojimą, siekiant palengvinti ir pagerinti valdžios paslaugų ir informacijos teikimą piliečiams, įmonėms ir kitoms suinteresuotoms šalims. E. valdžia gali apimti įvairią veiklą, pavyzdžiui, registraciją internetu, mokesčių ir rinkliavų mokėjimą internetu, prieigą prie vyriausybės informacijos ir paslaugų bei elektroninį balsavimą.

Hibridinės grėsmės gali kelti didelę riziką e. valdžios sistemoms, nes gali sutrikdyti vyriausybės paslaugų teikimą, pažeisti jautrios informacijos konfidencialumą ir pakirsti piliečių pasitikėjimą valdžios sistemomis. Norint apsisaugoti nuo hibridinių grėsmių, svarbu, kad e. vadžios sistemos įdiegtų patikimas saugumo priemones, tokias kaip dvigubas autentifikavimas, šifravimas ir reguliarūs saugos atnaujinimai. Taip pat svarbu, kad vyriausybės mokytų piliečius ir įmones apie hibridinių grėsmių riziką ir apie tai, kaip nuo jų apsisaugoti.

Galiausiai nuo 2014 vykstantis karinis konfliktas Ukrainoje pademonstravo kad tradicinis karinis konfliktas taip pat keliasi į elektroninę erdvę (Warren et al., 2023,). Rusijos kibernetinis karas Ukrainoje reiškia daugybę kibernetinių atakų, kurias Rusijos valstybės remiami veikėjai įvykdė prieš Ukrainos taikinius, įskaitant vyriausybės institucijas, kritinę infrastruktūrą ir žiniasklaidą. Išpuoliai prasidėjo 2014 metais ir nuo to laiko sustiprėjo, siekiant destabilizuoti Ukrainos vyriausybę, remti prorusiškus separatistus ir pasėti dezinformaciją bei sumaištį tarp Ukrainos gyventojų. Tarp reikšmingiausių išpuolių yra 2015 m. elektros energijos tiekimo nutraukimas, kuris paveikė didelę Ukrainos dalį, ir 2017 m. „NotPetya“ išpirkos reikalaujančios programinės įrangos ataka, padariusi didelę žalą Ukrainos verslui ir valdžios institucijoms. Šios kibernetinės atakos yra platesnio Rusijos agresijos prieš Ukrainą modelio dalis ir prisidėjo prie besitęsiančio konflikto regione (Lohmann & Butrimas, 2022,).

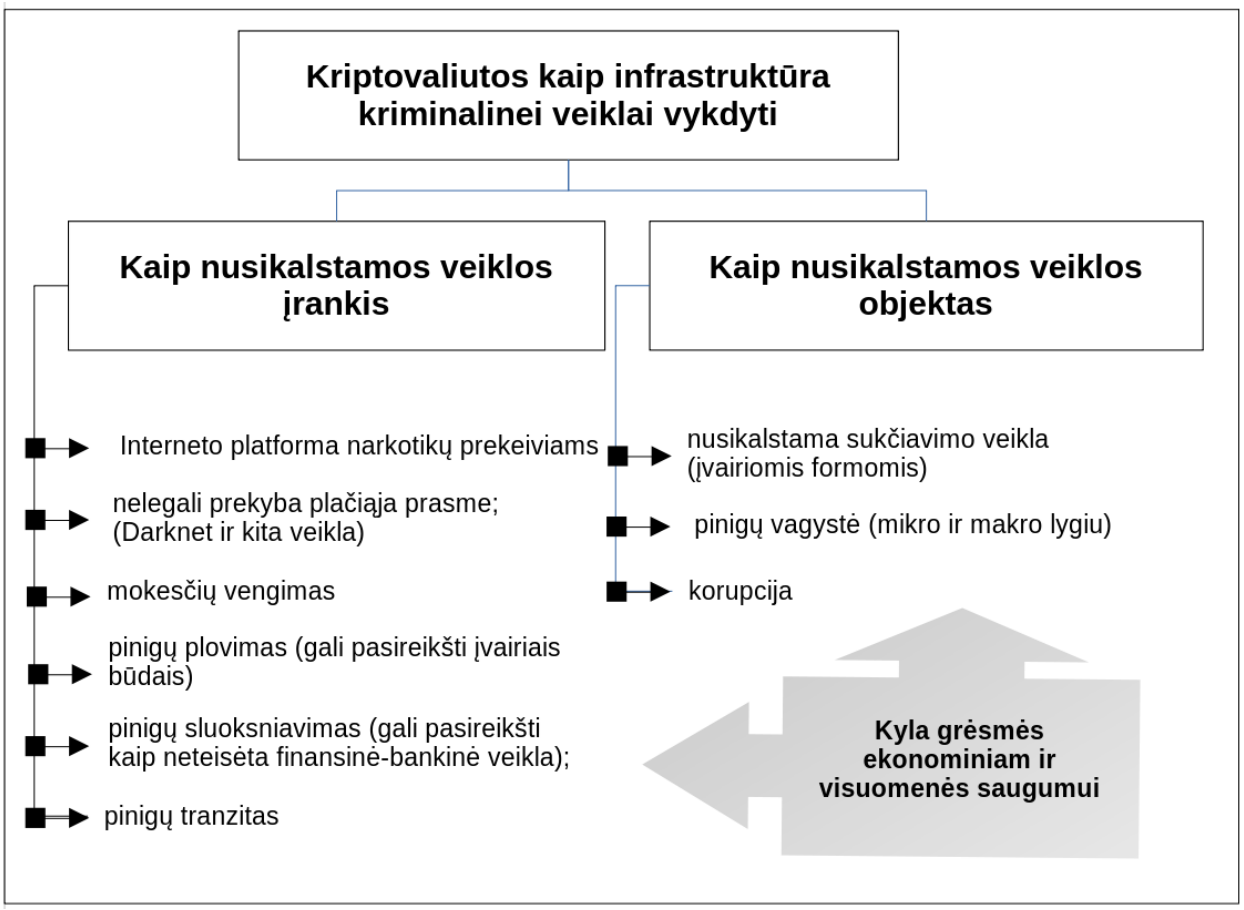
Apibendrinat galima teigti, kad elektroninės infrastruktūros plėtrą sudaro ženklią įtaką hibridinėms grėsmėms, kurios gali turėti neigiamą poveikį valstybės kritinės infrastruktūros

elementams. Naujų technologijų, pvz., dirbtinio intelekto, plėtra taip pat gali padidinti hibridinių grėsmių pavojų. Be to, kriptovaliutos ir debesų infrastruktūra taip pat gali būti naudojamos kaip įrankiai hibridinių grėsmių įgalinimui. Valstybės elektroninės valdžios plėtra gali būti naudojama gerinant valdžios paslaugų ir informacijos teikimą, tačiau taip pat gali padidinti pavojų dėl hibridinių grėsmių. Hibridinės grėsmės gali pasireikšti įvairiais būdais, įskaitant kibernetinėmis atakomis, manipuliacijomis socialiniais tinklais ir žiniasklaida, kriptovaliutų naudojimu ir debesijų infrastruktūros išnaudojimu.

1.3 Hibridinių grėsmių poveikis nacionaliniam saugumui

Apsiginti nuo hibridinių grėsmių yra pakankamai sunku kadagi hibridines atakas gali vykdyti tiek veikejais kurie savęs neriša su atskira valstybe, pavyzdžiu teroristinės grupuotės, kriminalinės organizacijos tačiau tokias hibridines atakas gali vykdyti ir viena šalis prieš kitą (Hickton, 2023).

Tuo pačiu hibridinės atakos gali būti vykdomos įvairiausiomis priemonėmis, ir naudojant skirtingus atakų vektorius. Vienas iš naujų pavyzdžių yra kriptovaliutų keliamos grėsmės valstybės ir piliečių saugumui.



Šaltinis: (Limba et al., 2020) adaptuota autoriaus

3 pav. Kriptovaliutų keliamos grėsmės nac. saugumui

Tokios hibridinių atakų charakteristikos skatina valstybes ieškoti naujų priemonių ir metodų identifikuoti, valdyti ir atliepti pastoviai besikeičiančias hibridines grėsmes.

Jeigu hibridinė grėsmės nėra liaku identifikuojamos ir jų poveikis nėra valdomas tiek valsybei tiek visuomenei gręsia eilė neigiamų pasekmių. Sutrikdžius kritinės infrastruktūros, tokios kaip elektros tiekimo linijas, vandens tiekimo ar valymo įrenginių veiklą, paralyžavus transporto sistemos veiklą gali sukelti rimtų pasekmių visuotinei tvarkai ir netoleruojamų nepatogumų šalies gyventojams. (Soldatos et al., 2020, Bogdanoski, 2022).

Sėkmingos hibridinės atakos nukreiptos prieš valstybės kritinę infrastruktūra gali sugriauti pasitikėjimą valdžios institucijomis ir neigiamai įtakoti valstybės valdyma, reformų ir pokyčių politikos vykdymą.

Detali hibridinių grėsmių poveikio matrica valstybei pateikiama ES Hibridinių grėsmių kompetencijų centro parengtoje publikacijoje (European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) & Joint Research Centre (JRC), 2020). Koncepcinis hibridinių grėsmių supratimo modelis nustato veikėjus, sritį, įrankius ir grėsmės vystymosi etapus besikeičiančioje geopolitinėje aplinkoje. Pabrėžiama, kaip svarbu suprasti veikėjų motyvus, doktrinas ir tikslus bei nustatyti priemones, kurios įgalina valstybinius ir nevalstybinius veikėjus kurti hibridines grėsmes.

Galiausiai hibridinės grėsmės kelia didelį visuomenės susirūpinimą. Yra keletas pagrindinių susirūpinimą keliančių sričių, susijusių su hibridinėmis grėsmėmis.

Hibridinės grėsmės gali būti naudojamos siekiant pažeisti asmeninių ir finansinių duomenų konfidencialumą, o tai gali sukelti tapatybės vagystę, finansinį sukčiavimą ir kitas rimtas pasekmes asmenims. Tai gali sukelti didelį nerimą ir stresą žmonėms, kurie nerimauja dėl savo asmeninio ir finansinio saugumo (Romansky & Noninska, 2020).

Hibridinės grėsmės taip pat gali kelti didelį pavojų nacionaliniam saugumui, nes jos gali būti naudojamos siekiant sutrikdyti ypatingos svarbos infrastruktūrą, pavogti slaptą vyriausybės informaciją ir pakirsti piliečių pasitikėjimą valdžios sistemomis. Tai gali sukelti visuomenės susirūpinimą dėl vyriausybių gebėjimo apsaugoti savo piliečius ir išlaikyti savo visuomenės stabilumą. (The European Centre of Excellence for Countering Hybrid Threats & NATO Strategic Communications Centre of Excellence, 2022,)

Hibridinės grėsmės gali būti naudojamos norint sutrikdyti svarbių paslaugų, pvz., sveikatos priežiūros, švietimo ir finansinių paslaugų, prieinamumą. Tai gali sukelti didelių nepatogumų ir sunkumų žmonėms, kurie naudojasi šiomis paslaugomis, taip pat gali turėti rimtų pasekmių įmonėms, kurios priklauso nuo šių paslaugų (Skarmeta & Bernabe, 2019).

Apskritai visuomenė yra labai susirūpinusi dėl hibridinių grėsmių ir galimų pasekmių asmenims, įmonėms ir vyriausybėms. Svarbu, kad vyriausybės ir organizacijos imtųsi priemonių apsisaugoti nuo tokių grėsmių ir šviestų visuomenę, apie galimas grėsmes ir apsaugos priemones.

Apibendrinat galima teigti, kad valstybėms ir kitoms organizacijoms reikia ieškoti naujų priemonių ir metodų, kaip identifikuoti, valdyti ir atliepti hibridines grėsmes. Sėkmingos hibridinės atakos gali sugriauti pasitikėjimą valdžios institucijomis ir neigiamai įtakoti valstybės valdymą. Todėl yra svarbu suprasti, kaip veikia hibridinės grėsmės, ir kurti veiksmingas priemones, kurios padėtų apsaugoti valstybę nuo jų poveikio.

1.4 Hibridinių grėsmių valdymas

Krizių valdymas – tai procedūrų ir metodų rinkinys, kurį organizacijos naudoja krizių prevencijai, joms pasiruošimui, atsakui į jas ir atsistatymui po jų. Veiksmingam krizių valdymui reikalingas visapusiškas požiūris, apimantis rizikos vertinimą, komunikaciją, koordinavimą ir sprendimų priėmimą. Yra keletas dažniausiai naudojamų krizių valdymo modelių.

- Keturių pakopų krizių valdymo modelis

  Keturių pakopų krizių valdymo modelis, kurį sukūrė Ianas Mitrofas, susideda iš keturių etapų: signalo aptikimo, prevencijos ir pasiruošimo, žalos kontrolės ir mokymosi po krizės. Modelyje pabrėžiama ankstyvo signalų, pavyzdžiui, įspėjamųjų ženklų, aptikimo svarba, siekiant išvengti krizių arba sumažinti jų poveikį. Taip pat pabrėžiamas veiksmingo bendravimo, rizikos vertinimo ir mokymosi iš praeities krizių poreikis. Šis modelis plačiai naudojamas verslo ir vyriausybinėse organizacijose.

- Trifazis krizių valdymo modelis

  Trijų fazių krizių valdymo modelis, sukurtas W. Timothy Coombso, susideda iš fazių prieš krizę, reagavimą į krizę ir pokrizinį etapą. Modelyje akcentuojamas pasiruošimo ir planavimo poreikis prieš įvykstant krizei, efektyvi komunikacija krizės metu, mokymasis ir tobulėjimas po krizės. Modelis taip pat pabrėžia reputacijos valdymo ir suinteresuotųjų šalių įtraukimo svarbą. Šis modelis plačiai naudojamas viešųjų ryšių ir komunikacijos srityse.

- Šešių žingsnių krizių valdymo modelis

  Šešių žingsnių krizių valdymo modelis, kurį sukūrė Gerard Seijts ir Dan Crim, susideda iš šešių žingsnių: problemos identifikavimo, krizių įvertinimo, strategijos kūrimo, įgyvendinimo, vertinimo ir mokymosi. Modelis pabrėžia sistemingo ir iniciatyvaus požiūrio į krizių valdymą, įskaitant rizikos vertinimą, sprendimų priėmimą ir nuolatinį tobulėjimą, poreikį. Taip pat pabrėžiama lyderystės, komunikacijos ir suinteresuotųjų šalių įtraukimo svarba. Šis modelis plačiai naudojamas vadybos ir lyderystės srityse.

- Integruotas krizių valdymo modelis

  Integruoto krizių valdymo modelis, sukurtas Martino Finkenstädto ir kolegų, susideda iš trijų fazių: fazės prieš krizę, krizės fazės ir pokrizinės fazės. Kiekvienas etapas apima

strateginės, operatyvinės ir taktinės veiklos derinį, įskaitant rizikos vertinimą, komunikaciją, koordinavimą, sprendimų priėmimą ir mokymąsi. Modelyje pabrėžiamas koordinuoto ir integruoto požiūrio į krizių valdymą, įtraukiant daug suinteresuotųjų šalių ir funkcijų, poreikis. Šis modelis plačiai naudojamas ekstremalių situacijų valdymo ir reagavimo į nelaimes srityse.

Pritaikant krizių valdymo modelius taikoma keltą analitinių metodikų iš kurių dažniausiai taikomos sękančios.

- Rizikos vertinimas: tai apima galimų hibridinių grėsmių nustatymą ir analizę bei jų tikimybės ir galimo poveikio vertinimą. Tai galima padaryti naudojant tokias priemones kaip pažeidžiamumo ir rizikos vertinimai, kurie gali padėti nustatyti išteklių ir pastangų prioritetus.
- Situacijos analizė. Tai apima konteksto, kuriame egzistuoja hibridinė grėsmė, supratimą, įskaitant potencialių veikėjų motyvaciją ir galimybes, taip pat taikinio pažeidžiamumą ir stipriąsias puses.
- SSGG analizė: tai strateginio planavimo įrankis, padedantis organizacijoms nustatyti savo stipriąsias, silpnąsias puses, galimybes ir grėsmes. Jis gali būti naudojamas įvairiems hibridinės grėsmės komponentams nustatyti ir įvertinti bei tinkamoms atsako priemonėms sukurti.
- Pagrindinės priežasties analizė: Metodika apima pagrindinių problemos priežasčių nustatymą, įskaitant veiksnius, kurie prisideda prie hibridinės grėsmės atsiradimo ir evoliucijos.
- Scenarijų planavimas: Apima galimų ateities scenarijų kūrimą ir analizę, kad būtų galima numatyti galimas grėsmes ir iššūkius ir joms pasiruošti.

Šios analitinės metodikos gali būti naudojamos kartu siekiant pateikti visapusišką ir holistinį požiūrį į hibridinių grėsmių supratimą ir valdymą. Svarbu nuolat vertinti besikeičiančias grėsmes ir prie jų prisitaikyti bei ugdyti reikiamus gebėjimus nuo jų apsiginti.

Tradiciškai analizuojant hibridines grėsmes minimas konfliktas Ukrainoje, kai Rusijos invazinės pajėgos, naudodamos netradicinius kovinių veiksmų metodus aneksavo, Ukrainai priklausantį Krymo pusiasalį. Siekiant numatyti, pasirengti ir atremti tokias, didelio masto, hibridines grėsmes vyriausybė, valsybės mastu, gali imtis sekančių priemonių.

- Sukurti nacionalinę hibridinių grėsmių valdymo strategiją. Vyriausybės gali parengti nacionalinę strategiją, kurioje būtų nurodyta, kaip jos nustatys, įvertins ir reaguos į hibridines grėsmes. Ši strategija turėtų būti parengta bendradarbiaujant su kitomis atitinkamomis agentūromis šalies viduje ir išorėje, privačiu sektoriumi, tarptautinėmis organizacijomis tokiomis kaip Europos sąjunga ir NATO ir kitomis suinteresuotosiomis šalimis.
- Parengti žvalgybos pajėgumus. Vyriausybės gali plėtoti savo žvalgybos pajėgumus, kad geriau suprastų ir sektų hibridines grėsmes. Tai galėtų apimti žvalgybos agentūrų finansavimo didinimą, dalijimosi duomenimis sistemų tobulinimą ir ryšių su kitų šalių žvalgybos agentūromis kūrimą.
- Koordinuoti su tarptautiniais partneriais: vyriausybės gali bendradarbiauti su tarptautiniais partneriais, kad keistųsi informacija ir koordinuotų savo atsaką į hibridines grėsmes. Tai galima padaryti per esamas tarptautines organizacijas, tokias kaip NATO ir Europos sąjungą, arba per dvišalius susitarimus tarp atskirų šalių.
- Įgyvendinti atsparumo priemones. Vyriausybės gali įgyvendinti atsparumo priemones, skirtas apsisaugoti ir greitai atsistatyti nuo hibridinių grėsmių poveikio, pavyzdžiui, stiprinti ypatingos svarbos infrastruktūros objektų apsaugą, gerinti kibernetinį saugumą ir stiprinti reagavimo į ekstremalias situacijas pajėgumus.
- Skatinti visuomenės sąmoningumą. Vyriausybės gali šviesti visuomenę apie hibridines grėsmes ir kaip nuo jų apsisaugoti. Tai gali apimti viešųjų paslaugų skelbimus, mokymo programas ir kitas visuomenės informavimo priemones ir metodus.

Apibedrinat galima sakyti, kad krizių valdymas yra valstybių ir organizacijų naudojamas procedūrų ir metodų rinkinys, skirtas krizių prevencijai, pasiruošimui, atsakui ir atsistatymui po jų. Veiksmingam krizių valdymui reikalingas visapusiškas požiūris, apimantis rizikos vertinimą, komunikaciją, koordinavimą ir sprendimų priėmimą. Yra keletas dažniausiai naudojamų krizių valdymo modelių, tokie kaip keturių pakopų, trifazis, šešių žingsnių ir integruotas modeliai. Visi šie modeliai susideda iš etapų, kurie apima pasiruošimą krizei, reagavimą į ją ir atsistatymą po jos, taip pat pabrėžiama komunikacijos, rizikos vertinimo ir mokymosi iš praeities krizių svarba. Skirtingi modeliai akcentuoja skirtingus aspektus, pvz., keturių pakopų modelis pabrėžia ankstyvo signalų aptikimo svarbą, o šešių žingsnių modelis pabrėžia sistemingo ir iniciatyvaus požiūrio reikalingumą. Šie modeliai plačiai naudojami

įvairiose organizacijose ir srityse, pvz., vadyboje, viešųjų ryšių ir komunikacijos srityse bei ekstremaliųjų situacijų valdyme valstybės mastu.

1.5 Tarptautinių organizacijų vaidmuo

Reikia pabrėžti tarptautinių organizacijų svarbą ir paramą valstybei atpažystant, reaguojant ir atremiant hibridines grėsmes. Dvi pagrindinės tarptautinės organizacijos kurios supranta hibridinių grėsmių keliamus iššūkius yra NATO ir Europos sąjunga.

