MYKOLO ROMERIO UNIVERSITETAS
EKONOMIKOS IR VERSLO FAKULTETAS

JUOZAS BREIVĖ

VIEŠOJO IR PRIVATAUS SEKTORIŲ PARTNERYSTĖ UŽTIKRINANT KIBERNETINĮ SAUGUMĄ LIETUVOJE

Magistro baigiamasis darbas

Vadovas
Prof. dr. Darius Štitilis

VILNIUS, 2018

MYKOLO ROMERIO UNIVERSITETAS
EKONOMIKOS IR VERSLO FAKULTETAS

VIEŠOJO IR PRIVATAUS SEKTORIŲ PARTNERYSTĖ UŽTIKRINANT KIBERNETINĮ SAUGUMĄ LIETUVOJE

Verslo vadybos magistro baigiamasis darbas

Studijų programa 6211LX066

Vadovas
Prof. dr. Darius Štitilis
2018

Recenzentas

2018

Atliko
KSVvmns 16-0 gr. stud.
J. Breivė
2018

VILNIUS, 2018

TURINYS

LENTELĖS

PAVEIKSLAI

PRIEDAI

SANTRUMPOS

CSP3	Viešojo ir privataus sektorių partnerystė kibernetinio saugumo srityje
ENISA	Europos Sąjungos tinklų ir informacijos saugumo agentūra
ES	Europos Sąjunga
JAV	Jungtinės Amerikos Valstijos
NATO	Šiaurės Atlanto Sutarties Organizacija
NIST	Nacionalinis technologijų ir standartų institutas
P3	Viešojo ir privataus sektorių partnerystė
PPP	Viešojo ir privataus sektorių partnerystė

ĮVADAS

Per paskutinius kelerius metus sparčiai besivystančios informacinės ir pramoninių procesų valdymo technologijos sukuria terpę populiarėjantiems elektroniniams nusikaltimams kibernetinėje erdvėje dominuoti. Tokių nusikaltimų taikiniais vis dažniau tampa kritinė infrastruktūra, sveikatos apsauga ir kitos visuomenei gyvybiškai svarbios funkcijos.

Spartus technologinis progresas pasauliniu mastu vis dažniau po kibernetinio saugumo domenu apjungia valstybes, įmones ir žmones. Nors ši plėtra ženkliai skatina gerovės vystymąsi, tačiau tuo pačiu atneša ir naujai kylančių grėsmių bei rizikų, kurios gali neigiamai paveikti viešąsias paslaugas, verslo vystymąsi ir jo valdymą, tuo pačiu ir visapusišką visuomenės vientisumą.

Temos aktualumas. Informacinių sistemų saugumo užtikrinimo klausimas šiuo metu keliamas kaip vienas iš valstybinių strateginių tikslų daugelyje Europos (Solana, Saz-Carranza ir Estebanez Gomez, 2016) ir kitų pasaulio šalių gynybiniame kontekste (Shafqat ir Masood, 2016).

Kaip teigia D. Štitilis elektroninės erdvės globalumas sukūrė beprecedentes sąlygas daryti nusikaltimus iš bet kurios pasaulio vietos, kurioje yra internetas (Štitilis, 2013).

Nepaisant nuolankios kovos su sunkiai apibrėžiamomis kibernetinėmis grėsmėmis daugeliu atveju kuriama kibernetinio saugumo strategija grindžiama bendradarbiavimu. Vienas iš esminių kibernetinio saugumo, grėsmių neapibrėžtumui valdyti, strategijos elementų yra bendradarbiavimo tobulinimas ir informacijos dalybų įgalinimas tarp įvairių suinteresuotųjų šalių sukuriantis prielaidas viešojo ir privataus sektorių partnerystei. Tokia partnerystė dažnai laikoma atsakymu į neapibrėžtumo valdymo iššūkį didinant žinių pasitelkimo lankstumą, tačiau lieka neišspręstas skirtingo požiūrio į grėsmes klausimas kurį iškelia šios partnerystės atsiradimas, todėl būtina ištirti viešojo ir privataus sektorių partnerystės situaciją kibernetinio saugumo srityje Lietuvoje ir apibrėžti galimas bendradarbiavimo gaires.