NATO (Šiaurės Atlanto sutarties organizacija) pripažįsta, kad hibridinės grėsmės kelia didelį iššūkį jos valstybių narių ir platesnės tarptautinės bendruomenės saugumui. Hibridines grėsmes NATO apibrėžia kaip „daugybę karinių, sukarintų, diplomatinių, ekonominių, kibernetinių ir psichologinių priemonių, kurios sąmoningai derinamos siekiant strateginio efekto“.

NATO įgyvendino daugybę priemonių hibridinėms grėsmėms spręsti, įskaitant:

Valstybės atsparumo didinimą. NATO sukūrė atsparumo hibridinėms grėsmėms plėtros sistemą, kuri apima tokias priemones kaip ypatingos svarbos infrastruktūros objektų saugumo didinimą, kibernetinio saugumo stiprinimą ir gebėjimų reaguoti į atakas bei atsigauti po jų gerinimą.

Žvalgybos ir stebėjimo pajėgumų stiprinimą. NATO investuoja į tvirtų žvalgybos ir stebėjimo pajėgumų kūrimą, kad būtų galima aptikti ir sekti galimas hibridines grėsmes.

Tarptautinio bendradarbiavimo stiprinimą. NATO glaudžiai bendradarbiauja su šalimis partnerėmis ir organizacijomis, skatina ir kuria įrankius keistis informacija ir koordinuoti pastangas ginantis nuo hibridinių grėsmių.

Kibernetinės gynybos stiprinimą. NATO sukūrė visapusišką požiūrį į kibernetinį saugumą, kuris apima tokias priemones kaip kibernetinės gynybos centro įkūrimas ir kibernetinės gynybos pajėgumų plėtra.

Įsitraukimą į diplomatiją ir komunikaciją. NATO išnaudoja diplomatinius kanalus, kad išspręstų kylančias problemas ir dalyvauja viešoje komunikacijoje, kad informuotų visuomenę ir atgrasytų galimus užpuolikus.

Apskritai NATO pripažįsta, kad hibridinės grėsmės yra sudėtingos ir daugialypės, todėl jas įveikti reikia visapusiško ir koordinuoto požiūrio. Ji įsipareigojusi bendradarbiauti su savo valstybėmis narėmis ir partneriais, kad sukurtų reikiamus pajėgumus apsiginti nuo hibridinių grėsmių ir į jas reaguoti. (NATO STRATCOM COE et al., 2022, Fry, 2022,)

Europos Sąjunga (ES) hibridines grėsmes vertina kaip didelį iššūkį savo valstybių narių ir platesnės tarptautinės bendruomenės saugumui. Hibridines grėsmes ES apibrėžia kaip „daugybę karinių, sukarintų, diplomatinių, ekonominių, kibernetinių ir psichologinių priemonių, kurios sąmoningai naudojamos siekiant strateginio efekto“.

ES įgyvendino daugybę priemonių hibridinėms grėsmėms spręsti, įskaitant:

Išsamios strategijos kūrimą. ES parengė išsamią kovos su hibridinėmis grėsmėmis strategiją, kuri apima tokias priemones kaip ypatingos svarbos infrastruktūros objektų saugumo didinimas, kibernetinio saugumo stiprinimas ir gebėjimų reaguoti į atakas bei atsigauti po jų gerinimas.

Žvalgybos ir stebėjimo pajėgumų stiprinimą. ES investavo į tvarių žvalgybos ir stebėjimo pajėgumų, skirtų galimams hibridinėms grėsmėms aptikti ir sekti, kūrimą.

Tarptautinio bendradarbiavimo stiprinimą. ES glaudžiai bendradarbiauja su šalimis partnerėmis ir organizacijomis, kad keistųsi informacija ir koordinuotų pastangas apsiginti nuo hibridinių grėsmių.

Kibernetinės gynybos stiprinimą. ES sukūrė visapusišką požiūrį į kibernetinį saugumą, kuris apima tokias priemones kaip kibernetinės gynybos centro įkūrimas, kibernetinės gynybos pajėgumų plėtra, kibernetinio saugumo teisinės bazės plėtrą.

Įsitraukimą į diplomatiją ir komunikaciją. ES naudoja diplomatinius kanalus, kad spręstų susirūpinimą keliančius klausimus ir viešai informuotų visuomenę ir atgrasytų galimus užpuolikus.

Apskritai ES pripažįsta, kad hibridinės grėsmės yra sudėtingos ir daugialypės, todėl jas įveikti reikia visapusiško ir koordinuoto požiūrio. Ji įsipareigojusi bendradarbiauti su savo valstybėmis narėmis ir partneriais, kad sukurtų reikiamus pajėgumus apsiginti nuo hibridinių grėsmių ir į jas reaguoti.

Papildomai tarptautinės organizacijos gali koordinuoti atsaką į hibridines grėsmes įvairiose šalyse ir sektoriuose. Pavyzdžiui, JT gali bendradarbiauti su valstybėmis narėmis, kad

sukurtų suderintą strategiją kovai su kibernetinėmis atakomis, o NATO gali koordinuoti karinius atsakus į hibridinį karą.

Tarptautinės organizacijos gali teikti paramą ir teikti išteklius šalims, kurios neturi reikiamų gebėjimų pačios spręsti hibridines grėsmes. Tai galėtų apimti mokymus ir techninę pagalbą kibernetinio saugumo, elektroninių nusikaltimų tyrimų ir reagavimo į nelaimes klausimais.

Tarptautinės organizacijos gali kurti ir skatinti atsakingo technologijų naudojimo ir ypatingos svarbos infrastruktūros objektų apsaugos normas ir standartus. Tai gali padėti atgrasyti ir užkirsti kelią hibridinėms grėsmėms.

Tarptautinės organizacijos gali panaudoti savo diplomatinius svertus, siekdamos kovoti su hibridinėmis grėsmėmis derybomis ir kitomis diplomatinėmis pastangomis. Tai galėtų apimti bendradarbiavimą su kitomis šalimis siekiant pagerinti kibernetinį saugumą ir užkirsti kelią kibernetinių atakų naudojimui nusikalstamais tikslais.

Apibendrinati galima teigti, kad tarptautinės organizacijos yra labai svarbios ir teikia paramą valstybei reaguojant į hibridines grėsmes. Dvi pagrindinės organizacijos, kurios supranta hibridinių grėsmių keliamus iššūkius, yra NATO ir Europos Sąjunga (ES). NATO suvokia, kad hibridinės grėsmės kelia didelį iššūkį jos valstybių narių ir platesnės tarptautinės bendruomenės saugumui, o ES hibridines grėsmes vertina kaip didelį iššūkį savo valstybių narių ir tarptautinės bendruomenės saugumui.

NATO įgyvendino daugybę priemonių, įskaitant valstybės atsparumo didinimą, žvalgybos ir stebėjimo pajėgumų stiprinimą, tarptautinio bendradarbiavimo stiprinimą, kibernetinės gynybos stiprinimą, ir įsitraukimą į diplomatiją ir komunikaciją. Visapusiškas ir koordinuotas požiūris yra būtinas hibridinėms grėsmėms įveikti, ir NATO yra pasiryžusi bendradarbiauti su savo valstybėmis narėmis ir partneriais, kad sukurtų reikiamus pajėgumus apsiginti nuo hibridinių grėsmių ir į jas reaguoti.

ES taip pat įgyvendino daugybę priemonių, įskaitant energetinio saugumo stiprinimą, kibernetinio saugumo plėtojimą, ir informacijos apsaugą, kad atremtų hibridines grėsmes. ES yra pasiryžusi bendradarbiauti su savo valstybėmis narėmis ir tarptautinėmis organizacijomis, kad sukurtų veiksmingas strategijas kovojant su hibridinėmis grėsmėmis.

2. EMPIRINIS TYRIMAS

1.6 Suomijos hibridinių grėsmių valdymo modelio analizė

Tyrimui buvo pasirinkta kokybinė vieno atvejo studijos instrumentinė strategija (Yin, 2018, Merriam & Tisdell, 2016, Creswell & Poth, 2018,). Tyrimo metu buvo atliktas nuodugnus vieno atvejo tyrimas, remiantis strateginių ir mokslinių dokumentų kokybinio turinio analizės metodu. (Krippendorff, 2018, Neuendorf, 2002, Weber, 1990,)

Autoriai turinio analizę apibrėžia kaip tyrimo metodą, leidžiantį daryti išvadas iš teksto. Jie aiškina, kad turinio analizė gali būti naudojama atsakant į įvairių tipų tyrimo klausimus ir gali būti taikoma įvairiems tekstiniams duomenims, įskaitant rašytinius dokumentus, garso įrašus ir vaizdus.

Aprašomi įvairūs turinio analizės etapai, įskaitant:

- Tyrimo klausimo apibrėžimas ir analizuojamų duomenų parinkimas
- Kodavimo schemos sprendimas ir duomenų kodavimas
- Koduotų duomenų analizė, siekiant padaryti išvadas ir išvadas
- Rezultatų interpretavimas ir turinio analizės patikimumo bei pagrįstumo vertinimas

Mokslinėje literatūroje pabrėžiama sistemingo ir skaidraus turinio analizės metodo naudojimo svarbą, siekiant užtikrinti rezultatų patikimumą ir pagrįstumą.

Remiantis tirtu atveju buvo atlikta tyrimo duomenų klasifikacija ir tarpusavio ryšių nustatymas, iškelti teiginiai įvertinti dėl jų pritaikomumo kitoms situacijoms.

Keletas pagrindinių statistinių duomenų apie Suomiją (Statistics Finland, 2023):

Gyventojų skaičius: 2021 m. apskaičiuota, kad Suomijoje gyvena apie 5,5 mln. BVP: apskaičiuota, kad Suomijos bendrasis vidaus produktas (BVP) 2020 m. sieks 214,3 mlrd.

Ekonomika: Suomijos ekonomika yra labai išvystyta ir technologiškai pažangi, o pagrindinės pramonės šakos apima elektroniką, mašinas ir miško produktus.

Švietimas: Suomijoje yra labai išvystyta švietimo sistema, kurios raštingumo lygis siekia beveik 100 %. Šalis garsėja tuo, kad akcentuoja lygias švietimo galimybes ir kokybišką mokytojų rengimą.

Vidutinė gyvenimo trukmė Suomijoje yra viena didžiausių pasaulyje, o vidutinė gyvenimo trukmė yra maždaug 83 metai.

Sveikatos priežiūra: Suomijoje yra visapusiška visuomenės sveikatos priežiūros sistema, kuri suteikia visuotinę aprėptį visiems piliečiams.

Aplinka: Suomija garsėja savo pastangomis skatinti aplinkos tvarumą ir ėmėsi veiksmų, siekdama sumažinti šiltnamio efektą sukeliančių dujų išmetimą ir tausoti gamtos išteklius.

Politinė sistema: Suomija yra parlamentinė respublika, kurios prezidentas eina valstybės vadovo pareigas ir ministras pirmininkas – vyriausybės vadovas.

Socialinė gerovė: Suomija turi stiprią socialinės gerovės sistemą, kuri suteikia piliečiams galimybę naudotis įvairiomis išmokomis, įskaitant nedarbo draudimą, sveikatos priežiūrą ir pensijas.

Technologijos: Suomijoje yra daugybė pasaulyje pirmaujančių technologijų įmonių ir ji yra plačiai pripažinta viena technologiškai pažangiausių pasaulio šalių.

Suomija yra plačiai pripažinta kaip turinti tvirtą kibernetinio saugumo poziciją ir tarptautiniuose kibernetinio saugumo indeksuose nuolat užima aukštas vietas. (*Finland Succeeds in Cyber Security Comparisons*, 2022)

Pasaulinis kibernetinio saugumo indeksas: Suomija užėmė 8 vietą pasaulyje pagal 2021 m. pasaulinį kibernetinio saugumo indeksą, pagal kurį vertinamas šalių įsipareigojimas siekti kibernetinio saugumo.

Pasaulio ekonomikos forumas: Pasaulio ekonomikos forumo 2020 m. Pasaulinio konkurencingumo ataskaitoje Suomija buvo įvertinta kaip 4-oji saugiausia šalis pasaulyje.

NIST kibernetinio saugumo sistema: Suomija buvo pripažinta už tai, kad įgyvendino Nacionalinio standartų ir technologijų instituto (NIST) kibernetinio saugumo sistemą, kurioje pateikiamos gairės organizacijoms, kaip valdyti ir sumažinti kibernetinio saugumo riziką.

Suomija susiduria su įvairiomis hibridinėmis grėsmėmis, kurios kyla iš įvairių šaltinių, įskaitant valstybinius veikėjus, nevalstybinius veikėjus ir nusikalstamas organizacijas. (Secretariat of the Security Committee, 2013) Kai kurios ryškiausios hibridinės grėsmės Suomijai yra šios:

- Kibernetinės atakos: Suomija yra pažeidžiama įvairių kibernetinių atakų, įskaitant išplėstines nuolatines grėsmes (APT), kenkėjiškas programas ir sukčiavimą. Šios atakos gali turėti didelį poveikį kritinei infrastruktūrai, nacionaliniam saugumui ir ekonomikai.
- Dezinformacija ir propaganda: Suomija yra pažeidžiama dezinformacijos kampanijų, kuriomis siekiama manipuliuoti viešąja nuomone ir skleisti melagingą informaciją. Šios kampanijos gali būti naudojamos sėti nesantaiką, pakirsti pasitikėjimą institucijomis ir destabilizuoti visuomenę.
- Kišimasis į rinkimus: Suomija, kaip ir daugelis kitų šalių, yra pažeidžiama kišimosi į rinkimus, įskaitant kibernetines atakas prieš balsavimo sistemas, propagandos kampanijas, kuriomis siekiama manipuliuoti viešąja nuomone, ir melagingos informacijos skleidimą.
- Ekonominis ir tradicinis šnipinėjimas: stipri Suomijos ekonomika ir pažangių technologijų sektorius daro ją ekonominio šnipinėjimo taikiniu, kai užsienio veikėjai siekia pavogti komercines paslaptis ir neskelbtiną informaciją.Suomija taip pat yra pažeidžiama tradicinės šnipinėjimo veiklos, o užsienio veikėjai siekia rinkti neskelbtiną informaciją ir žvalgybos informaciją.

Šios hibridinės grėsmės nuolat vystosi ir keičiasi, todėl Suomijai svarbu ir toliau investuoti į gebėjimą jas aptikti, užkirsti kelią ir į jas reaguoti. Tai apima investicijas į kibernetinio saugumo infrastruktūrą, visuomenės informuotumo ir žiniasklaidos raštingumo didinimą bei jos žvalgybos ir saugumo pajėgumų stiprinimą.

Suomija taip pat susiduria su įvairiomis karinėmis hibridinėmis grėsmėmis. (Finnish Government, 2021) Kai kurios ryškiausios karinės hibridinės grėsmės Suomijai yra šios:

- Hibridinis karas: Hibridinis karas reiškia karinių ir nekarinių priemonių naudojimą strateginiams tikslams pasiekti. Tokio pobūdžio grėsmės tampa vis dažnesnės, o Suomija yra pažeidžiama hibridinio karo taktikos, kurią taiko valstybės veikėjai, pavyzdžiui, Rusija.

- Informacinės operacijos: informacines operacijas, įskaitant dezinformacijos kampanijas, propagandą ir psichologines operacijas, naudoja valstybiniai ir nevalstybiniai veikėjai, siekdami manipuliuoti viešąja nuomone ir sėti nesantaiką. Šios operacijos gali būti naudojamos siekiant pakirsti pasitikėjimą institucijomis ir destabilizuoti visuomenę.

- Kibernetinės atakos: kibernetinės atakos yra reikšminga karinė hibridinė grėsmė Suomijai, nes jos gali turėti didelį poveikį karinėms sistemoms, operacijoms ir infrastruktūrai.
- Nekonvencinis karas: Netradicinis karas, įskaitant nereguliarų ir partizaninį karą, yra karinė hibridinė grėsmė Suomijai, galinti mesti iššūkį jos saugumui ir stabilumui.
- Įtakos operacijos: įtakos operacijas naudoja valstybiniai ir nevalstybiniai veikėjai, norėdami daryti įtaką asmenų ir organizacijų veiksmams ir sprendimams. Šios operacijos gali būti naudojamos manipuliuoti viešąja nuomone ir sprendimų priėmimu ir gali turėti didelį poveikį nacionaliniam saugumui ir stabilumui.

Svarbu, kad Suomija išlaikytų savo karinius pajėgumus, taip pat gebėjimą aptikti, užkirsti kelią ir reaguoti į šias hibridines grėsmes, kad išlaikytų savo saugumą ir stabilumą šių besikeičiančių iššūkių akivaizdoje. Tai apima investicijas į jos karinius pajėgumus, partneryščių ir aljansų kūrimą bei jos žvalgybos ir saugumo pajėgumų stiprinimą.

Suomijos 2017 m. visuomenės saugumo strategija (Finish Government, 2017) grindžiama visapusiško saugumo koncepcija, kai visi visuomenės veikėjai, įskaitant vyriausybę, verslą, pilietinės visuomenės organizacijas ir piliečius, dirba kartu, kad apsaugotų gyvybiškai svarbias visuomenės funkcijas. Tai apima dalijimąsi informacija, bendrų planų kūrimą ir mokymą bei bendrą darbą atliekant kasdienes operacijas.

Saugumo strategijoje saugumo veikėjai apibrėžiami kaip visi subjektai, dalyvaujantys koordinuotame saugumo darbe ar veikloje. Jame pabrėžiamas tarpsektorinis pasirengimo pobūdis ir pabrėžiamas atskirų piliečių ir namų ūkių vaidmuo skatinant visuomenės atsparumą. Nevyriausybinės organizacijos, tokios kaip Suomijos Raudonasis Kryžius, atlieka pagrindinį vaidmenį teikiant paslaugas, koordinuojant savanorius ir išlaikant patirtį tokiose srityse kaip nenumatytų atvejų operacijos. Ministro Pirmininko tarnyba yra atsakinga už vyriausybės situacijos informavimą, pasirengimą ir saugumo tarnybas. Saugumo komitetas yra nuolatinė ir plataus masto bendradarbiavimo nenumatytų atvejų planavimo institucija, padedanti vyriausybei ir ministerijoms visapusiškais saugumo klausimais. Krašto apsaugos kursuose vyksta įvairių visuomenės sluoksnių lyderių mokymai, kuriais siekiama gerinti bendradarbiavimą ekstremaliomis sąlygomis ir skatinti tinklų kūrimą. Regioniniuose kursuose pagrindinis dėmesys skiriamas pasirengimui regioniniu lygiu įvairiems sutrikimams ir ekstremalioms sąlygoms.

(Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation & Kalniete, 2021)

Tokia Suomijos visuotinio saugumo strategija sudaro prielaidas visiems visuomenės nariams, valstybiniam ir privačiam sektoriui dalyvauti atsako į valstybines krizes pasirengimo, planavimo ir vykdymo procese. Vienas iš tokio pasirengimo galimai hibridinei krizei yra Visapusiškas tiekimo saugumo modelis.

Suomija taiko visapusišką tiekimo saugumo modelį, pagrįstą viešojo ir privačiojo sektorių partneryste. 2017 m. saugumo strategijoje pabrėžiamas didėjantis verslo subjektų vaidmuo užtikrinant ekonomikos ir kitos ypatingos svarbos infrastruktūros objektų funkcionavimą krizės metu. Tiekimo saugumo koncepcija apima daugybę svarbių sektorių ir ją valdo Suomijos nacionalinė skubaus tiekimo agentūra (NESA).

Daugumą svarbiausių funkcijų Suomijoje valdo privataus sektoriaus veikėjai, kurie yra priklausomi nuo pasaulinių tiekimo grandinių, todėl viešojo ir privataus sektoriaus bendradarbiavimas tiekimo grandinės valdymo srityje yra labai svarbus. NESA remia įmones teikdama įrankius ir gaires veiklos tęstinumo valdymui.

Suomijos tiekimo saugumo modelis yra unikalus, jį palengvina Nacionalinės skubios pagalbos tiekimo organizacijos (NESO) sektoriai ir telkiniai, integruojantys visuomenės ir verslo bendruomenės tikslus bei interesus. NESO telkiniai suteikia informacijos apie situaciją kritiniuose sektoriuose, taip pat pagerina visuomenės atsparumą ir teikia naudos dalyvaujantiems privatiems subjektams. (Europos Sąjunga, 2021)

Suomijoje daug dėmesio skiriama visuomenės informavimui, edukavimui ir švietimui. Toks proaktyvus visuomenės edukavimo modelis suteikia piliečiams pakankamų įgūdžių orientuotis socialinėje erdvėje, tinkamai vertinti gaunamą informacijos srautą, atpažinti ir atmesti kenksmingą turinį.

Tokiam rezultatui pasiekti Suomija taiko visapusišką visuomenės požiūrį į žiniasklaidos raštingumą ir masinę komunikaciją. Vyriausybė teikia pirmenybę atsakingai žiniasklaidos komunikacijai ir įkūrė NESO telkinį „Mediapooli“, kad būtų sprendžiamos tokios problemos kaip dezinformacija, hibridinės grėsmės ir žiniasklaidos veiklos tęstinumas. Mediapooli taip pat organizuoja mokymus žurnalistams ir žiniasklaidos organizacijoms. Suomija pirmauja žiniasklaidos raštingumo indekse Europoje ir turi ilgą žiniasklaidos švietimo istoriją bei platų žiniasklaidos priemonių naudojimo raštingumo skatinimo veikėjų ir institutų tinklą. Tačiau

Suomijos modelyje yra tam tikrų iššūkių, tokių kaip informacijos mainų stoka, sunkumai priverčiant įmones bendradarbiauti, problemos dėl išteklių ir dalyvių pasitikėjimo. (Europos Sąjunga, 2021)

Suomijoje suprantama ir kibernetinės erdvės svarba. Suomijos kibernetinio saugumo strategija siekiama užtikrinti skaitmeninių tinklų patikimumą ir saugumą šalyje. Tai pasiekiama stiprinant tarptautinį bendradarbiavimą kibernetinio saugumo srityje ir Užsienio reikalų ministerijai koordinuojant Suomijos dalyvavimą tarptautiniame kibernetiniame bendradarbiavime. Kibernetinis domenas reiškia skaitmeninę lygiagrečią tikrovę, jungiančią žmones ir įrangą visame pasaulyje per informacines technologijas, internetą ir socialinę žiniasklaidą. Sparčiai augant informacinėms technologijoms, kibernetinis domenas atnešė didelių galimybių, bet ir naujų grėsmių, tokių kaip elektroniniai nusikaltimai, kibernetinis šnipinėjimas ir kibernetinės atakos. Siekiant užtikrinti saugų ir saugų kibernetinio domeno naudojimą, labai svarbu imtis priemonių apsisaugoti nuo šių grėsmių. Vidaus reikalų ministerija yra pasirengusi pagerinti informacijos srautą ir nustatyti grėsmes, kurios padės atremti hibridinės įtakos veiklai prieš Suomiją. (Government of Finland, 2013)

Kibernetinis domenas ir kibernetinis saugumas tapo svarbiu Suomijos užsienio ir saugumo politikos aspektu. Užsienio reikalų ministerija koordinuoja Suomijos dalyvavimą tarptautiniame kibernetiniame bendradarbiavime. Kibernetinis domenas reiškia žmogaus sukurtą skaitmeninę lygiagrečią realybę, kuri per informacines technologijas ir internetą sujungia žmones ir įrangą tarpvalstybiniu mastu. Kasdienės funkcijos, tokios kaip pramonė, bankininkystė, sveikatos priežiūra ir transportas, priklauso nuo skaitmeninių tinklų. Skaitmeninių tinklų atsiradimas suteikė ne tik ekonomikos augimo, inovacijų ir socialinio dalyvavimo galimybių, bet ir naujų rūšių grėsmių, pvz., elektroninių nusikaltimų ir kibernetinių atakų. Siekiant užtikrinti, kad šie tinklai veiktų kuo patikimiau ir saugiau, svarbu stiprinti tarptautinį bendradarbiavimą kibernetinio saugumo srityje. (Hutchinson, 2022)

Neseniai priimtas sprendimas dėl Suomijos narystė Šiaurės Atlanto sutarties organizacijoje (NATO) turi reikšmingų padarinių tiek Suomijai, tiek aljansui.

Suomijos narystė NATO suteiktų tvirtesnį jos saugumo ir gynybos pagrindą, taip pat padidintų bendradarbiavimo ir dalijimosi informacija galimybes su kitomis NATO narėmis. Tai padidintų jos gebėjimą apsiginti nuo hibridinių grėsmių, kibernetinių atakų ir kitų saugumo

iššūkių. Narystė NATO suteiktų Suomijai didesnį politinį ir ekonominį stabilumą, nes ji būtų didesnės šalių bendruomenės dalis, įsipareigojusi laikytis tų pačių vertybių ir interesų. NATO yra reikšmingas pasaulinis veikėjas, o Suomijos narystė padidintų jos įtaką ir galimybes formuoti tarptautinę saugumo ir gynybos politiką.

Narystė aljnase suteiktų naujų galimybių partnerystei ir bendradarbiavimui su kitomis NATO šalimis bei palengvintų glaudesnius darbo santykius su pagrindiniais sąjungininkais Europoje ir Šiaurės Amerikoje.

Tačiau narystė NATO taip pat sukeltų naujų sudėtingumo ir iššūkių, įskaitant poreikį prisitaikyti prie NATO procesų ir struktūrų bei galimą įtampą su NATO nepriklausančiomis šalimis, tokiomis kaip Rusija.

Apibendrinant galima teigti, kad Suomijos potenciali narystės NATO demonstruoja valstybės ir visuomenės rįžtą stiprinti valstybės nacionalinį saugumą ir atsparumą, įskaitant atsparumą kylančioms ir pastoviai kintančioms hibridinėms grėsmėms. Suomijos apsisprendimas demonstruoja lankstumą reaguojant į pastoviai kintančią geopolitinę aplinką ir naujus iššūkius.

Valstybės mastu Suomijoje už pasirengimą krizių valdymui, įskaitant hibridinių krizių, ir jų valdymą atsakinga Vidaus reikalu ministerija. Vidaus reikalų ministerija yra Suomijos vyriausybės departamentas, atsakingas už vidaus saugumą, migraciją, Suomijos pilietybę, gelbėjimo tarnybas, reagavimą į ekstremalias situacijas, sienų saugumą ir paiešką bei gelbėjimą jūroje. Jos trys pagrindinės pareigos – rengti teisės aktus, valdyti agentūrų veiklą, tvarkyti tarptautinius ir ES reikalus. Ministerija vadovaujasi skaidrumo, sąžiningumo ir bendro darbo vertybėmis. (Ministry of the Interior Fi, 2023)

Vidaus reikalų ministerija aiškiai vertina hibridines grėsmes ir jų poveikio svarbą. Hibridinės grėsmės reiškia sistemingą valstybės įtaką kitai valstybei, naudojant įvairias priemones. Tai gali būti atliekama slaptai ir gali apimti politines, diplomatines, ekonomines, karines ir kibernetines priemones. Saugumo aplinka Suomijoje prastėjo, buvo pastebėta daugiau hibridinės įtakos veiklos. Siekiant kovoti su šiomis grėsmėmis buvo sukurtas bendru partneriu tinklu pagrįstas pasirengimas ir valdymo modelis.

Ministerija turi tinklą, koordinuojamą Nacionalinio saugumo skyriaus, siekiant nustatyti ir užkirsti kelią hibridinės įtakos veiklai bei didinti atsparumą. Tinklas yra atsakingas už hibridinės veiklos grėsmių vertinimo parengimą, bendradarbiaudamas su Suomijos saugumo ir

žvalgybos tarnyba, koordinuoja hibridinių grėsmių vertinimą su ES ir kitais tarptautiniais partneriais. (*Hybrid Threats and Hybrid Influence Activities - Ministry of the Interior*, 2023)

Suomijos hibridinių grėsmių valdymo modelis geriausiai apibūdinamas kaip visapusiškas požiūris, apimantis įvairius nacionalinio saugumo elementus, įskaitant karines, žvalgybos, teisėsaugos ir diplomatines priemones, siekiant veiksmingai spręsti hibridines grėsmes ir jas sušvelninti. Jame pripažįstamas kintantis grėsmių nacionaliniam saugumui pobūdis ir lankstaus bei prisitaikančio atsako poreikis. Modelis apima bendradarbiavimą ir koordinavimą tarp įvairių vyriausybinių agentūrų, pilietinės visuomenės organizacijų ir privataus sektoriaus, sprendžiant tiek fizines, tiek kibernetines grėsmes, taip pat hibridinius iššūkius, kurie derina abiejų elementus. Modeliu siekiama padidinti šalies atsparumą ir gebėjimą reaguoti į įvairius ir besikeičiančius saugumo iššūkius, įskaitant dezinformaciją, kibernetines atakas, terorizmą ir kitas hibridinio karo formas.

Pagrindiniai Suomijos hibridinių grėsmių modelio elementai yra šie:

- Strateginis žvalgybos duomenų rinkimas: Suomija turi patikimą žvalgybos duomenų rinkimo sistemą, kuri padeda nustatyti galimas grėsmes ir pažeidžiamumą ir iš anksto įspėja apie galimas krizes.
- Išsamus nenumatytų atvejų planavimas: Suomija parengė išsamius nenumatytų atvejų planus, skirtus reaguoti į įvairių tipų hibridines krizes, įskaitant planus kovai su kibernetinėmis atakomis, dezinformacijos kampanijomis ir kitomis netradicinėmis grėsmėmis saugumui.
- Tarpinstitucinis bendradarbiavimas: hibridinių krizių valdymui Suomijoje būdingas glaudus bendradarbiavimas ir koordinavimas tarp skirtingų vyriausybinių agentūrų, įskaitant policiją, kariuomenę ir žvalgybos tarnybas. Tai padeda užtikrinti veiksmingą ir efektyvų atsaką į krizes.
- Viešojo ir privačiojo sektorių partnerystė: Suomijos vyriausybė pripažįsta svarbų privataus sektoriaus ir pilietinės visuomenės organizacijų vaidmenį valdant hibridines krizes ir užmezgė partnerystę su šiais veikėjais, kad užtikrintų koordinuotą atsaką.

- Visuomenės žiniasklaidos priemonių naudojimo raštingumo politika: Suteikdama piliečiams įgūdžių ir žinių, kurių jiems reikia norint naršyti skaitmeninės žiniasklaidos

aplinkoje, Suomija stengiasi užtikrinti, kad jos piliečiai turėtų prieigą prie tikslios informacijos ir galėtų visapusiškai dalyvauti demokratiniuose procesuose.

- Krizių valdymo procedūros: Suomija turi nusistovėjusias krizių valdymo procedūras, įskaitant sprendimų priėmimo, komunikacijos ir dalijimosi informacija protokolus krizės metu. Šios procedūros padeda užtikrinti veiksmingą ir efektyvų atsaką į krizes.

Suomijos hibridinių grėsmių valdymo modelis plačiai laikomas visapusišku ir veiksmingu metodu sprendžiant įvairius hibridinių grėsmių keliamus iššūkius. Šiame modelyje pirmenybė teikiama integruotam ir bendradarbiaujančiam požiūriui, kuriuo siekiama suburti kelis veikėjus įvairiuose sektoriuose ir valdžios lygmenyse, kad būtų galima geriau suprasti ir spręsti sudėtingą hibridinių grėsmių pobūdį.

Vienas iš pagrindinių Suomijos hibridinio grėsmių valdymo modelio aspektų yra keitimasis informacija ir jos analizė. Tai apima reguliarų galimų grėsmių vertinimą ir dalijimąsi informacija tarp atitinkamų veikėjų, įskaitant karines, žvalgybos ir teisėsaugos institucijas. Tai padeda užtikrinti, kad visi dalyviai aiškiai suprastų besikeičiančią grėsmę ir galėtų koordinuotai bei veiksmingai reaguoti.

Kitas svarbus Suomijos hibridinių grėsmių valdymo modelio aspektas – dėmesys atsparumui ir pasirengimui. Tai apima nuolatines pastangas gerinti šalies pasirengimą ir gebėjimą reaguoti į galimas grėsmes, taip pat sumažinti jos pažeidžiamumą hibridinėms atakoms. Tai apima tokias priemones kaip kibernetinio saugumo gerinimas, ypatingos svarbos infrastruktūros stiprinimas ir nenumatytų atvejų planų kūrimas, siekiant užtikrinti greitą ir veiksmingą atsaką į krizę.

Sekantis svarbus Suomijos hibridinių grėsmių valdymo modelio elementas yra reagavimo į krizes planavimas. Tai reiškia nustatytą reagavimo į krizę strategijų ir procedūrų rengimo ir kūrimo procesą. Tai apima galimų krizių nustatymą, su kiekviena iš jų susijusios rizikos ir poveikio įvertinimą ir išsamių planų, kaip veiksmingai reaguoti, rengimą. Reagavimo į krizes planavime paprastai dalyvauja kelios suinteresuotosios šalys, įskaitant vyriausybines agentūras, teisėsaugą, pirmuosius gelbėtojus, įmones ir kitas organizacijas, kurios dirba kartu, kad būtų užtikrintas koordinuotas ir veiksmingas atsakas krizės atveju.

Pagrindinis reagavimo į krizes planavimo tikslas – kuo greičiau sumažinti neigiamus krizės padarinius ir atkurti normalią veiklą. Tai apima pasirengimą įvairiems scenarijams,

įskaitant stichines nelaimes, pandemijas, kibernetines atakas ir kitų tipų ekstremalias situacijas. Reagavimo į krizes planai dažnai apima tokius elementus kaip evakuacijos procedūros, ryšio protokolai, incidentų valdymo sistemos ir išteklių paskirstymo strategijos.

Suomijos vidaus reikalų ministerija atskirai sukurtame administraciniame padalinyje valdo priemones, skirtas užtikrinti informacijos srautą ir nustatyti kylančias. Vidaus reikalų ministerija turi kovos su hibridinėmis grėsmėmis tinklą, kurio darbą koordinuoja Nacionalinio saugumo skyrius. Tinkle sprendžiami klausimai yra susiję su bendru Vyriausybės ir ES pasirengimu atpažinti ir atliepti hibridines grėsmes. Tinklas taip pat nustato ir valdo sąveiką tarp ministerijos ir atskirų valstybės funkcionavimą užtikrinančių sektorių, koordinuoja bendrą nenumatytų atvejų planavimą. Tinklas, bendradarbiaudamas su Suomijos saugumo ir žvalgybos tarnyba, yra atsakingas už hibridinių grėsmių vertinimo parengimą. Vidaus reikalų ministerijos Nacionalinio saugumo skyrius Vyriausybės lygiu taip pat koordinuoja hibridinių grėsmių vertinimą, atliekamą su Europos Sąjunga ir kitais tarptautinio bendradarbiavimo partneriais.

Apibendrinant galima teigti, kad Suomijos hibridinių grėsmių valdymo modelis yra visapusiškas ir apima kelis nacionalinį saugumą įtakojančius elementus ir karines, žvalgybos, teisėsaugos ir diplomatines priemones. Modelis yra lankstus ir prisitaikantis prie besikeičiančių grėsmių pobūdžio, o jo tikslas yra padidinti šalies atsparumą ir gebėjimą reaguoti į įvairius ir besikeičiančius saugumo iššūkius, įskaitant dezinformaciją, kibernetines atakas, terorizmą ir kitas hibridinio karo formas. Pagrindiniai modelio elementai yra strateginis žvalgybos duomenų rinkimas, išsamus nenumatytų atvejų planavimas, tarpinstitucinis bendradarbiavimas, viešojo ir privačiojo sektorių partnerystė, visuomenės žiniasklaidos priemonių naudojimo raštingumo politika ir krizių valdymo procedūros. Suomijos modelis plačiai laikomas veiksmingu metodu sprendžiant įvairius hibridinius iššūkius.

2.1.1 Tyrimo duomenų klasifikacija ir tarpusavio ryšio analizė

Tyrimo duomenys klasifikuojami į tris plačias kategorijas:

- Tyrimo erdvė ir joje veikiančios grėsmės
- Veikėjai ir jų atsakomybės
- Indelis ir Rezultatas

Tyrimo erdvė apibūdinama kaip tarptautinė ir valstybės elektroninė erdvė kurioje prasideda ir vystosi hibridinės grėsmės.

Veikėjai - elektroninės erdvės naudotojai.

Indėlis ir Rezultatas - produktas gautas elektroninėje erdvėje sąveikaujant veikėjams ir jo efektas.

Tyrimo erdvė ir joje veikiančios grėsmės	Veikėjai	Indėlis ir rezultatas
Kibernetinės atakos	Valstybės institucijos (Parlamentas, Vyriausybė ir ministerijos, valstybiniai ir privatūs kritinės infrastruktūros valdytojai, žvalgybos bendruomenė,krašto gynybos sektorius)	Strateginių dokumentų rengimas. Įgyvendinančių teisės aktų rengimas, grėsmių analizė, rizikų vertinimas, atsako ir atsistatymo planų rengimas, tarptautinis bendradarbiavimas
Dezinformacija ir propaganda	Valstybinis ir privatus sektorius, visuomenė	Kibernetinio saugumo gerinimas, budrumas, sąmoningumo auklėjimas ir švietėjiška veikla
Kišimasis į rinkimus	Valstybė, visuomenė	Kibernetinis saugumas, e. Valdžios veiksmingumo užtikrinimas
Ekonominis ir tradicinis šnipinėjimas	Valstybinis ir privatus sektorius	Kibernetinis saugumas, švietėjiška veikla
Hibridinis karas	Valstybė, gynybos sektorius, visuomenė	Grėsmių analizė ir vertinimas, planų rengimas, tarptautinis bendradarbiavimas
Kibernetinės atakos	Gynybos sektorius	Grėsmių analizė ir vertinimas,

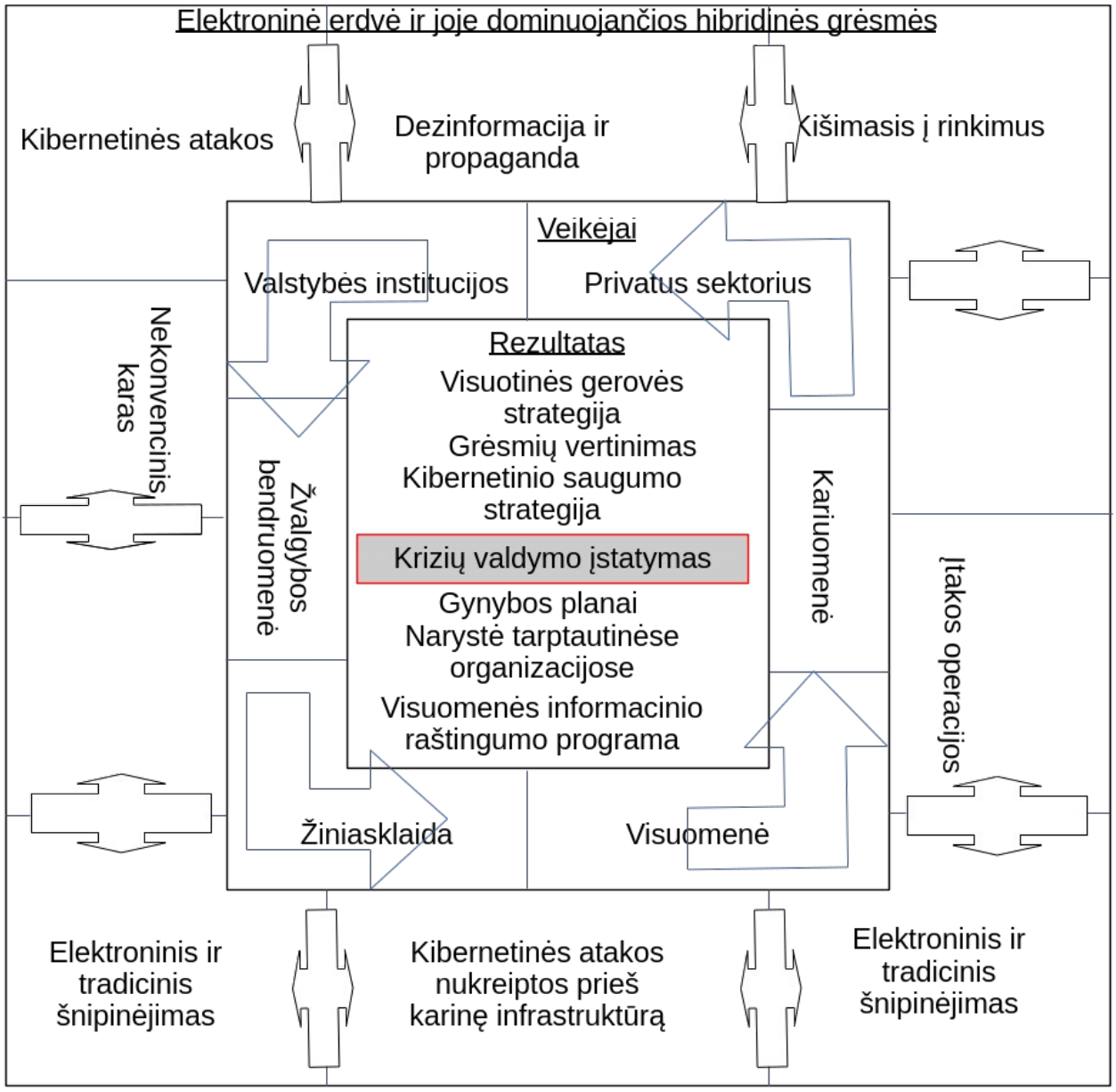
nukreiptos prieš karinę infrastruktūrą		planų rengimas, tarptautinis bendradarbiavimas
Nekonvencinis karas	Valstybė, gynybos sektorius, visuomenė	Grėsmių analizė ir vertinimas, planų rengimas, visuotinis pasirengimas tarptautinis bendradarbiavimas, diplomatinė veikla
Įtakos operacijos	Valstybė, gynybos sektorius	Psichologinis atsparumas, informacijos operacijos

Šaltinis: Parengta autoriaus

1 lentelė. Tyrimo duomenų klasifikacija

Tyrimo duomenų klasifikacijos matrica demonstruoja Valstyės ir jos institucijų, privataus sektoriaus ir visuomenės vaidmenį siekiant tinkamai pasirengti ir reaguoti į hibridinių grėsmių keliamus iššūkius ir grėsmes nacionalinam saugumui. Kiekvienas veikėjas operuojantis elektroninėje erdvėje gali susidurti su hibridinio pobūdžio grėsmėmis ir turi atlikti jam nustatytą vaidmenį ruošiantis atremti, atliepiant ir atsistatant po hibridinės atakos. Iš veikėjų ir jų indėlio analizės ryškėja koordinuojantis Vyriausybės vaidmuo ruošiantis, atremiant ir atsistatant po hibridinių atakų.

Veikėjų sąveiką elektroninėje erdvėje atsakant į hibridines grėsmes sąveiką grafiškai galima pavaizduoti sekančiai.



Šaltinis: Parengta autoriaus

4. pav. Sąveika e. erdvėje

Apibendrintai galima teigti, kad Suomijos hibridinių grėsmių valdymo modelis yra vertinamas kaip geriausios praktikos modelis ir dažnai minimas kaip pavyzdys kitoms šalims, norinčioms sukurti savo hibridinių grėsmių valdymo sistemas.

1.7 Hibridinių grėsmių elektroninėje erdvėje valstybės mastu valdymo modelio konstravimo ir taikymo tyrimas

Tyrimui buvo pasirinktas kombinuotas kokybinio - kiekybinio tyrimo metodas (Plano Clark & Ivankova, 2015, Teddlie et al., 1998,) - ekspertų nuomonę norima išsiaiškinti taikant strukturizuota DELPHI (Schmidt, n.d., 2008, Okoli & Pawlowski, 2004,) sprendimų priėmimo modelį. Autoriai pabrėžia Delphi metodo stipriąsias puses, įskaitant jo gebėjimą pasiekti sutarimą arba susitarimą tarp ekspertų grupės, lankstumą prisitaikant prie nuomonių pokyčių laikui bėgant ir gebėjimą visapusiškai suprasti sudėtingą problemą. Jie taip pat aptaria kai kuriuos Delphi metodo apribojimus, įskaitant galimą šališkumą ir sunkumus užtikrinti dalyvių anonimiškumą.

Autoriai daro išvadą, kad Delphi metodas yra vertingas tyrimo įrankis, kuris gali būti naudojamas norint gauti ekspertų nuomones įvairiomis temomis įvairiose srityse, įskaitant informaciją ir valdymą, inžineriją ir sveikatos priežiūrą. Jie rekomenduoja mokslininkams atidžiai apsvarstyti Delphi metodo dizainą ir įgyvendinimą, kad būtų užtikrintas gautų rezultatų pagrįstumas ir patikimumas.

Galima teigti, kad DELPHI metodas yra struktūrizuota komunikacijos technika, naudojama gauti ekspertų nuomones tam tikra tema. Tai yra grupinis sprendimų priėmimo procesas, apimantis anoniminių nuomonių rinkimą iš ekspertų grupės, naudojant kelis anketų etapus, siekiant sutarimo. Kiekvieno turo grįžtamasis ryšys naudojamas siekiant patikslinti klausimus ir pagerinti tolesnių turų rezultatų tikslumą, kol pasiekiamas patenkinamas susitarimo lygis. DELPHI metodas plačiai naudojamas tokiose srityse kaip prognozavimas, rizikos analizė ir politikos formavimas, ir yra laikomas patikimu būdu rinkti ir apibendrinti ekspertų nuomones.

Taikant DELPHI metodą buvo atlikti sekatys veiksmai:

- Apibrėžta ir paaiškinta tyrimo problema ir nustatytas tyrimo tikslas.
- Sudarytos keturios ekspertų grupės atskiriems problemoms aspektams ištirti.
- Kiekvienai grupei sudarytas atskiras klausimynas, kuriame iškelti klausimai, susiję su pagrindiniu tyrimo klausimu ir pritaikyti įvertinant grupės turimą ekspertizę. Nustatyti klausimai buvo aiškūs, glausti ir lengvai suprantami.
- Atskiras klausimynas išplatintas kiekvienai ekspertų grupei su prašymu anonimiškai pateikti savo nuomonę.

- Surinkti ir apibendrinti pirmojo turo atsakymai, nustatyti duomenų modeliai ir tendencijos.
- Pirmojo etapo rezultatai buvo pristatyti kiekvienam tyrimo dalyviui.
- Antras tyrimo turas buvo vykdomas naudojant MS Teams platformą. Naudojant “Baltos lentos” funkciją buvo kuriamas bendrai priimtinas problemos sprendimo minčių žemėlapis.
- Antro turo duomenys buvo išanalizuoti ir rezultatai apibendrinti, kad padaryti išvadas apie tyrimo klausimą.
- Tyrimo išvados buvo naudojamos hibridinių grėsmių elektroninėje erdvėje valstybės mastu modelio sudarymui.

Tyrimo tikslas - pasitelkiant ekspertų žinias, išsiaiškinti e. erdvėje kylančias hibridines grėsmes, jų poveikį valstybės kritinei infrastruktūrai, visuomenei ir nacionaliniam saugumui, nustatyti galimas atsako į hibridines grėsmes priemones.

Tyrimo uždaviniai:

- Išsiaiškinti ekspertų nuomonę apie valstybei kylančias hibridines grėsmes.
- Sužinoti ekspertų nuomonę apie tai, ar valstybėje egzistuojančių strateginių ir teisinių dokumentų visuma yra pakankama hibridinėms grėsmėms identifikuoti ir jas valdyti.
- Apibrėžti Vyriausybės vaidmenį identifikuojant ir valdant hibridines grėsmes.
- Išsiaiškinti, kokios didžiausios kibernetinės grėsmės kyla valstybei, jos kritinei infrastruktūrai ir visuomenei.
- Sužinoti veiksmingiausius atsako į kibernetines grėsmes metodus ir priemones.
- Apibrėžti hibridinių grėsmių poveikį visuomenei.
- Išsiaiškinti ekspertų nuomonę apie galimybes ir metodus valdyti hibridines grėsmes.
- Išskirti sutarta hibridinių grėsmių elektroninėje erdvėje valdymo modelį.

Tyrimo objektas - hibridinės grėsmės kylančios valstybei elektroninėje erdvėje ir jų valdymas

Grupių sudarymas ir ekspertų parinkimas

Tyrimui atlikti buvo sudarytos keturios ekspertų grupės:

Politikos grupė - 4 ekspertai;

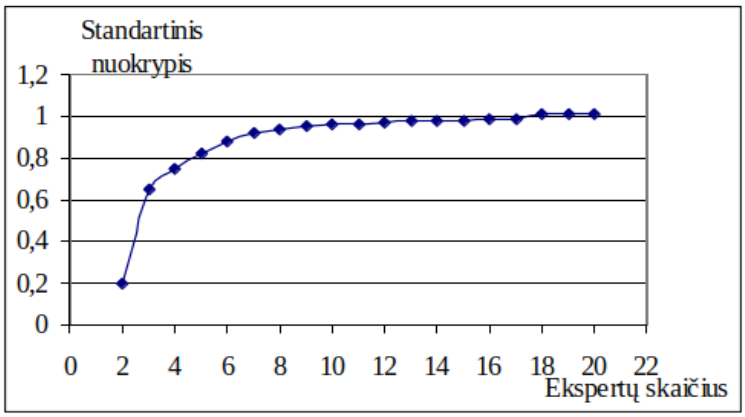
Kibernetinio saugumo grupė - 5 ekspertai;

Visuomenės informavimo grupė - 4 ekspertai;
Krizių valdymo grupė - 4 ekspertai;
Viso tyrime dalyvavo 17 ekspertų.

Ekspertų atrankai buvo naudotas netikimybinis atrankos tipas. Imtis - ekspertų imtis. Atrenkant ekspertus Delphi apklausai, buvo atsižvelgta į šiuos kriterijus: (Turoff & Linstone, 2002, Keeney et al., 1977, Rowe & Wright, 1999, Hsu & Sandford, 2007, Van de Ven & Delbecq, 1971)

- Atitinkama patirtis: ekspertai turi reikiamų žinių, įgūdžių ir patirties, susijusių su tyrimo klausimu.
- Pasiekiamumas: ekspertai nori ir gali dalyvauti apklausos procese.
- Reprezentatyvumas: ekspertų grupė įvairi ir reprezentuoja skirtingus požiūrius bei nuomones srityje, susijusioje su tyrimo klausimu.
- Prieinamumas: ekspertai yra lengvai pasiekiami ir apklausos procesas jiems yra patogus.
- Atsakingumas: ekspertai kurie greičiausiai atsakys į apklausą ir pateiks prasmingą informaciją.
- Tinkamas dydis: pagal tyrimo temą ir turimus išteklius buvo pasirinkta 17 ekspertų grupė. Paprastai daugumai Delphi apklausų pakanka maždaug 10–20 ekspertų grupės.

Pasirenkant ekspertų skaičių taip pat buvo vadovaujamasi metodologinėmis prielaidomis, suformuluotomis klasikinėje testų teorijoje. Teorija teigia, kad agreguotų sprendimų patikimumą ir priimančių sprendimą (šiuo atveju ekspertų) skaičių sieja greitai gęstantis netiesinis ryšys (žr. 16 pav.). Yra įrodyta, kad agreguotų ekspertinių vertinimo moduliuose su vienodais svoriais nedidelės ekspertų grupės sprendimų ir vertinimų tikslumas nenusileidžia didelės ekspertų grupės sprendimų ir vertinimų tikslumui (Libby, Blashfield, 1978; Baležentis, Žalimaitė, 2011).



Šaltinis: Baleţentis, Žalimaitė, 2011, p. 25

5 pav. Ekspertų vertinimų standartinio nuokrypio priklausomybė nuo ekspertų skaičiaus

Sprendimų ir vertinimų tikslumas yra pakankamai didelis, kai ekspertų skaičius pasiekia 9 ir daugiau, todėl 17 ekspertų pakanka gauti tiksliai informacijai. (G. Gulevičiūtė, 2013)

Klausimyno sudarymas:

Tyrimui buvo pasirinktas kombinuotas **kokybinis - kiekybinis metodas**. Toks kombinuotas metodų metodų derinys padeda giliau suprasti tyrimo problemą, įskaitant kintamųjų santykių supratimą ir išsamesnį sudėtingų reiškinių supratimą. Kiekybiniai tyrimai pateikia skaitinius duomenis ir statistinę analizę, o kokybiniai tyrimai suteikia išsamų supratimą ir kontekstą.

Kokybinių tyrimų taikytojai teigia, kad tokiu būdu gauti duomenys pateikia išsamesnę informaciją apie nagrinėjamą objektą, nei gauti kiekybiniais tyrimais (Tidikis, 2003, p. 357). Ekspertams asmeniškai buvo pateikta 11 klausimų anketa (žr. 1 priedą), su jais betarpiškai bendraujama su anketa susijusiais klausimais. Pateikta anketa atitinka bendruosius anketos reikalavimus (Kardelis, 2002, p. 93- 94):

- motyvuotai, logiškai paaiškinta, dėl ko atliekamas tyrimas, po to pateikta trumpa anketos užpildymo instrukcija;
- apklausiamojo pastangos atsakyti turi būti minimalios, todėl klausimai sugalvoti konkretūs, o atsakymų variantai suprantami;
- kuo mažiau respondentui tenka rašyti, tuo daugiau jis tiki, kad bus išlaikytas anonimiškumas, todėl tik pusė klausimų buvo atviri;

- svarbi anketos apimtis: ilga anketa tiriamąjį atbaido, nėra noro atidžiai ją skaityti, todėl galimi paviršutiniški atsakymai; svarbus ir anketos apipavidalinimas, klausimų kompozicija - tai gali sušvelninti kilusias neigiamas nuostatas - pasirinkta 10 klausimų anketa, stengtasi pateikti vienas su kitu susijusius klausimus;
- vengta klausimų, kurie stumia respondentą į vieną atsakymą - tam pateikta daug atsakymų variantų, jei nei vienas netinka, respondentai turėjo galimybę patys įrašyti tinkamiausią;
- respondentui palikta galimybė pagrįsti pasirinktą atsakymo variantą;
- vengta sudėtingų, erzinančių klausimų.

Klausimynui sudaryti ir apklausai atlikti buvo naudojama Google Forms platforma.

Ekspertų nuomonių suderinamumas:

Prieš pradedant analizuoti gautus duomenis buvo reikalinga išsiaiškinti ekspertų nuomonių

suderinamumą. „Dviejų ekspertų suderinamumą kiekybiškai gali įvertinti koreliacijos koeficientas. Jei ekspertų skaičius didesnis už du, grupės ekspertų suderinamumo lygį rodo konkordacijos koeficientas“ (Podvezko, 2005, p. 101- 102). Statistinio paketo socialiniams mokslams (SPSS) programa buvo apskaičiuotas Kendallo konkordacijos koeficientas. Tačiau ekspertų suderinamumas nebuvo apskaičiuotas atsižvelgiant į visus anketos klausimus, nes „<...> konkordacijos koeficientui skaičiuoti tinka tik ekspertų rodiklių rangavimas. Jei ekspertų vertinimai buvo bet kokio kitokio pavidalo, juos preliminariai reikia ranguoti“ (Podvezko, 2005, p. 102). 5 anketos klausimai yra nominalūs- jų kategorijų išdėstymas ar numeravimo tvarka gali būti bet kokia ir dėl to niekas nepasikeičia (Vaitkevičius, Saudargienė, 2006), kiti anketoje pateikti klausimai yra atviri, todėl jie neįtraukti skaičiuojant Kendallo konkordacijos koeficientą. Gautas Kendallo konkordacijos koeficientas: W= 0,707 (žr. 17 lent.).

		Kvadratų suma	df	Kvadratų vidurkis	Friedman'o Chi-Square	Patikimumo lygmuo
Tarp žmonių		4.259	8	.532		
Per žmones	Tarp element	46.759[a]	5	9.352	34.030	.000
	Likęs	15.074	40	.377		
	Iš viso	61.833	45	1.374		
Iš viso		66.093	53	1.247		

Šaltinis: Autoriaus skaičiavimai

2 lentelė Kendallo konkordacijos koeficiento skaičiavimas

Didžiausias vidurkis = 2.8704

a. Kendall'o konkordacijos koeficientas W = .707.

„Jei ekspertų nuomonės suderintos, konkordacijos koeficiento W reikšmė yra arti vieneto, jei vertinimai labai skiriasi- W reikšmė yra arti nulio“ (Podvezko, 2005, p. 102). Kadangi mano gautaskoeficientas yra arčiau vieneto, nei nulio, daroma išvada, kad ekspertų nuomonės yra pakankamai suderintos. (G. Gulevičiūtė, 2013)

1.1.1. Pirmo turo duomenų analizė

Politikos formavimo grupė

Politikos ekspertų grupę sudarė keturi respondentai. Ekspertams buvo pateikta anketu su dešimt klausimų siekiant įvertinti politikos, strateginių dokumentų, tarptautinio bendradarbiavimo ir pratybų ir mokymų įtaką ir reikšmę ruošiantis krizių, tame tarpe krizių elektroninėje erdvėje valdymui. Visų ekspertų patirtis politikos formavimo srityje buvo daugiau kaip penki metai. Gauti anketinės apklausos duomenys buvo apdoroti naudojant SPSS, grafikams buvo naudotas Libreoffice programinės įrangos paketas.

Ekspertų nuomonės sutapo vertinant politikos formavimo, strateginių dokumentų ir tarptautinio bendradarbiavimo svarbą valdant hibridines krizes.

Politikos formavimas, strateginiai dokumentai, tarptautinis bendradarbiavimas ir pratybos ir mokymai yra esminiai veiksniai, siekiant efektyviai tvarkyti hibridines krizes. Hibridinės

krizės yra sudėtingos ir daugiasluoksnės, dažnai apimančios konvencines ir nekonvencines taktikas, kuriomis valstybės ir nevalstybinės organizacijos siekia savo tikslų.

Pagrindiniai ekspertų teiginiai pateikiami žemiau.

Dominuojančios atsakymų temos	Atsakymų apibendrinimas
Aiškios hibridinių krizių valdymo politikos buvimas	Aiškios ir išsamios politikos buvimas yra būtina sąlyga, siekiant valdyti hibridines krizes. Politika suteikia gaires tiek sprendimų priėmėjams tiek kitoms suinteresuotoms šalims, kaip efektyviai reaguoti į krizę ir ją valdyti. Politika turi būti pakankamai lanksti, kad galėtų prisitaikyti prie sparčiai kintančios hibridinių grėsmių prigimties, tuo pačiu būdama išsami, kad apimtų visus krizės aspektus.
Strateginių dokumentų svarba	Strateginiai dokumentai yra svarbūs, nustatant bendrus tikslus ir uždavinius, siekiant valdyti hibridines krizes. Šie dokumentai nustato būdus, kaip reaguoti į krizę ir padeda užtikrinti, kad visos suinteresuotos šalys būtų sutelktos ir dirbtų siekiant bendro tikslo. Taip pat padeda nustatyti pagrindinius rizikos ir pažeidžiamumo veiksnius, kuriuos būtina pašalinti, siekiant efektyviai valdyti krizę.
Tarptautinis bendradarbiavimas	Hibridinės krizės dažnai yra tarpvalstybinio pobūdžio ir jas veiksmingai valdyti reikia aktyvaus ir veiksmingo tarptautinio bendradarbiavimo. Tarptautinis bendradarbiavimas gali būti įvairių formų, įskaitant dalijimąsi žvalgybos duomenimis ir informacija, atsakomųjų veiksmų koordinavimą ir paramos nukentėjusioms šalims teikimą. Kelių

	suinteresuotųjų šalių iš skirtingų šalių ir organizacijų įtraukimas gali padėti panaudoti išteklius, patirtį ir gebėjimus veiksmingiau spręsti krizę.

Šaltinis**:** Parengta autoriaus

3 lentelė Respondentų atsakymų suvestinė

Kita klausimų grupe buvo siekiama išsiaiškinti naujų, proveržio techonologijų, teisinio reglamentavimo svarbą siekiant identifikuoti galimas hibridines krizes.

Pagrindiniai ekspertų teiginiai pateikiami žemiau.

Dominuojančios atsakymų temos	Atsakymų apibendrinimas
Politikos formavimas	Norint išvengti hibridinių krizių, labai svarbu suformuluoti politikos reglamentus naujoms atsirandančioms technologijoms.
Naujų technologijų atpažinimas	Pirmasis žingsnis formuojant politikos nuostatas dėl naujų technologijų yra nustatyti, kurios technologijos yra naujos ir gali sukelti hibridines krizes. Tai apima tokias technologijas kaip dirbtinis intelektas, kvantinis skaičiavimas, blokų grandinė ir kt.
Naujų technologijų keliamų rizikų nustatymas	Nustačius naujas technologijas, svarbu atlikti rizikos vertinimą, siekiant nustatyti galimą riziką ir pažeidžiamumą, susijusį su jų naudojimu. Tai apima technologijos poveikio privatumui, saugumui ir kitoms pagrindinėms sritims įvertinimą.
Teisinis reguliavimas	Remiantis rizikos vertinimais, turėtų būti parengtos reguliavimo sistemos, užtikrinančios, kad naujos technologijos būtų naudojamos atsakingai ir neprisidėtų prie hibridinių krizių. Tai gali apimti

	taisykles, susijusias su duomenų privatumu, kibernetiniu saugumu ir kitomis sritimis.
Standardizacija	Atsižvelgiant į tai, kad naujos technologijos dažnai naudojamos tarpvalstybiniu mastu, svarbu nustatyti tarptautinius standartus siekiant užtikrinti, kad jie būtų naudojami atsakingai ir saugiai. Tarptautinis bendradarbiavimas ir bendradarbiavimas gali padėti plėtoti ir įgyvendinti šiuos standartus.
Naujų technologijų plėtros monitoringas	Besivystančioms technologijoms ir toliau tobulėjant, svarbu stebėti jų naudojimą ir prireikus pritaikyti politikos reglamentus, kad būtų išvengta hibridinių krizių. Tai apima nuolatinius rizikos vertinimus ir reguliavimo sistemų atnaujinimus, kai nustatomos naujos rizikos ir pažeidžiamumo vietos.

Šaltinis**:** Parengta autoriaus

4 lentelė Respondentų atsakymų suvestinė

Apibendrinant galima pasakyti, kad naujų naujų technologijų politikos reglamentai yra labai svarbūs siekiant užkirsti kelią hibridinėms krizėms. Identifikuodami naujas technologijas, atlikdami rizikos vertinimus, kurdami reguliavimo sistemas, nustatydami tarptautinius standartus, stebėdami ir prireikus pritaikydami, galime užtikrinti, kad šios technologijos būtų naudojamos atsakingai ir neprisidėtų prie hibridinių krizių.

Paskutiniu klausimų bloku buvo siekiamai išsiaiškiti pratybų ir mokymų svarbą siekiant valdyti hibridines grėsmes.

Dominuojančios atsakymų temos	Atsakymų apibendrinimas
Pratybų ir mokymų reikšmė	Mokymai ir pratybos padeda sustiprinti valstybės veikėjų ir suinteresuotųjų šalių pasirengimą veiksmingai reaguoti į hibridines krizes. Tai apima žinių, įgūdžių ir gebėjimų, reikalingų užkirsti kelią

	tokioms krizėms, sušvelninti ir atsigauti nuo jų, kūrimą.
Politikos ir procedūrų tikrinimas	Per mokymus ir pratybas galima nustatyti esamos politikos, procedūrų ir pajėgumų spragas ir trūkumus bei juos pašalinti. Tai padeda pagerinti bendrą pasirengimą ir užtikrinti, kad visi valstybės veikėjai efektyviai bendradarbiautų kartu valdydami hibridines krizes.
Sąveikos stiprinimas	Hibridinės krizės dažnai apima daugybę suinteresuotųjų šalių ir veikėjų iš skirtingų sektorių ir valdžios lygių. Mokymai ir pratybos padeda pagerinti šių suinteresuotųjų šalių koordinavimą ir bendravimą, įskaitant keitimosi informacija ir sprendimų priėmimo protokolų kūrimą.
Krizių valdymo planų tikrinimas	Mokymai ir pratybos suteikia galimybę išbandyti atsako planus ir nustatyti tobulinimo sritis. Tai apima reagavimo planų veiksmingumo patikrinimą pagal skirtingus scenarijus ir skirtingų suinteresuotųjų šalių veiklos vertinimą reaguojant į krizę
Pasitikėjimo stiprinimas	Mokymai ir pratybos padeda stiprinti valstybės veikėjų ir suinteresuotųjų šalių pasitikėjimą jų gebėjimu reaguoti į hibridines krizes. Tai apima pasitikėjimo ir bendradarbiavimo tarp įvairių suinteresuotųjų šalių kūrimą ir užtikrinimą, kad kiekvienas suprastų savo vaidmenį ir atsakomybę valdant krizę.

Šaltinis**:** Parengta autoriaus

5 lentelė Respondentų atsakymų suvestinė

Apibendrinant ekspertų teiginių galima daryti išvadą, kad mokymai ir pratybos strateginiu valstybės lygiu yra labai svarbūs ruošiantis valdyti hibridines krizes. Stiprindami pasirengimą, nustatydami spragas ir trūkumus, gerindami koordinavimą ir komunikaciją, išbandydami reagavimo planus ir kurdami pasitikėjimą, valstybės veikėjai ir suinteresuotosios šalys gali veiksmingai užkirsti kelią tokioms krizėms, sušvelninti jas ir atsigauti nuo jų.

Kibernetinio saugumo grupė:

Apklausos metu buvo siekiama išsiaiškinti kibernetinį saugumą valstybės mastu reglamentuojančių dokumentų, kritinę infrastruktūrą valdančių subjektų kibernetinio saugumo užtikrinimo svarbą hibridinių grėsmių prevencijai. Taip pat buvo siekiama priemonių spektrą siekiant gerinti kibernetinį saugumą valstybės mastu.

Dominuojančios atsakymų temos	Atsakymų apibendrinimas
Kritinės infrastruktūros kibernetinė sauga	Ypatingos svarbos infrastruktūros objektai, tokie kaip energetika, telekomunikacijos ir transporto sistemos, dažnai yra nukreipiami kibernetinių atakų metu. Kibernetinio saugumo taisyklės gali padėti apsaugoti šias sistemas nuo atakų ir užkirsti kelią esminių paslaugų sutrikimams.
Duomenų sauga	Kibernetinio saugumo taisyklės gali padėti užkirsti kelią duomenų pažeidimams, dėl kurių gali būti prarasta arba pavogta neskelbtina informacija. Šią informaciją piktybiški veikėjai gali panaudoti hibridinėms krizėms, pvz., dezinformacijos kampanijoms ar ypatingos svarbos infrastruktūros atakoms, vykdyti.
Naujos technologijos, naujos grėsmes	Kibernetinio saugumo taisyklės gali padėti spręsti kylančias grėsmes, pvz., kylančias dėl vis didėjančio dirbtinio intelekto ir daiktų interneto naudojimo. Taisyklės gali užtikrinti, kad šios technologijos būtų naudojamos saugiai ir atsakingai, o galimi pažeidžiamumai būtų nustatyti ir pašalinti.

Tarptautinis bendradarbiavimas	Kibernetinis saugumas yra pasaulinė problema, o valstybės lygmens reglamentai gali padėti pagerinti tarptautinį bendradarbiavimą ir bendradarbiavimą užkertant kelią kibernetinėms atakoms ir į jas reaguojant. Tai apima dalijimąsi informacija ir gerąja patirtimi, taip pat tarptautinių standartų ir gairių kūrimą.
Pasitikėjimo stiprinimas	Kibernetinio saugumo taisyklės gali padėti sukurti piliečių, įmonių ir kitų suinteresuotųjų šalių pasitikėjimą. Tai apima užtikrinimą, kad asmeninė informacija būtų apsaugota ir kad asmenys būtų tikri, kad jų duomenys naudojami saugiai ir atsakingai.

Šaltinis**:** Parengta autoriaus

6 lentelė Respondentų atsakymų suvestinė

Ekspertai išskyrė keleta būdų, kaip pagerinti kibernetinį saugumą valstybės lygiu:

Dominuojančios atsakymų temos	Atsakymų apibendrinimas
Kibernetinio saugumo politika	Reikėtų parengti visapusišką kibernetinio saugumo politiką, apimančią visus kibernetinio saugumo aspektus, įskaitant prevenciją, aptikimą, reagavimą ir atkūrimą. Politika turėtų būti reguliariai peržiūrima ir atnaujinama, kad būtų pašalintos kylančios grėsmės.
Didinti informuotumą apie kibernetinį saugumą	Stengtis didinti piliečių, įmonių ir kitų suinteresuotųjų šalių informuotumą apie kibernetinį saugumą. Tai apima švietimą ir mokymą apie geriausią kibernetinio saugumo praktiką, taip pat stiprių slaptažodžių, dviejų veiksnių autentifikavimo ir kitų saugumo priemonių skatinimą.

Stiprinti saugumo priemones	Reikėtų sustiprinti savo saugumo priemones, kad užkirstų kelią ir aptiktų kibernetines atakas. Tai apima ugniasienės, įsibrovimo aptikimo sistemų ir kitų saugumo technologijų diegimą, taip pat reguliarų pažeidžiamumo vertinimą.
Reagavimo į incidentus planai	Valstybė turėtų parengti reagavimo į incidentus planus, kuriuose būtų pateiktos aiškios gairės, kaip reaguoti į kibernetines atakas. Į planus turėtų būti įtrauktos pranešimo apie incidentus, paveiktų sistemų izoliavimo ir normalios veiklos atkūrimo procedūros.
viešojo ir privačiojo sektorių partnerystė	Valstybė turėtų skatinti viešojo ir privačiojo sektorių partnerystę, kad pagerintų kibernetinį saugumą. Tai apima bendradarbiavimą su įmonėmis, pramonės grupėmis ir kitomis suinteresuotosiomis šalimis, siekiant dalytis informacija ir geriausia praktika, taip pat plėtoti ir įgyvendinti kibernetinio saugumo iniciatyvas.
Investicijos į kibernetinio saugumo tyrimus ir plėtrą	Valstybė turėtų investuoti į kibernetinio saugumo tyrimus ir plėtrą, kad būtų pašalintos kylančios grėsmės ir sukurtos naujos technologijos bei priemonės kibernetiniam saugumui stiprinti.

Šaltinis**:** Parengta autoriaus

7 lentelė Respondentų atsakymų suvestinė

Apibendrinant galima teigti, kad kibernetinio saugumo reguliavimas valstybės lygiu yra labai svarbus siekiant užkirsti kelią hibridinėms krizėms. Saugant ypatingos svarbos infrastruktūrą, užkertant kelią duomenų pažeidimams, šalinant kylančias grėsmes, gerinant tarptautinį bendradarbiavimą ir didinant pasitikėjimą, reglamentai gali padėti užtikrinti, kad

skaitmeninė aplinka būtų saugi ir stabili, o piktavališki veikėjai negalėtų pasinaudoti pažeidžiamumu ir sukelti hibridines krizes.

Siekiant stiprinti valstybės kibernetinį saugumą reikia bendro požiūrio, apimančio politikos kūrimą, informuotumo didinimą, saugumo priemonių stiprinimą, reagavimo į incidentus planų kūrimą, viešojo ir privačiojo sektorių partnerystės skatinimą bei investicijas į mokslinius tyrimus ir plėtrą. Įgyvendindamos šias priemones, valstybės gali pagerinti savo kibernetinio saugumo laikyseną ir geriau užkirsti kelią kibernetinėms atakoms bei į jas reaguoti.

Visuomenės informavimo grupė:

Tyrimo metu siekiama išsiaiškinti ekspertų vertinimą dėl visuomenės informuotumo apie hibridines grėsmes bei jų keliamus iššūkius ir visuomenės informuotumo didinimo priemonių.

Tyrimo rezultatų apibendrinimas pateikiamas lentelėje.

Dominuojančios atsakymų temos	Atsakymų apibendrinimas
Visuomenės informuotumo lygis	Atrodo, kad plačioji visuomenė ir daugelis organizacijų vis labiau suvokia hibridinių ir kibernetinių grėsmių riziką ir galimas pasekmes. Pastaraisiais metais buvo įvykdyta daugybė didelio atgarsio sulaukusių kibernetinių atakų ir dezinformacijos kampanijų, kurios sulaukė didelio žiniasklaidos dėmesio ir visuomenės susirūpinimo. Šie incidentai išryškino kibernetinio saugumo ir informacinio karo svarbą ir paskatino didinti asmenų bei organizacijų sąmoningumą ir pasirengimą. Pavyzdžiui, Europos Sąjunga sukūrė Bendrą kovos su hibridinėmis grėsmėmis sistemą, kuri apima priemones, skirtas gerinti situacijos suvokimą, didinti atsparumą ir atgrasyti nuo galimų agresorių.
Švietimas ir mokymas	Vienas iš efektyviausių būdų didinti visuomenės informavimo lygį yra švietimas ir mokymas. Tai gali apimti pagrindinius kibernetinio saugumo informuotumo mokymus asmenims ir įmonėms, taip pat pažangesnius mokymus kibernetinio saugumo specialistams. Švietimo

	institucijos taip pat gali atlikti pagrindinį vaidmenį didindamos sąmoningumą ir supratimą apie hibridines ir kibernetines grėsmes, įtraukdamos kibernetinio saugumo temas į savo mokymo programas.
Visuomenės informavimo kampanijos	Ggali padėti didinti informuotumą apie hibridinių ir kibernetinių grėsmių riziką ir pasekmes. Šios kampanijos gali naudoti įvairias priemones, tokias kaip televizija, radijas ir socialinė žiniasklaida, kad pasiektų plačią auditoriją. Pranešimuose daugiausia dėmesio gali būti skiriama kibernetinės higienos svarbai, saugaus elgesio internete svarbai ir būtinybei sustiprinti kibernetinio saugumo priemones įmonėse ir organizacijose.
Bendradarbiavimas ir dalijimasis informacija	Vyriausybinių agentūrų, privataus sektoriaus, akademinės bendruomenės ir asmenų bendradarbiavimas gali būti veiksmingas didinant visuomenės informavimo apie hibridines ir kibernetines grėsmes lygį. Tai gali apimti dalijimąsi geriausia praktika, grėsmių žvalgyba ir technologiniais sprendimais, siekiant pagerinti kibernetinio saugumo priemones.
Reguliavimas ir politika	Įgyvendindamos kibernetinio saugumo įstatymą ir politiką, vyriausybė gali atlikti pagrindinį vaidmenį didindamos visuomenės informavimo lygį. Ši politika gali apimti privalomus pranešimus apie kibernetinius incidentus, duomenų apsaugos taisykles ir minimalius kibernetinio saugumo standartus įmonėms ir organizacijoms.
Partnerystė su žiniasklaida	Žiniasklaida gali atlikti lemiamą vaidmenį didinant visuomenės informuotumą hibridinių ir kibernetinių grėsmių klausimu. Bendradarbiavimas su žiniasklaidos

	priemonėmis, siekiant padidinti aprėptį kibernetinio saugumo klausimais, išryškinti geriausią praktiką ir dalytis ekspertų nuomonėmis, gali būti veiksmingas būdas įtraukti visuomenę ir padidinti jos informacijos lygį.

Šaltinis**:** Parengta autoriaus

8 lentelė Respondentų atsakymų suvestinė

Apibendrinant galima teigti, kad norint padidinti visuomenės informavimo apie hibridines ir kibernetines grėsmes lygį, reikia bendrų visų suinteresuotųjų šalių pastangų. Daugeliui asmenų ir organizacijų vis dar trūksta žinių ir išteklių, reikalingų veiksmingai apsisaugoti nuo šių pavojų. Visų pirma, mažos ir vidutinės įmonės (MVĮ) dažnai turi ribotą kibernetinio saugumo biudžetą ir gali neturėti patirties veiksmingai saugumo priemonėms įgyvendinti. Norint išspręsti šiuos iššūkius, bus svarbu, kad vyriausybės, pramonės lyderiai ir kibernetinio saugumo ekspertai dirbtų kartu, kad pagerintų visų visuomenės sluoksnių sąmoningumą ir pasirengimą. Tai gali apimti iniciatyvas teikti mokymus ir paramą MVĮ, taip pat pastangas skatinti didesnį tarptautinį bendradarbiavimą ir keitimąsi informacija.

Mokydami asmenis, didindami visuomenės sąmoningumą, skatindami bendradarbiavimą ir dalijimąsi informacija, įgyvendindami veiksmingą politiką ir bendradarbiaudami su žiniasklaidos priemonėmis, galime sukurti saugesnę ir atsparesnę skaitmeninę ateitį.

Krizių valdymo ekspertų grupė

Tyrimo metu buvo siekiama išsiaiškinti ekspertų nuomonę dėl galimų hibridinių grėsmių elektroninėje erdvėje valdymo metodų ir veikėjų.

Tyrimo metu buvo nustatyta kad ekspertai nemato esminio skirtumo tarp tradicinių hibridinių grėsmių ir hibridinių grėsmių kurios vystosi elektroninėje erdvėje valdymo. Iš esmės hibridinė grėsmė kibernetinėje erdvėje yra platesnės tradicinių hibridinių grėsmių pogrupis, apimantis kibernetines atakas kaip pagrindinį grėsmės elementą. Hibridinė grėsmė kibernetinėje erdvėje konkrečiai reiškia grėsmę, kuri savo tikslams pasiekti naudoja tradicinės karinės jėgos ir kibernetinių atakų derinį. Tokio tipo grėsmė gali būti susijusi su kibernetiniu šnipinėjimu, kibernetiniu sabotažu ar kitokiomis kibernetinėmis atakomis, kartu su fizinėmis atakomis ar kitomis karinės jėgos formomis.

Ekspertai įvardina šiuos pagrindinius hibridinės krizės elektroninėje erdvėje evoliucijos etapus:

- Ankstyvoji stadija: kibernetinis šnipinėjimas. Pirmosiomis dienomis valstybės naudojo kibernetinį šnipinėjimą siekdamos surinkti žvalgybos informaciją apie kitas valstybes, dažnai naudodamos pažangias nuolatines grėsmes (APT), kad įsiskverbtų į vyriausybę ir karinius tinklus. Šiame etape buvo įvykdyta daug valstybės remiamų atakų, nukreiptų į kritinę infrastruktūrą, intelektinę nuosavybę ir kitus jautrius duomenis.
- Tarpinis etapas: Informacinės operacijos – Internetui tapus vis dažniau, valstybės pradėjo jį naudoti kaip informacijos operacijų įrankį. Šiame etape padaugėjo dezinformacijos kampanijų, propagandos ir kitų taktikos, kuriomis siekiama paveikti viešąją nuomonę ir formuoti pasakojimą apie konkrečias problemas.
- Aktyvusis etapas: hibridinis karas – aktyviajame etape valstybės naudoja kibernetines atakas kaip platesnių hibridinio karo strategijų dalį, kuriose karinė jėga derinama su nekarinėmis priemonėmis, tokiomis kaip propaganda, ekonominis spaudimas ir kibernetinės atakos. Šiam etapui būdingas ribos tarp karinių ir nekarinių sričių, nes valstybės naudoja kibernetines atakas, kad sutrikdytų svarbiausią infrastruktūrą, vykdytų sabotažą, sėtų sumaištį ir chaosą.
- Krizės pabaiga ir atsistatymas po krizės - šis etapas ypač svarbus kadangi sudaro sąlygas pritaikyti krizės metu išmoktas pamokas ir pereiti į kokybiškai aukštesnį pasirengimo sękančiai krizei lygį.

Ekspertai įvardina visą eilę pagrindinių veikėjų, dalyvaujančių hibridiniame krizių valdyme valstybės lygiu, įskaitant:

- Nacionalinė saugumo taryba (NSC): NSC yra atsakinga už valstybės vadovo konsultavimą nacionalinio saugumo ir užsienio politikos klausimais bei už vyriausybės atsako į krizes koordinavimą. Hibridinių grėsmių kontekste NSC atliktų pagrindinį vaidmenį kuriant ir įgyvendinant visapusišką krizių valdymo strategiją.
- Gynybos ir žvalgybos agentūros: Gynybos ir žvalgybos agentūros yra atsakingos už galimų grėsmių nustatymą ir stebėjimą, taip pat reagavimo strategijų kūrimą ir įgyvendinimą. Hibridinių grėsmių kontekste šioms agentūroms būtų pavesta aptikti ir reaguoti į kibernetines atakas, dezinformacijos kampanijas ir kitas netradicines karo formas.
- Teisėsaugos agentūros: teisėsaugos institucijos yra atsakingos už nusikalstamos veiklos, įskaitant elektroninius nusikaltimus, tyrimą ir patraukimą baudžiamojon atsakomybėn.

Hibridinių grėsmių kontekste teisėsaugos institucijos dalyvautų tiriant kibernetines atakas ir kitas nusikalstamos veiklos formas, kurios gali būti naudojamos hibridiniam karui palaikyti.

- Civilinės agentūros: civilinės agentūros, pvz., ekstremalių situacijų valdymo, visuomenės sveikatos ir infrastruktūros apsaugos agentūros, atliktų svarbų vaidmenį reaguojant į hibridines krizes, ypač susijusias su fizine infrastruktūra arba visuomenės saugumu.
- Privatus sektorius. Privatus sektorius, ypač įmonės, eksploatuojančios ypatingos svarbos infrastruktūrą arba teikiančios esmines paslaugas, taip pat būtų įtrauktos į hibridinį krizių valdymą. Privataus sektoriaus organizacijoms reikėtų glaudžiai bendradarbiauti su vyriausybinėmis agentūromis, kad galėtų keistis informacija ir koordinuoti atsaką į grėsmes.

Ekspertų vertinimu reikalingi šie pagrindiniai elementai norint sėkmingai valdyti hibridines grėsmes:

- Išsamus grėsmių įvertinimas: visapusiškas ir nuolatinis grėsmių vertinimas yra labai svarbus veiksmingam krizių valdymui. Tai apima galimų grėsmių nustatymą ir stebėjimą, grėsmės pobūdžio supratimą ir galimo grėsmės poveikio įvertinimą.
- Daugelio suinteresuotųjų šalių koordinavimas: norint veiksmingai valdyti hibridinę krizę, reikia koordinuoti ir bendradarbiauti tarp daugelio suinteresuotųjų šalių, įskaitant vyriausybines agentūras, privataus sektoriaus organizacijas ir pilietinės visuomenės grupes. Šis koordinavimas turi būti gerai suplanuotas ir gerai atliktas, turi būti aiškios komunikacijos linijos ir bendras kiekvienos suinteresuotosios šalies vaidmenų ir atsakomybės supratimas.
- Greitojo reagavimo pajėgumai: norint veiksmingai valdyti hibridinę krizę, būtini greitojo reagavimo pajėgumai. Tai apima gebėjimą greitai aptikti grėsmes ir į jas reaguoti, taip pat gebėjimą greitai sutelkti išteklius ir darbuotojus reaguojant į krizę.
- Atspari ypatingos svarbos infrastruktūra: ypatingos svarbos infrastruktūros, pvz., energijos, transporto ir ryšių sistemos, dažnai yra skirtos hibridinėms atakoms. Kritinės infrastruktūros atsparumo užtikrinimas yra būtinas veiksmingam krizių valdymui, įskaitant galimybę greitai atkurti paslaugas atakos atveju.
- Kibernetinės gynybos pajėgumai: kibernetinės gynybos pajėgumai yra labai svarbūs veiksmingam hibridinės krizės valdymui, nes kibernetinės atakos dažnai yra pagrindinė

hibridinio karo sudedamoji dalis. Tai apima galimybę aptikti ir reaguoti į kibernetines atakas, taip pat galimybę apsaugoti jautrius duomenis ir tinklus nuo neteisėtos prieigos.

- Visuomenės komunikacija ir informuotumas: veiksminga komunikacija ir informuotumo didinimas yra būtini norint valdyti hibridinę krizę, įskaitant galimybę greitai skleisti tikslią informaciją visuomenei ir suinteresuotosioms šalims, taip pat gebėjimą valdyti visuomenės suvokimą ir reagavimą į krizę.

Apibendrinant verta paminėti, kad hibridinės krizės elektroninėje erdvėje raidos etapai ne visada yra linijiniai ir kad valstybė gali vienu metu naudoti kelias taktikas arba jas keisti priklausomai nuo savo tikslų ir situacijos vietoje. Tačiau apskritai hibridinių grėsmių evoliucija elektroninėje erdvėje valstybės lygmeniu pasižymėjo nuolatiniu kibernetinių atakų sudėtingumo ir masto didėjimu, taip pat jų integravimu į platesnes valstybinio valdymo strategijas.

Veiksmingas hibridinės krizės valdymas reikalauja visapusiško ir daugialypio požiūrio, apimančio daugelio suinteresuotųjų šalių koordinavimą ir bendradarbiavimą, taip pat gebėjimą greitai aptikti grėsmes, į jas reaguoti ir atsigauti nuo jų.

Veiksmingam hibridiniam krizių valdymui reikalingas glaudus visų šių veikėjų bendradarbiavimas, aiškios komunikacijos linijos ir gerai koordinuotas reagavimo planas.

Pirmo turo duomenų apibendrinimas

Remiantis keturių ekspertų grupių apklausos rezultatais buvo parengta raktinių teiginių koreliacijos matrica. Koreliacijos matrica siekiama nustatyti raktinių faktorių susijusių su hibridinių krizių valdymu koreliacija tarp atskirų espetų grupių siekiant įvertinti kiekvieno raktinio teiginio išvestinę svarbą hibridinių krizių valdyme.

Keletas mokslinių tyrimų parodė raktinių žodžių analizės svarbą tyrimuose. Pavyzdžiui, (Ayanso et al., 2011) nustatė, kad raktinių žodžių analizė buvo veiksmingas būdas nustatyti kylančias temas ir tendencijas tam tikroje tyrimų srityje. Kitas tyrimas, kurį atliko (Avoine et al., 2014) naudojo raktinių žodžių analizę, kad nustatytų elektroninių nusikaltimų modelius internetiniuose forumuose.

Apibendrinant galima teigti, kad raktinių žodžių arba raktinių frazių analizė yra svarbi mokslininkų priemonė, teikianti daugybę privalumų nustatant tendencijas ir modelius, gerinant paieškos rezultatus, gerinant turinio kūrimą ir remiant duomenų analizę.

Raktinių teiginių vertinimui matricoje naudojami du kiekybiniai parametrai:

- pirmas skaičius - raktinio teiginio naudojimas respondentų atsakymuose;

- Antras skaičius - raktinio teiginio pasikartojimo vidurkis respondetnų atsakymuose. Vidurkis n apskaičiuotas pagal formulę $n=\sum(m)/r$, kur m - raktinių teiginių pasikartojimo skaičius visų respondentų atsakymuose, r - respondentų skaičius grupėje.

Tekstų analizei atlikti buvo naudojama awk tekstų manipuliacijos programa taikant autoriaus sukurus teksto analizės parametrus: *awk '/search_pattern/ {action_to_take_on_matches; another_action;}' file_to_parse.*

Raktiniai teiginiai	Politika	Kibernetinis saugumas	Visuomenės informavimas	Krizių valdymas	Raktinio teiginio svarbos skaitmeninė išraiška
Krizių valdymo politika, strateginiai dokumentai, planai	4[11.75]	5[7]	4[4.25]	4[8.65]	17[31.65]
Technologijų plėtra, keliamų grėsmių įvertinimas, moksliniai tyrimai	3[6.75]	5[12.25]	2[2.25]	2[5.25]	12[26.5]
Tarptautinis bendradarbiavimas	4[9.75]	5[7]	3[4.75]	4[8.75]	16[30.25]
Informacijos rinkimas, dalijimasis informacija	4[10.25]	4[12]	3[3.75]	4[7]	15[33]
Sąveika (tarpžinybinė, valstybinis/privatus sektorius, valstybė/visuomenė)	4[8.75]	4[7.55]	2[1.75]	4[9.25]	14[27.3]
Kibernetinis saugumas (valstybės, kritinės infrastruktūros)	4[8]	5[11.75]	3[1]	4[7.25]	14[28]
Informuotumo didinimas	3[2.55]	4[3.25]	4[10.25]	3[7.75]	14[23.5]

Pratybos ir mokymai	3[5.25]	4[5]	4[3.75]	4[8.75]	15[22.75]

Šaltinis**:** Parengta autoriaus

9 lentelė Respondentų atsakymų kiekybinė analizė

Apibendrinant galima teigti, kad atlikus raktinių teiginių analizę išryškėjo, kad respondentų nuomone norint sėkmingai valdyti hibridines krizes elektroninėje erdvėje reikia reikia atkreipti ypatingą dėmesį į galimybę ir priemones užtikrinant dalijimasi informacija tarp visų veikėjų, krizių valdymo politikos ir reglamentuojančių ir politikas įgyvendinačių dokumentų rengimą. Svarbų vaidmenį atlieka tarptuatinis bendradarbiavimas ir bendras valsytibės kibernetinio saugumo lygis.

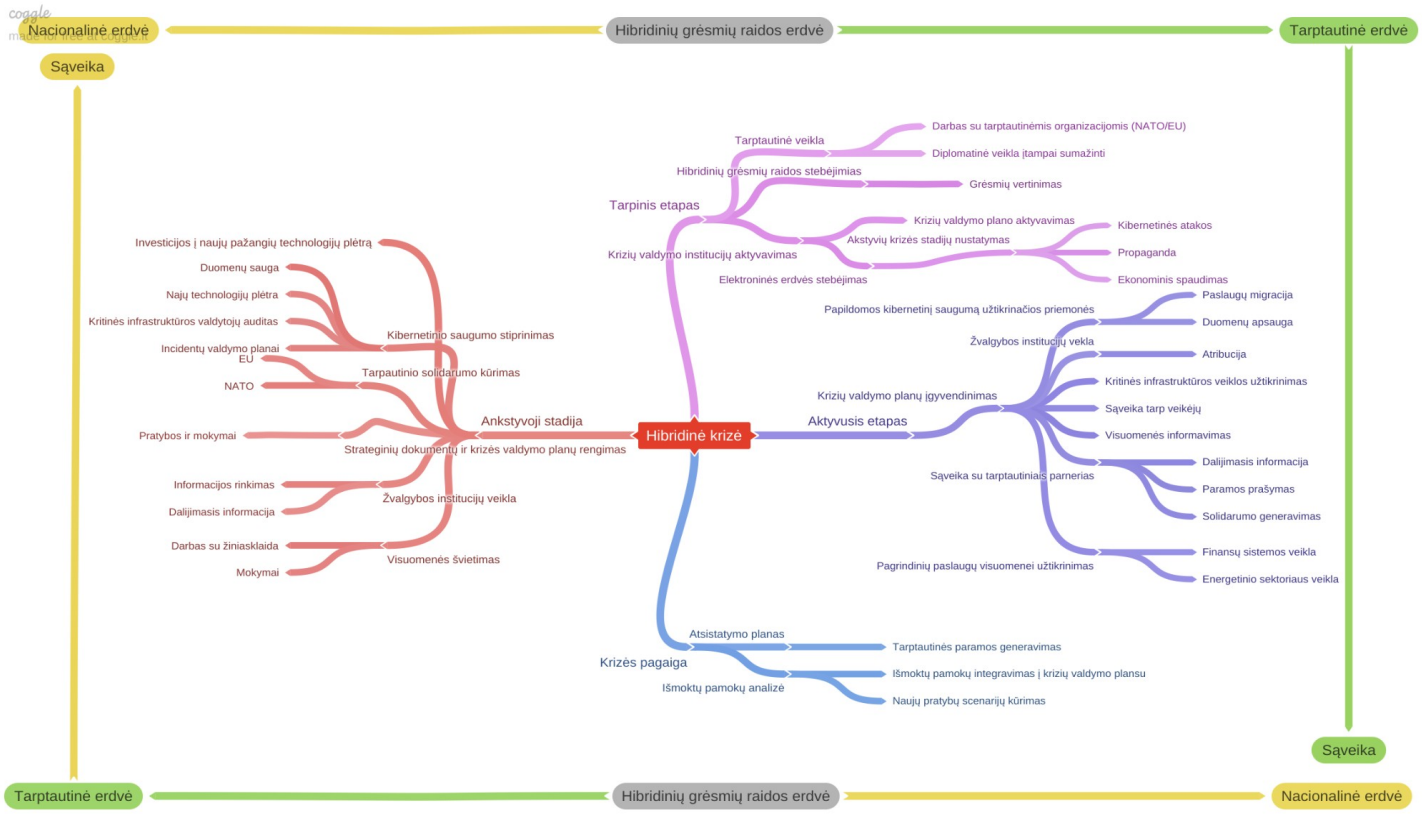
Primame, DELFI metodu įgalinto, tyrimo ture gauti rezultatai naudoti kartu su ekspertų grupe sudarant minčių žemėlapį hibridinių krizių elektroninėje erdvėje modeliui sukonstruoti.

2.2.2 Antro turo duomenų analizė

Minčių žemėlapių sudarymas yra naudingas įrankis sudėtingoms idėjoms, sistemoms ar procesams modeliuoti (Buzan, 2018, Novak & Gowin, 1984,). Minčių žemėlapio sudarymui, kartu su bendra ekspertų grąupe buvo atlikti šie žingsniai.

- Nustatyta modeliavimo tema - hibridinių krizių elektroninėje erdvėje valdymo modelis.
- Nustatyti pagrindiniai komponentai - keturi krizės raidos etapai.
- Diskusijos metu pridėtos papildomos minčių žemėlapio šakos. Kiekviena šaka išplėtė keturis krizės raidos etapus.
- Prie kiekvienos šakos buvo pridėta papildoma detali informacija atsižvelgiant į pirmo turo rezultatus.
- Atskiros minčių žemėlapio šakos buvo sujungtos parodant sąveiką.
- Diskusijos pabaigoje minčių žemėlapis buvo peržiūrėtas atlliean pataisisymus ir patobulinimus.

Diskusijai su ekspertais organizuoti ir minčių žemėlapiui kurti buvo naudojama programinės įrangos MS Teams “baltosios lentos” funkcija. Grafinė minčių žemėlapio adaptacija buvo atlikta Coggle programinės įrangos pagalba.



Šaltinis**:** Parengta autoriaus

6 pav. Respondentų minčių žemėlapis

Gautas minčių žemėlapis sukūrė vaizdinį hibridinių krizių valdymo elektroninėje erdvėje modelio vaizdinį kurio pagrindu buvo sudarytas siūlomas hibridinių grėsmių elektroninėje erdvėje valstybės mastu valdymo modelis.

2.2.3 Tyrimo išvados

Keturios apklaustų ekspertų grupės padarė panašias išvadas. Politikos formavimas, strateginiai dokumentai, tarptautinis bendradarbiavimas, pratybos ir mokymai laikomi esminiais hibridinių krizių valdymo veiksniais. Kibernetinio saugumo taisyklės valstybės lygmeniu yra būtinos siekiant užkirsti kelią hibridinėms krizėms, ypač siekiant apsaugoti kritinę infrastruktūrą, užkirsti kelią duomenų pažeidimams ir sušvelninti kylančias grėsmes. Visuomenės informavimas ir informuotumo didinimas yra labai svarbūs didinant visuomenės informuotumą apie hibridines ir kibernetines grėsmes, ypač mažoms ir vidutinėms įmonėms, kurioms gali trūkti kibernetinio saugumo biudžetų ir patirties.

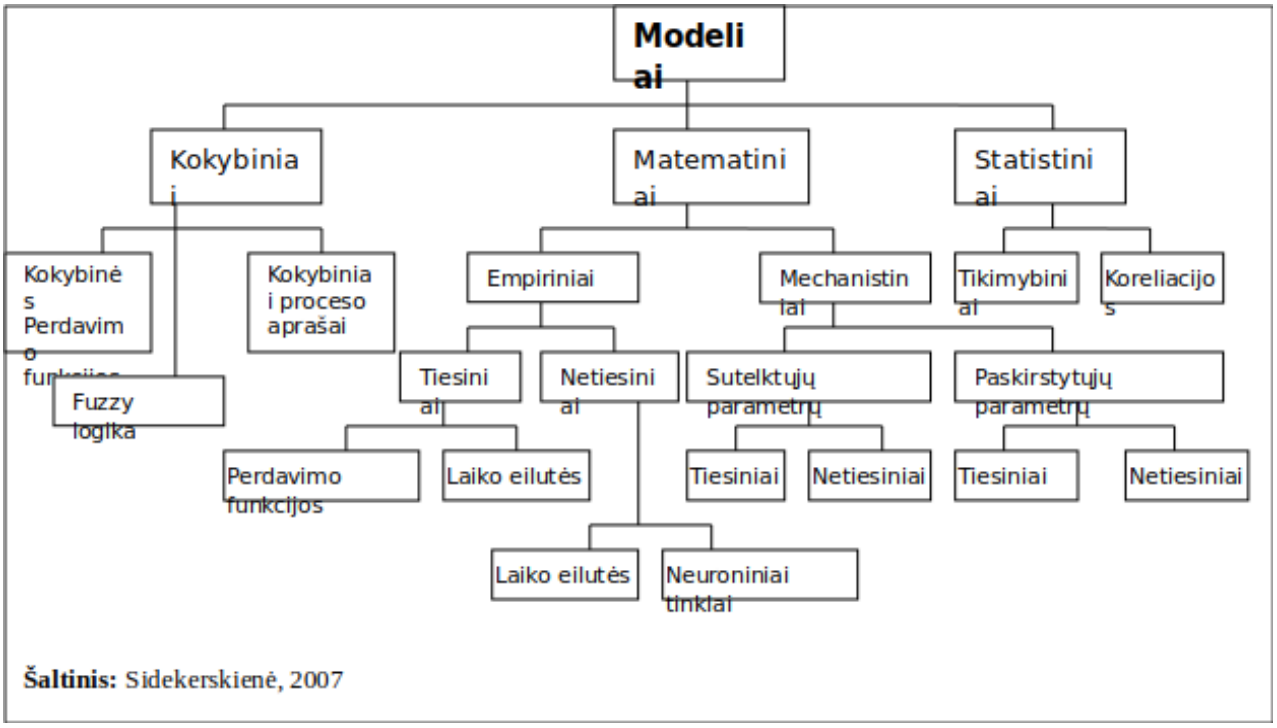
Ekspertai taip pat nemato esminio skirtumo tarp tradicinių hibridinių grėsmių valdymo ir tų, kurios vystosi virtualioje erdvėje. Jie nustato šiuos pagrindinius hibridinės krizės kibernetinėje

erdvėje etapus: ankstyvoji stadija (kibernetinis šnipinėjimas), tarpinis etapas (informacinės operacijos), aktyvioji fazė (hibridinis karas) ir krizės pabaiga bei atsigavimas po krizės. Galiausiai ekspertai nustato daugybę pagrindinių veikėjų, dalyvaujančių hibridiniame krizių valdyme valstybės lygiu, įskaitant Nacionalinį saugumo tarybą, gynybos ir žvalgybos agentūras bei kibernetinio saugumo ekspertus.

3. HIBRIDINIŲ GRĖSMIŲ E. ERDVĖJE VALSTYBĖS MASTU VALDYMO MODELIO KŪRIMAS

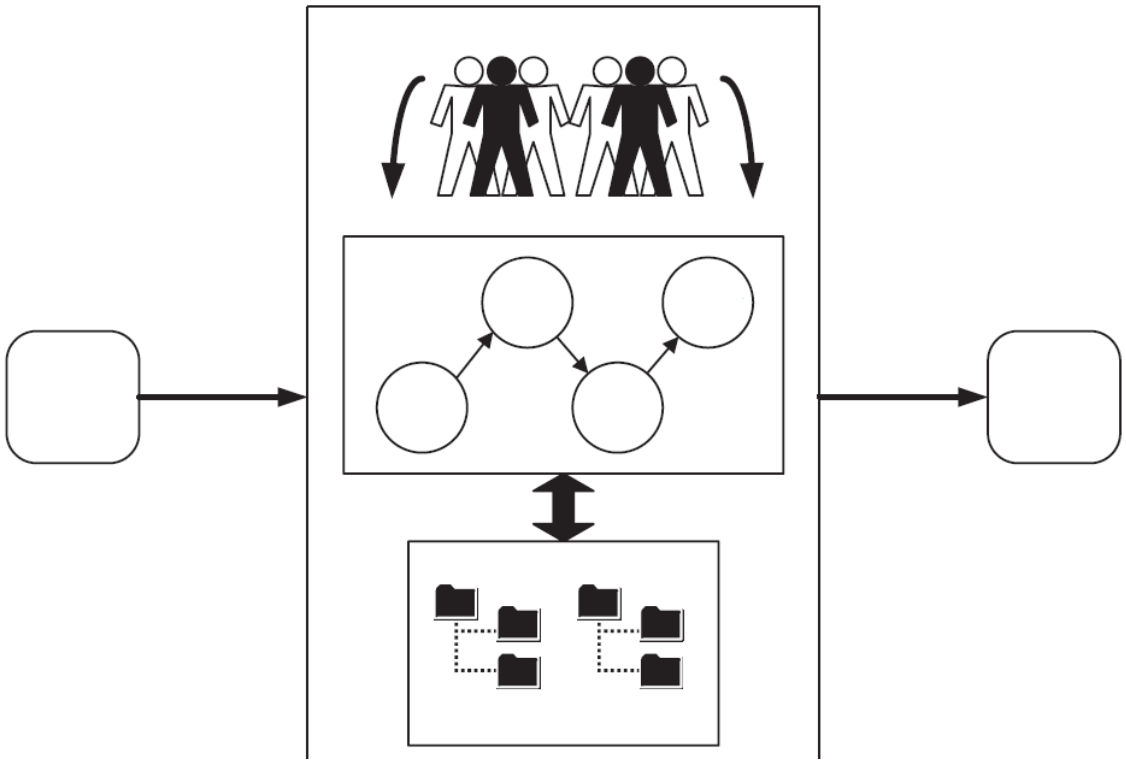
2.1 Metodologija

Atlikus hibridinių grėsmių valstybės mastu analizę siūlomas jų valdymo modelis. Modeliai gali būti skirstomi į matematinius, statistinius ir kokybinius (žr. 7 pav.) (Sidekerskienė, 2007, G. Gulevičiūtė, 2013).



Šaltinis: Siderskienė, 2007
7 pav. Modelių klasifikacija

Šiuo atveju kuriamas kokybinis modelis pasinaudojant kokybiniais proceso aprašais. Kuriant bet kokį modelį, galioja tam tikros taisyklės. Kiekvienas modelio veiklos procesas yra nepriklausomas, bet gali veikti kartu su kitais procesais. Kiekvieną procesą sudaro tam tikri resursai, veikla, bei informacija. Svarbu nustatyti modelio įeigą ir išeigą. Jokia veikla neprasidės be įeigos, tuo tarpu išeiga yra modelio rezultatas (žr. 24 pav.) (Aytulun, Guneri, 2008, G. Gulevičiūtė, 2013).



Šaltinis: Aytulun, Guneri, 2008, p. 2745.

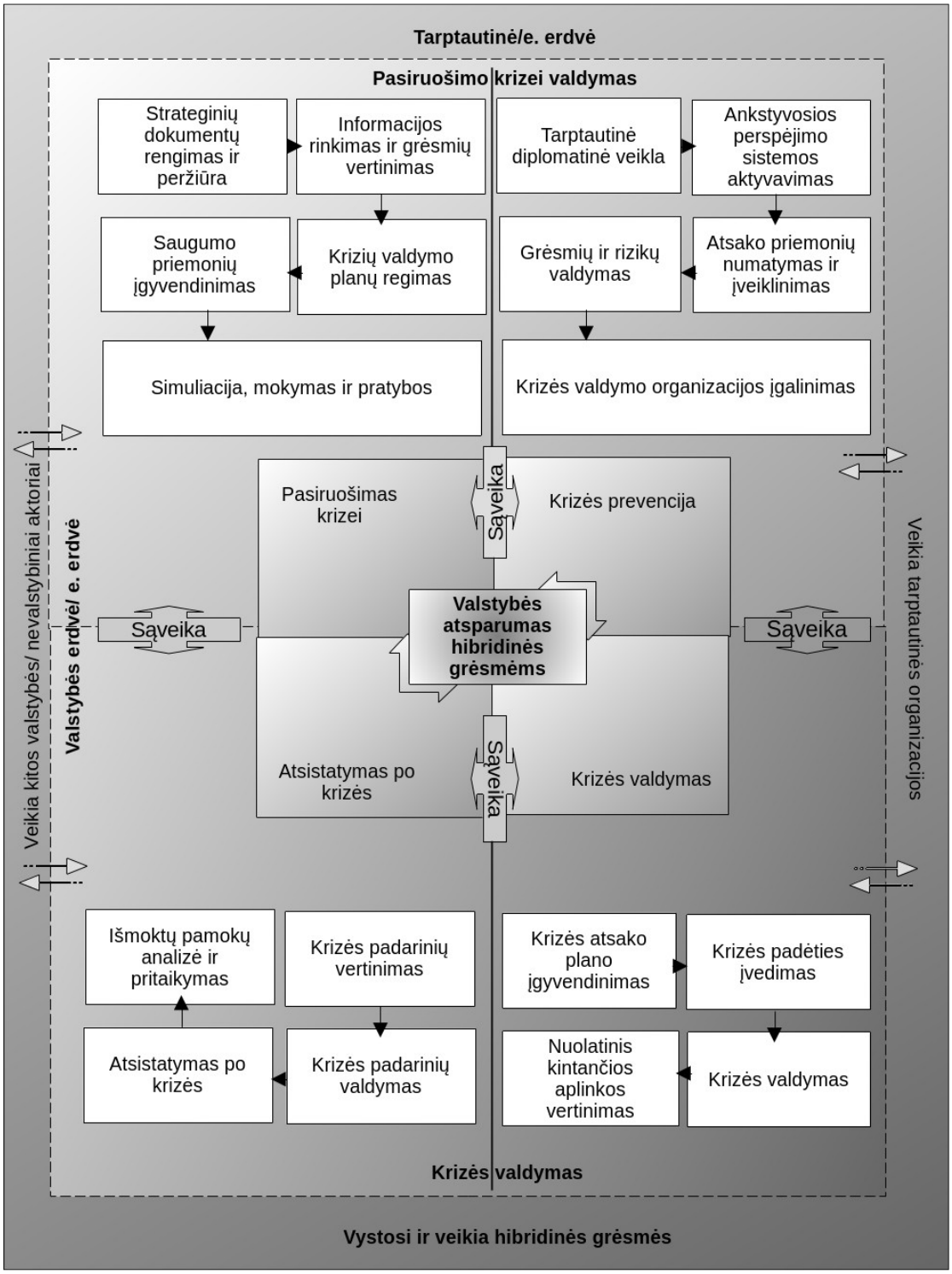
8 pav. Modelio sandara ir sąveika

Hibridinių grėsmių ir jų sukeltų krizių valdymo modelis – tai koncepcinė sistema, apimanti visus pasirengimo krizei, jos prevencijos, įveikos ir atsigavimo nuo jos aspektus. Vertinant įvykius per modelį, hibridinių krizių valdymas įgyja kontekstą ir sukuria sąlygas pritaikyti gerąsias praktikas.

Modeliui sudaryti buvo adaptuotas Reliacinis krizių valdymo modelis. (Jaques, 2007, Teo et al., 2017) Reliacinis krizių valdymo modelis yra teorinė sistema, paaiškinanti, kaip organizacijos ir suinteresuotosios šalys sąveikauja viena su kita krizės metu. Modelis teigia, kad krizių valdymas yra santykių procesas, kai vienos suinteresuotosios pusės atsakymai įtakoja kitų veiksmus ir suvokimą. Pagal šį modelį krizių valdymas yra dinamiškas procesas, apimantis

daugybę suinteresuotųjų šalių, įskaitant paveiktą organizaciją, žiniasklaidą, vyriausybines agentūras ir plačiąją visuomenę. Kiekviena iš šių suinteresuotųjų šalių turi savo interesus, tikslus ir motyvus, o krizės metu jos sąveikauja viena su kita kompleksiškai. Reliacinis modelis pabrėžia suinteresuotųjų šalių bendravimo ir dalijimosi informacija svarbą efektyviame krizių valdyme. Jame siūloma, kad organizacijos turėtų aktyviai bendradarbiauti su suinteresuotosiomis šalimis ir laiku teikti tikslią informaciją, kad sukurtų bendrą informacinį lauką, skatintų pasitikėjimą ir bendradarbiavimą. Savo ruožtu suinteresuotosios šalys gali teikti vertingą grįžtamąjį ryšį ir paramą, kuri gali padėti organizacijoms veiksmingiau reaguoti į krizę. Modelis suteikia išsamų vaizdą apie tarpusavyje susijusius ir sudėtingus santykius, atsirandančius krizės metu, ir pabrėžia visų suinteresuotųjų šalių bendradarbiavimo ir bendravimo svarbą sėkmingam krizių valdymui. (Pearson & Clair, 1998, Jaques, 2007, Pearson & Mitroff, 1993)

Modelio schematinis vaizdavimas



Šaltinis**:** Parengta autoriaus

9 pav. Hibridinių krizių valdymo e. erdvėje valdymo modelis

Aprašytomis taisyklėmis ir remiantis mokslinės literatūros ir strateginių dokumentų analize bei atliktų empirinių tyrimų duomenims sukonstruotas hibridinių krizių e. Erdvėje valstybės mastu valdymo ir vertinimo modelis. Modelis sudaro prielaidas hipotezei, kad hibridinės grėsmės elektroninėje erdvėje sukurdamos daugybę destabilizuojančių padarinių, galinčių iššaukti krizę valstybėje gali būti valdomos taikant elektroninei erdvei adaptuotą tradicinių krizių valdymo modelį.

2.2 Modelio analizė

Modelio grafinė konstrukcija įgalina aiškiai suvokti hibridinių krizių valdymą valstybės mastu kaip ciklinį procesą. Šis modelis yra apibendrinantis tiriamą reiškinį - hibridinių grėsmių valdymą valstybėje ir sukonstruotas adaptuojant mokslinėje literatūroje aprašomus modelius. Modelio dizaine taip pat remiamasi autoriaus įžvalgomis ir empirinio tyrimo rezultatais.
Modelį paaiškinančios struktūrinės dalys (žr. 9 pav.)

- Tarptautinė erdvė ir susisisiejanti valstybės erdvė (gali būti e. Erdvė kurioje vystosi hibridinė krizė).
- Pasiruošimo krizei etapas ir procesai.
- Krizės prevencijos etapas ir procesai.
- Krizės valdymo etapas ir procesai.
- Atsistatymo po krizės etapas ir procesai.
- Išmoktų pamokų integracija (proceso tobulinimas, ciklišKumas).
- Sąveika tarp valstybės ir tarptautinės erdvės (tarptautinis bendradarbiavimas).
- Sąveika tarp atskirų etapų, procesų ir veikėjų (procesų tobulinimas).
- Valstybės atsparumo didinimas (kiekvienos naujos modelio taikymo iteracijos metu, spiralinis ciklišKumas).

Modeliu siekiama išryškinti ciklišKumą, kurį apibūdina nenutrūkstama sąveika tarp kiekvieno krizės valdymo etapą. Sėkmingai suvaldžius viena hibridinę krizę gali prasidėti kita tačiau valstybės atsparumas ir pasiruošimas atremti naują krizę bus kokybiškai padidėjęs. Modeliu taip

pat siekiama akcentuoti elektroninės erdvės integralumą t.y. Valstybės erdvė yra integrali tarptautinės erdvės dalimi todėl pokyčiai ar krizės vienoje erdvėje betarpiškai įtakoją kitą.

Hibridinė krizė gali prasidėti tarptautinėje erdvėje ir iššaukti ar turėti padarinių valstybės elektroninėje erdvėje tiek ir prasidėti valstybės erdvėje ir peraugti į tarptautinę krizę. Modelis suskirstytas į du periodus: pasiruošimo krizei valdymo ir krizės valdyom periodai. Pasiruošimo krizei periodą sudaro du etapai: pasiruošimo krizei ir krizės prevencijos etapas. Antrą periodą sudaro du sekantys etapai: krizės valdymas ir atsistatymas po krizės.

Pasiruošimo krizei etape, akcentuojama tarptautinio bendradarbiavimo svarba, informacijos rinkimo ir grėsmių vertinimo bei strateginių dokumentų, įgalinančių krizės atpažinimą ir valdymą svarba. Pagrindiniai dokumentai galėtų būti:

- Nacionalinio saugumo strategija.
- Grėsmių valstybei vertinimas
- Nacionalinė kibernetinio saugumo strategija ir kibernetinio saugumo įstatymas.
- Nacionalinis krizių valdymo planas.
- Nacionalinis incidentų valdymo planas.
- Žvalgybos įstatymas.
- Tarptautinio ir dvišalio bendradarbiavimo susitarimai, t.t.

Pasiruošimo krizei etape atliekamas pasirengimo vertinimas, mokymai ir pratybos, vykdomos visuomenės informavimo ir kibernetinio raštingumo kampanijos, vertinamos rizikos, kuriami scenarijai, gali būti taikomas imitacinis modeliavimas.

Krizei eskaluojantis pereinama į krizės prevencijos etapą. Šis etapas akcentuoja aktyvios diplomatinės veiklos svarbą siekiant sustabdyti krizės eskalaciją. Tuo pačiu aktyvuojama, iš anksto numatyta, ankstyvoji perspėjimo apie krizę sistema, aktyvuojamos struktūros gebančios reaguoti ir atremti hibridines grėsmes, sudaromas arba aktyvuojamas esantis krizių valdymo padalinys.

Veiksmingas pasirengimas krizei apima visapusišką ir proaktyvų požiūrį, kuriuo siekiama užkirsti kelią arba sumažinti krizės poveikį valstybės veiklai, reputacijai ir suinteresuotosioms šalims. Taikoma keletas svarbiausių pasirengimo krizei žingsnių:

- Rizikos vertinimas: sistemingai vertinkite galimą riziką ir grėsmes, kurios gali sukelti krizę, pvz., stichinių nelaimių, kibernetinių atakų, finansinio sukčiavimo ar žalos

reputacijai. Nustatykite kiekvienos rizikos tikimybę ir galimą poveikį ir suskirstykite joms prioritetus pagal jų sunkumą ir dažnumą.

- Krizių planavimas: Sukurkite išsamų krizių valdymo planą, kuriame būtų išdėstyti kiekvieno krizių valdymo komandos nario vaidmenys ir atsakomybė, komunikacijos protokolai, sprendimų priėmimo procesai ir ištekliai, reikalingi reaguoti į krizę. Siekiant užtikrinti jo veiksmingumą, planas turėtų būti reguliariai atnaujinamas ir išbandomas atliekant modeliavimą ir pratimus ant stalo.
- Krizių komunikacija: sukurkite aiškią ir veiksmingą komunikacijos strategiją, kurioje būtų nurodyta, kaip bendrauti su vidinėmis ir išorinėmis suinteresuotosiomis šalimis krizės metu. Strategija turėtų apimti ryšių su žiniasklaida, socialinės žiniasklaidos, darbuotojų bendravimo ir komunikacijos su klientais protokolus. Apmokykite pagrindinius darbuotojus, kaip veiksmingai bendrauti krizės metu.
- Mokymas ir švietimas: reguliariai mokykite ir mokykite darbuotojus ir pagrindines suinteresuotąsias šalis apie krizių valdymo principus, politiką ir procedūras. Tai padės užtikrinti, kad visi žinotų organizacijos krizių valdymo planą ir žinotų savo vaidmenis bei pareigas krizės metu.
- Išteklių paskirstymas: Užtikrinti, kad organizacija turėtų pakankamai išteklių, tokių kaip personalas, technologijos ir įranga, kad galėtų reaguoti į krizę. Tai apima nenumatytų atvejų planų kūrimą pagrindinėms paslaugoms ir svarbioms funkcijoms, tokioms kaip IT, finansai ir klientų aptarnavimas.
- Stebėsena ir vertinimas: Reguliariai stebėkite ir vertinkite krizių valdymo plano veiksmingumą ir, remdamiesi atsiliepimais bei įgyta patirtimi, atlikite reikiamus pakeitimus. Tai padės užtikrinti, kad organizacija nuolat tobulins pasirengimą krizėms ir reagavimo pajėgumus.

Apibendrinant galima teigti, kad efektyvus pasirengimas krizei apima kruopštų rizikos įvertinimą, išsamaus krizių valdymo plano parengimą, aiškių komunikacijos protokolų sudarymą, reguliarų mokymą ir švietimą, pakankamai išteklių skyrimą, reguliarų plano efektyvumo stebėjimą ir vertinimą. Imdamosi šių veiksmų, vyriausybės gali būti geriau pasirengusios reaguoti į krizę ir sušvelninti jos poveikį savo veiklai, reputacijai ir suinteresuotosioms šalims.

Krizei vystantis toliau Valstybė pereina į krizės valdymo etapą. Aktyvuojamas krizės valdymo planas, priklausomai nuo krizės dydžio, šalyje gali būti įvedama krizinė padėtis. Krizės valdymas pilnai perduodamas dedikuotam krizių valdymo padaliniui ar institucijai. Svarbu pažymėti, kad krizės metu atsiranda daug nenumatytų aplinkybių ir reiškinių kurie tarpusavyje sąveikauja ir gali nukreipti krizės vystymąsi neplanuota linkme. Krizės valdymo etapo metu svarbu nuolat vertinti kintančią aplinką, atitinkamai reaguoti ir adaptuoti ir tikslinti krizės valdymo planą ir veiksmus.

Krizei vykstant elektroninėje erdvėje gali būti taikomi tokie kibernetinių krizių valdymo modeliai.

- NIST kibernetinio saugumo sistema yra plačiai naudojamas kibernetinių krizių valdymo modelis, sukurtas Nacionalinio standartų ir technologijų instituto (NIST). Sistemą sudaro penkios pagrindinės funkcijos: identifikavimas, apsauga, aptikimas, atsakymas ir atkūrimas. Sistema suteikia struktūrizuotą metodą organizacijoms valdyti kibernetines rizikas, įvertinti savo dabartinę kibernetinio saugumo padėtį ir parengti pritaikytą kibernetinio saugumo planą. Sistemoje taip pat pabrėžiama nuolatinio tobulėjimo ir suinteresuotųjų šalių įtraukimo svarba.
- CERT atsparumo valdymo modelis yra kibernetinių krizių valdymo modelis, sukurtas Carnegie Mellon universiteto Programinės įrangos inžinerijos instituto. Modelį sudaro keturi etapai: paruošimas, identifikavimas, talpinimas ir atkūrimas. Modelyje pabrėžiama rizikos vertinimo, reagavimo į incidentus planavimo, suinteresuotųjų šalių įtraukimo ir nuolatinio tobulėjimo svarba. Modelyje taip pat pateikiamos gairės, kaip įgyvendinti NIST kibernetinio saugumo sistemą.
- ISO/IEC 27001:2013 standartas yra tarptautinis informacijos saugumo valdymo standartas, sukurtas Tarptautinės standartizacijos organizacijos (ISO) ir Tarptautinės elektrotechnikos komisijos (IEC). Standartas suteikia organizacijoms pagrindą sukurti, įdiegti, prižiūrėti ir nuolat tobulinti informacijos saugumo valdymo sistemą (ISMS). Standartas pabrėžia rizikos vertinimo, turto valdymo, prieigos kontrolės, incidentų valdymo ir veiklos tęstinumo planavimo svarbą.
- SANS instituto reagavimo į incidentus planas yra SANS instituto sukurtas kibernetinių krizių valdymo modelis. Planą sudaro šeši etapai: pasirengimas, identifikavimas, sulaikymas, išnaikinimas, atkūrimas ir išmoktos pamokos. Plane pabrėžiama savalaikio

reagavimo į incidentą, komunikacijos, dokumentacijos ir suinteresuotųjų šalių įtraukimo svarba. Plane taip pat pateikiamos gairės, kaip sukurti reagavimo į incidentus komandą, nustatyti reagavimo į incidentus procedūras ir atlikti analizę po incidento.

Galiausiai krizei pasibaigus atliekamas krizės padarinių vertinimas ir jų valdymas inicijuojami atsistatymo po krizės procesai ir atliekama išmoktų pamokų analizė. Pastarasis procesa yra ypač svarbus kadangi užtikrina modelio ciklišKumą ir perėjimą į aukštesnį kokybinį lygį sekančios iteracijos metu. Tokios hibridinių krizių valdymo modelio iteracijos užtikrina nuoseklų Valstybės atsparumo hibridinėms grėsmėms didinimą.

Pagrindiniai žingsniai po krizės, įskaitant kibernetinę krizę, gali būti suskirstyti į šias kategorijas:

- Vertinimas ir vertinimas: Ištikus krizei pirmiausia reikia nuodugniai įvertinti situaciją ir įvertinti padarytą žalą. Tai gali apimti krizės priežasties ir masto nustatymą, poveikio suinteresuotosioms šalims įvertinimą ir atsigavimui reikalingų išteklių nustatymą.
- Bendravimas: Krizės metu ir po jos itin svarbus efektyvus bendravimas. Labai svarbu suinteresuotąsias šalis informuoti apie situaciją, kokių veiksmų imamasi ir ko jos gali tikėtis ateityje. Bendravimas turi būti aiškus, nuoseklus ir savalaikis.
- Atkūrimo planavimas: Turėtų būti parengtas atkūrimo planas, kuriame būtų nurodyti veiksmai, kurių reikia imtis norint atkurti veiklą ir atnaujinti įprastą verslo veiklą. Tai turėtų apimti prioritetų nustatymą, išteklių paskirstymą ir atkūrimo termino nustatymą.
- Išmoktų pamokų analizė, pritaikymas ir pokyčių įgalinimas: Ištaisymas apima neatidėliotinus veiksmus siekiant ištaisyti bet kokią krizės padarytą žalą. Kibernetinės krizės atveju tai gali apimti atsarginių kopijų atkūrimą, pažeidžiamumų pataisymą ir bet kokių nuolatinių grėsmių mažinimą. Išsprendus krizę, svarbu atlikti pomirtinį patikrinimą, siekiant nustatyti, kas nutiko ne taip ir ką galima padaryti, kad panašių krizių būtų išvengta ateityje. Tai gali apimti politikos, procedūrų ir mokymo programų peržiūrą, taip pat bet kokių būtinų pakeitimų įgyvendinimą.
- Testavimas ir patvirtinimas: Baigus taisymą, svarbu išbandyti sistemas ir procesus, siekiant užtikrinti, kad jie tinkamai veiktų. Tai gali apimti atsarginių kopijų testavimą, įsiskverbimo testavimą ir saugos kontrolės priemonių patvirtinimą.

Apibendrinant trečiajame skyriuje siūlomą hibridinių grėsmių elektroninėje erdvėje valstybės mastu valdymo ir vertinimo modelį, galima teigti, kad modelis pabrėžia

e.erdvės vientisumą, atspindi krizių valdymo proceso ciklišKumą ir kokybinę Valstybės atsparumo hibridinėms grėsmėms pažangą po kiekvienos naujos iteracijos.

Krizių valdymo modelio pagrįstumo vertinimas paprastai apima jo gebėjimo tiksliai reprezentuoti ir reaguoti į realaus pasaulio krizių scenarijus. Kai kurie pagrindiniai modelio galiojimo įvertinimo aspektai:

- Modelio prielaidos atitinka realias sąlygas ir modeliuojamą krizės scenarijų.
- Modeliui sukurti naudojami duomenys tiksliai atspindi modeliuojamą krizės scenarijų.
- Modelis geba tiksliai numatyti krizės scenarijaus baigtį.
- Modelis yra adaptyvus - įvesties parametrų pakeitimai veikia modelio išvestį.
- Modelio rezultatus galima palyginti su kitais esamais modeliais, kad patvirtinti jo efektyvumą.
- Modelis konstruotas konultuojantis su dalyko ekspertais, kad įvertinti modelio gebėjimą tiksliai atvaizduoti modeliuojamą krizės scenarijų.
- Modelis gali būti jį išbandant pratybų metu.

2.3 Modelio teorinė reikšmė ir praktinis pritaikomumas

Hibridinių grėsmių valdymo elektroninėje erdvėje valdymo valstybės masto modelio torinę reikšmę apibrėžia dvi pagrindinės išvados:

- Tradicinės hibridinės grėsmės ir naujai atsirandančios hibridinės grėsmės migruoja į elektroninę erdvę. Elektroninė erdvė tampa nauju valstybės kritinės infrastruktūros objektu;
- Valdant hibridines grėsmes elektroninėje erdvėje galima adaptuoti egzistuojančius krizių valdymo modelius.

Praktiškai pritaikant siūlomą hibridinių grėsmių valdymo elektroninėje erdvėje modelį galima pritaikyti planuojant aukšto, strateginio lygio, pratybas siekiant pasirengti hibridinių krizių sėkmingai suvaldymui.

Rengiant pratybas reikėtų imtis sekančių žingsnių (NATO, 2013):

- Identifikuoti kritinę infrastruktūrą, į kurią galėtų būti nukreipta hibridinė ataka;
- parengti galimų grėsmių ir pažeidžiamumų rizikos vertinimą;

- Sukurti scenarijų, kuriame derinami įvairių tipų išpuoliai, tokie kaip kibernetinė, fizinė ir socialinė inžinerija, kad būtų galima kuo išsamiau imituoti hibridinį išpuolį;
- Numatyti ir įtraukti į pratybas visas suinteresuotas šalis, tokias kaip vyriausybinės agentūras, privataus sektoriaus organizacijas ir kitus pagrindinius veikėjus, siekiant užtikrinti, kad visos suinteresuotos šalys būtų pasirengusios krizei ir žinotų savo vaidmenis ir atsakomybes;
- Sukurti pratybų scenarijų ir numatyti įvadus į pratybas;
- Atlikti pratybas kontroliuojamoje aplinkoje;
- Įvertinti pratybas ir nustatyti sritis, skirtas pagerinti reagavimo laiką, bendravimą ir koordinavimą tarp suinteresuotųjų šalių;
- Integruojant pratybų metu išmoktas pamokas sukurti arba atnaujinti krizės valdymo veiksmų planus, siekiant pagerinti kritinės hibridinių išpuolių infrastruktūros pasirengimą;

IŠVADOS IR REKOMENDACIJOS

Hibridinės grėsmės elektroninėje erdvėje yra didelis iššūkis nacionaliniam saugumui. Atsiranda vis daugiau naujų hibridinių grėsmių formų, o tradicinės hibridinės grėsmės migruoja į elektroninę erdvę. Pati elektroninė erdvė tampa kritinės infrastruktūros objektu. Sparčiai tobulėjant technologijoms, atsiranda naujų pažeidžiamumų ir atakų vektorių, kurie jeigu nevaldomi, kelią grėsmę valstybės kritinių sektorių veiklai, demokratinių procesų veiklą ir ardo pačios visuomenės darną. Tokia padėtis kelia susirūpinimą ne tik atskirų valstybių vyriausybės bet ir tarptautinėms organizacijoms tokioms kaip NATO ir ES. Tarptautinės organizacijos, pvz., NATO ir Europos Sąjunga, atlieka svarbų vaidmenį pripažįstant, reaguojant ir kovojant su hibridinėmis grėsmėmis. Hibridinės grėsmės yra sudėtingos ir daugiasluoksnės, reikalaujančios visapusiško ir suderinto požiūrio. NATO ir ES įgyvendino priemones, skirtas kovoti su hibridinėmis grėsmėmis, įskaitant atsparumo didinimą, žvalgybos ir stebėjimo gebėjimų stiprinimą, tarptautinės bendradarbiavimo gerinimą, kibernetinio saugumo stiprinimą ir diplomatinės veiklos plėtojimą ir komunikaciją.

Yra valstybių tokių kaip Suomija, kurios supranta hibridinių grėsmių keliamus iššūkius valstybei ir imasi priemonių, visuose lygiuose, tokias grėsmes valdyti. Suomijos strateginiai nacionalinio saugumo dokumentai įvardiją hibridinius iššūkius ir sukuria prielaidas, valstybės mastu, įgyvendinti visą eilę programų ir projektų kurie įgalintų atpažinti, įvertinti, pasiruošti ir valdyti hibridinių grėsmių sukeltas krizes. Suomijos vyriausybė siekia plataus privataus sektoriaus ir visuomenės įsitraukimo prevenciškai ruošiantis atsakyti į galimus hibridinių grėsmių keliamus iššūkius.

Ekspertai, kurie savo kasdieninėje veikloje susiduria su politikos formavimu, visuomenės informavimu, kibernetiniu saugumu ir krizių valdymu vieningai sutaria, kad hibridinės grėsmės kylančios elektroninėje erdvėje yra ne ateities o dabarties iššūkis. Stiprinant valstybės atsparumą hibridinių grėsmių poveikiui reikalinga jau dabar įgyvendinti visą eilę priemonių kurios sudarytų sąlygas atpažinti hibridines grėsmes, įvertinti jų keliamas rizikas, paruošti atsako į hibridinių grėsmių keliamus iššūkius planus, numatyti grėsmių valdymo modelį ir būti pasiruošus užtikrinti pagrindines valstybės funkcijas krizės metu ir atsistatant po krizės.

Reikalingas naujas, sisteminis požiūris į hibridinių grėsmių valdymą. Tradiciniai grėsmių valdymo modeliai ne visada gali būti taikomi siekiant sėkmingai identifikuoti, valdyti ir reaguoti į hibridines grėsmes elektroninėje erdvėje. Todėl reikalingas šios dienos poreikius atitinkantis hibridinių grėsmių valdymo ir vertinimo modelis visos valstybės mastu, kuris galėtų būti praktiškai pritaikytas rengiant reagavimo į hibridines grėsmes planus.

Rekomendacijos:

Sukurti teisinę bazę: valstybė turėtų sukurti tinkamą teisinę bazę hibridinėms grėsmėms elektroninėje erdvėje valdyti. Ši sistema turėtų apimti nacionalinio saugumo strategiją, kurioje būtų nustatytos galimos hibridinės grėsmės ir nurodyti būtini veiksmai joms valdyti.

Stiprinti pasipriešinimo ir gynybos planus: hibridinėms grėsmėms valdyti valstybė turėtų investuoti į ypatingos svarbos infrastruktūros objektų gynybą ir fizinę apsaugą. Ji turėtų paruošti personalą apsiginti ir greitai pašalinti atakos padarinius. Taip pat reikėtų stiprinti kibernetinę gynybą nacionaliniu mastu, segmentuoti tinklus, diegti ugniasienes, stiprinti apsaugos nuo kibernetinių atakų sistemas.

Bendradarbiauti su kitomis šalimis ir tarptautinėmis organizacijomis: Valstybė turėtų bendradarbiauti su kitomis šalimis ir tarptautinėmis organizacijomis, kad būtų dalijamasi informacija ir koordinuojamas atsakas į hibridines kibernetines grėsmes.

Sisteminis požiūris: tradiciniai grėsmių valdymo modeliai gali netikti hibridinėms grėsmėms valdyti. Todėl valstybė turėtų sistemingai valdyti hibridines grėsmes elektroninėje erdvėje. Šis požiūris turėtų apimti visos valstybės hibridinių grėsmių valdymo ir vertinimo modelio, kuris galėtų būti praktiškai pritaikytas rengiant reagavimo į hibridines grėsmes planus, sukūrimą.

Investuokite į mokslinius tyrimus: Valstybė turėtų investuoti į mokslinius tyrimus, siekdama skatinti naujas technologijas ir nustatyti naujus pažeidžiamumus bei atakų vektorius. Ji turėtų numatyti ir įgyvendinti apsaugos priemones, kad būtų užkirstas kelias žalingam tokių technologijų naudojimui.

Įgyvendindama šias rekomendacijas valstybė gali sėkmingai valdyti hibridines grėsmes kibernetinėje erdvėje ir užtikrinti ypatingos svarbos infrastruktūros saugumą.

LITERATŪROS ŠALTINIAI

1. Avoine, G., Bourbeau, M., & Petit, J. (2014). Keywords-based detection of cybercrime in online forums. *Computer Communications*, 17-27.
2. Ayanso, A., Wang, Q., & Yan, H. (2011). Topic modeling in social media: An empirical study. *Journal of Organizational Computing and Electronic Commerce*, *21*(3), 279-297.
3. Aytulun, S., & Guneri, A. (2008). Business process modelling with stochastic networks. *International Journal of Production Research*, *46*(10), 2743-2764. 10.1080/00207540701543601
4. Bachmann,, S.-D., & Gunneriusson, H. (2015). HYBRID WARS: THE 21st-CENTURY'S NEW THREATS TO GLOBAL PEACE AND SECURITY. *Scientia Militaria, 43*(1), 77 - 98. 10.5787/43-1-1110
5. Bajarunas, E. (2020). Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond. *European View*, *19*(1), 62-70. org/10.1177/1781685820912041
6. Bajarunas, E., & Kersanskas, V. (2018). Hybrid Threats: Analysis of Content, Challenges Posed and Measures to Overcome.Lithuanian annual strategic review, *16*. 10.2478/lasr-2018-0006
7. Belezentis, A., & Zalimaite, M. (2011). Ekspertinių vertinimų taikymas inovacijų plėtros veiksnių analizėje: Lietuvos inovatyvių įmonių vertinimas. *Vadybos mokslas ir studijos - kaimo verslų ir jų infrastruktūros plėtrai*, *27*(3), 23-31.
8. Bogdanoski, M. (Ed.). (2022). *Building Cyber Resilience Against Hybrid Threats*. IOS Press, Incorporated.
9. Bumbarner, J. B. (n.d.). The Russian-Georgian Cyberconflict of 2008: A Study in Attribution. *Journal of Strategic Security*, *6*(3).
10. Buzan, T. (2018). *Mind Map Mastery: The Complete Guide to Learning and Using the Most Powerful Thinking Tool in the Universe*. Watkins Media.
11. Carlson, B. (2019). The evolution of hybrid warfare and key drivers of change. *Journal of Strategic Studies*, *42*, 1-2, 60-84.
12. Creswell, J. W., & Poth, C. N. (2018). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches* (C. N. Poth, Ed.). SAGE Publications.
13. DeBenedictis, K. (2021). *Russian 'Hybrid Warfare' and the Annexation of Crimea: The Modern Application of Soviet Political Warfare*. Bloomsbury Academic.

14. Demaertzis, M., & Wolff, G. (n.d.). Hybrid and cybersecurity threats and the European Union's financial system. *Policy contribution*, (10).
15. Dupuy, A. C. (2021, January 13). *NATO Review - Energy security in the era of hybrid warfare*. NATO. Retrieved February 14, 2023, from https://www.nato.int/docu/review/articles/2021/01/13/energy-security-in-the-era-of-hybrid-warfare/index.html
16. The European Centre of Excellence for Countering Hybrid Threats. (2022). Hybrid threats from non-state actors: A taxonomy. *Hybrid CoE Research Report*, (6). ISBN (web) 978-952-7472-22-4
17. The European Centre of Excellence for Countering Hybrid Threats & NATO Strategic Communications Centre of Excellence. (2022). *Foreign information manipulation and interference defence standards: Test for rapid adoption of the common language and framework 'DISARM'* (2, 7th ed.) [Hybrid CoE Research Report].
18. European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) & Joint Research Centre (JRC). (2020). *The Landscape of Hybrid Threats: A Conceptual Model*. https://www.hybridcoe.fi
19. European Union Agency for Cybersecurity. (2020). *Threat landscape for the energy sector*.
20. Europos Sąjunga. (2016). *Joint Communication to the European Parliament and the Council* [Joint Framework on countering hybrid threats].
21. Europos Sąjunga. (2021, May 6). *Best Practices in the whole-of-society approach in countering hybrid threats*. European Parliament. Retrieved February 23, 2023, from https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf
22. Europos Sąjunga. (2021, May 6). *Best Practices in the whole-of-society approach in countering hybrid threats*. European Parliament. Retrieved February 23, 2023, from https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf
23. Finish Government. (2017). *Security Strategy for Society*. Security Strategy for Society. Retrieved February 23, 2023, from https://turvallisuuskomitea.fi/en/security-strategy-for-society/
24. *Finland succeeds in cyber security comparisons*. (2022, 09 03). https://ficom.fi/news/finland-succeeds-in-cyber-security-comparisons/
25. Finnish Government. (2021, September 9). *Government's Defence Report*. Government's Defence Report. Retrieved February 23, 2023, from https://julkaisut.valtioneuvosto.fi/handle/10024/163407
26. Fry, E. (2022). *Persuasion Not Propaganda: Overcoming Controversies of Domestic Influence in NATO Military Strategic Communications* (11th ed., Issue Defence Strategic Communications). 10.30966/2018.RIGA.11.6
27. Government of Finlad. (2013). *Finland´s Cyber security Strategy*. Finland´s Cyber security Strategy. Retrieved February 23, 2023, from https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf
28. Gross, J. A. (2018, March 21). *Ending a decade of silence, Israel confirms it blew up Assad's nuclear reactor*. The Times of Israel. Retrieved February 14, 2023, from https://www.timesofisrael.com/ending-a-decade-of-silence-israel-reveals-it-blew-up-assads-nuclear-reactor/
29. Gudmundsson, B. (n.d.). The nature of hybrid threats. *Joint Force Quarterly, 80*, 36-44.

30. Gulevičiūtė (2013) E. Verslo kokybinių kriterijų kūrimas, ir taikymas: Pasaulinė rinkos analizė, MBD, MRU.
31. Hickton, D. (2023, February 26). *We must treat cyber wars the same as we treat conventional military encounters*. The Hill. Retrieved March 12, 2023, from https://thehill.com/opinion/cybersecurity/3871911-we-must-treat-cyber-wars-the-same-as-we-treat-conventional-military-encounters/
32. Hill, C. (n.d.). The Russian annexation of Crimea: Origins and implications. *Journal of Slavic Military Studies*, *28*(3), 321-342.
33. Hsu, C., & Sandford, B. (2007). The Delphi Technique: Making Sense of Consensus. *Practical Assessment, Research & Evaluation*, *12*(10).
34. Hutchinson, G. (2022). *Cyber security and the cyber domain - Ministry for Foreign Affairs*. Cyber security and the cyber domain - Ministry for Foreign Affairs. Retrieved February 23, 2023, from https://um.fi/cyber-security-and-the-cyber-domain
35. *Hybrid threats and hybrid influence activities - Ministry of the Interior*. (2023). Finland's Ministry of Interior. Retrieved February 23, 2023, from https://intermin.fi/en/national-security/hybrid-threats
36. Janicke, H., Maglaras, L., & Ferrag, M. A. (Eds.). (2022). *Cyber Security and Critical Infrastructures*. MDPI Books.
37. Jaques, T. (2007). Issue management and crisis management: An integrated, non-linear, relational construct. *Public Relations Review*, *33*(2), 147-157. https://www.sciencedirect.com/science/article/abs/pii/S0363811107000185
38. Jaques, T. (2007). ssue management and crisis management: An integrated, non-linear, relational construct. *Public Relations Review*, *33*(2), 147-157. https://doi.org/10.1016/j.pubrev.2007.02.001.
39. Kardelis, K. (2002). *Mokslinių Tyrimų Metodologija Ir Metodai* (2nd ed.).
40. Keeney, R., Raiffa, H., & Rajala, D. (1977). Decisions with Multiple Objectives: Preferences and Value Trade-Offs. *IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS*, *9*(7), 403. 10.2307/2286244
41. Krippendorff, K. (2018). *Content Analysis: An Introduction to Its Methodology*. SAGE Publications.
42. Leonhard, R. (n.d.). The art of hybrid war: Russian doctrine and the military use of non-state proxies in Eastern Ukraine. *Journal of Strategic Studies*, *39*(1), 77-108.
43. Libby, R., & Blashfield, R. (1978). Performance of a composite as a function of the number of judges. *Organizational Behavior and Human Performance*, *21*(2), 121-129.
44. Limba, T., Driaunys, K., Stankevicius, A., & Andrulevicius, A. (2020). CRYPTOCURRENCY AND NATIONAL SECURITY: PECULIARITIES OF INTERACTION. *Transformations in Business & Economics*, *19*(2), 138- 158.
45. Lohmann, S. J., & Butrimas, V. (2022). *What Ukraine Taught NATO about Hybrid Warfare*. United States Army War College Press, Strategic Studies Institute.
46. LRV, (2018). Nacionalinė kibernetinio saugumo strategija, https://kam.lt/wp-content/uploads/2022/03/nacionaline-kibernetinio-saugumo-strategija.pdf
47. Merriam, S. B., & Tisdell, E. J. (2016). *Qualitative Research: A Guide to Design and Implementation*. Wiley.
48. Morfino, V., & Eampone, S. (2020). Towards Near-Real-Time Intrusion Detection for IoT Devices using Supervised Learning and Apache Spark. *Electronics*, *9*(3). 10.3390/electronics9030444

49. NATO. (2017). *Allied Joint Doctrine for Countering Hybrid Threats*.
50. NATO STRATCOM COE, Pamment, J., & Smith, V. (2022). *ATTRIBUTING INFORMATION INFLUENCE OPERATIONS IDENTIFYING THOSE RESPONSIBLE FOR MALICIOUS BEHAVIOUR ONLINE*. ISBN: 978-9934-619-14-4
51. Neuendorf, K. A. (2002). *The Content Analysis Guidebook*. SAGE Publications.
52. Niglia, A. (Ed.). (2016). *Critical Infrastructure Protection Against Hybrid Warfare Security Related Challenges*. IOS Press.
53. Novak, J. D., & Gowin, D. B. (1984). *Learning How to Learn*. Cambridge University Press.
54. Okoli, C., & Pawlowski, S. D. (2004). The delphi method as a research tool: An example, design considerations and applications. *Information & Management*, *42*(1), 15-29.
55. Pearson, M., & Clair, A. (1998). Reframing crisis management. *Academy of Management Review*, *23*(1), 59-76.
56. Pearson, M., & Mitroff, I. (1993). From crisis prone to crisis prepared: A framework for crisis management. *Academy of Management Executive*, *7*(1), 48-59.
57. Plano Clark, V. L., & Ivankova, N. V. (2015). *Mixed Methods Research: A Guide to the Field*. SAGE Publications.
58. Romansky, R., & Noninska, I. (2020, 08 10). Challenges of the digital age for privacy and personal data protection. *Mathematical Biosciences and Engineering*, *17*(5), 5288–5303. 10.3934/mbe.2020286
59. Rowe, G., & Wright, G. (1999). The Delphi technique as a forecasting tool: issues and analysis. *International Journal of Forecasting*, *15*(4), 353-375.
60. Ruhle, M., & Roberts, C. (2021). *Enlarging NATO's toolbox to counter hybrid threats*. https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html
61. Sanger, D. E. (2012, June 1). *Obama Ordered Wave of Cyberattacks Against Iran*. The New York Times. Retrieved February 14, 2023, from https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html
62. Schmidt, R. C. (n.d.). Managing delphi surveys using nonparametric statistical techniques. *Decision Sciences*, *28*(3), 763–774.
63. Secretariat of the Security Committee. (2013). *Finland´s Cyber security Strategy*. https://www.defmin.fi. https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf
64. Sidekerskiene, T. (2007). Valdymo sistemos su v ̇elavimais analizinis tyrimas. *Liet. matem. rink*, 473–478.
65. Simon, G. (2017). *Hybrid Warfare: A New Strategy of War* (Vol. 6). International Journal of Advanced Research in Computer Science and Software Engineering. pp. 23-26
66. Skarmeta, A., & Bernabe, J. B. (Eds.). (2019). *Challenges in Cybersecurity and Privacy: The European Research Landscape*. River Publishers.
67. Smith, H., Theocharidou, M., & Giannopoulos, G. (2021). *The Landscape of Hybrid Threats: A conceptual model*. 10.2760/44985
68. Soldatos, J., Philpot, J., & Giunta, G. (Eds.). (2020). *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures*. Now Publishers.
69. SØRENSEN, H., & NYEMANN, D. (2018). Going Beyond Resilience A revitalized approach to countering hybrid threats. *Hybid CoE Strategic Analysis*, (13).

70. Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation & Kalniete, S. (2021, June 14). *Building EU resilience against hybrid threats*. European Parliament. Retrieved February 23, 2023, from https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/INGE/DT/2021/06-22/1232460EN.pdf
71. Statistics Finland, (2023), https://stat.fi/index_en.html
72. Teddlie, C., Teddlie, C. B., & Tashakkori, A. (1998). *Mixed methodology : combining qualitative and quantitative approaches*. SAGE Publications.
73. Teo, W., Lee, M., & Lim, W. (2017). The relational activation of resilience model: How leadership activates resilience in an organizational crisis. *Contingencies and Crisis Management*, *25*(3), 136-147. https://onlinelibrary.wiley.com/doi/10.1111/1468-5973.12179
74. Tidikis, R. (2003). *SOCIALINIŲ MOKSLŲ TYRIMŲ METODOLOGIJA*. https://repository.mruni.eu/bitstream/handle/007/15459/Tidikis_tyrimu_metodologija.pdf?sequence=1&isAllowed=y
75. Turoff, M., & Linstone, H. A. (Eds.). (2002). *The Delphi Method: Techniques and Applications*. Addison-Wesley.
76. Vailshery, L. S. (2022, August 1). *Internet of Things (IoT) - statistics & facts*. Statista. Retrieved March 12, 2023, from https://www.statista.com/topics/2637/internet-of-things/#topicHeader__wrapper
77. Van de Ven, A., & Delbecq, L. (1971). The effectiveness of nominal, Delphi, and interacting group decision making processes. *Academy of Management Journal*, *14*(4), 466-492.
78. Warren, M., Stitilis, D., & Laurinaitis, M. (2023). THE IMPACT OF RUSSIAN CYBER ATTACKERS WITHIN THE UKRAINE SITUATION. *JOURNAL OF INFORMATION WARFARE*, *22*(1).
79. Weaver, C. K. (n.d.). Cybersecurity and cyberwar: An overview of the information threat landscape. *IEEE Communications Magazine*, *55*(2), 13-19.
80. Weber, R. P. (1990). *Basic Content Analysis*. SAGE Publications, Incorporated.
81. Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods*. SAGE Publications.