Temos ištirtumas. Užsienio literatūroje viešojo ir privataus sektorių bendradarbiavimo aspektai kibernetinio saugumo srityje aktyviai analizuojami jau gerą dešimtmetį: pradedant kibernetinio saugumo strategijose apibrėžtu bendradarbiavimo palyginimu (Carr, 2016), sugretinant tarptautinę vyriausybių patirtį viešojo ir privataus sektorių partnerystės srityje po 2008 m. finansinės krizės ieškant efektyvesnių valdymo būdų (Akintoye, Beck ir Kumaraswamy, 2015), nustatant 4 kertines sritis (CSP3 unikalumas, įgyvendinimo barjerai (tame tarpe teisinio reguliavimo įtaka), viešojo sektoriaus dalyvavimo svarba ir sėkmingos partnerystės metodai), kuriomis vadovaujantis CSP3 turi integruotis į strateginį kibernetinio saugumo užtikrinimo lygmenį (Germano, 2014), 2017 m. ENISA (2017) atliktos studijos metu analizuoti bendradarbiavimo modeliai įgyvendinant CSP3 keliant tikslą išsiaiškinti partnerystės metu kylančius

iššūkius ir suformuluoti bei pasiūlyti CSP3 diegimo Europoje rekomendacijas. Tais pačiais metais atlikto kito tyrimo metu bandyta identifikuoti kritinius sėkmės faktorius partnerystės kibernetinio saugumo srityje įgyvendinimui pateikiant CSP3 apibrėžimą (Bechkoum, Thomas, Campbell ir Brown, 2017).

Konkretūs viešojo ir privataus sektorių partnerystės aspektai kibernetinio saugumo srityje Lietuvių autorių išsamiai iki šiol analizuoti nebuvo ir daugiausiai rėmėsi privatizavimo problematika. G. Užkuraitytė (2015) ir B. Ropė (2015) nagrinėjo bendruosius kibernetinio saugumo strategijos principus. Tuo tarpu D. Štitilis (2013) savo darbuose orientavosi į teisinius kibernetinio saugumo užtikrinimo aspektus ir strategijų lyginamasias analizes. R. Žilinskas ir L. Trakimavičius (2016) analizavo kibernetines atakas prieš energetikos sektorių ir NATO grėsmių vertinimo bei politikų pokyčius po jų. Populiariausia mokslinių tyrimu sritis – teoriniai viešojo ir privataus sektorių partnerystės įgyvendinimo ir socialinio poveikio aspektai, kuriuos analizavo M. Dūda (2010) ir E. Skietrys bei prof. dr. A. Raipa (2009). D. Gudelis ir V. Rozenbergaitė (2004) nagrinėjo viešojo ir privataus sektorių partnerystės, kaip alternatyvios viešųjų paslaugų teikimo ir infrastruktūros plėtojimo formos, sampratą ir argumentus dėl tokios plėtros galimybių pasirinkimo. Tokios partnerystės poreikį ir galimybes Lietuvoje aprašė Ž. Šutavičienė (2011). Šiek tiek partnerystės principus kibernetinio saugumo apimtimi analizavo jaunųjų profesionalų programos „Kurk Lietuvai“ komanda (Rasimavičiūtė, Sadaunykaitė ir Bernotas, 2014), kuri, remiantis atlikta apklausa, parengė situacijos 2014 m. analizę ir bendradarbiavimo pasiūlymus.

Darbo mokslinis naujumas. Analizuotoje literatūroje galime aiškiai įžvelgti užsienio valstybių patirtį, tačiau šios patirties pritaikymo aspektai Lietuvos mastu plačiai nagrinėti nebuvo. Taip pat, nesant teisinio tokios partnerystės šalyje reglamentavimo, nėra aišku, kas apima viešojo ir privataus sektorių bendradarbiavimo gaires, kur yra įgyvendinimo apribojimai ar kokios jau egzistuojančios apraiškos Lietuvoje vyksta.

Tiriamoji problema. 2014 m. Lietuvoje atsiradęs Kibernetinio saugumo įstatymas sukūrė prielaidas teisiniam kibernetinio saugumo srities reglamentavimui ir reguliavimui, tame tarpe CSP3 atsiradimui, tačiau iki šiol partnerystės įgyvendinimas turi trūkumų, neišnaudojamos gerosios praktikos ar reguliariai neanalizuojama reiškinio būklė siekiant tobulinti procesus, atsakomybių paskirstymą ar į tikslą orientuotos naudos gavybą.

Galime kelti **hipotezę**, kad nepakankamas viešojo ir privataus sektorių bendradarbiavimas didina neracionalių kibernetinį saugumą reglamentuojančių teisės aktų ir reikalavimų atsiradimą, neišnaudojamas kibernetinio saugumo specialistų rengimo potencialas, neatsiranda tarpusavio pasitikėjimo stiprinimo prielaidos, o tai įtakoja investuojamų kaštų į kibernetinio saugumo užtikrinimą privačioje infrastruktūroje didėjimą ir neišnaudojamos visos įmanomos kibernetinio atsparumo priemonės valstybės mastu. Pastebėta,

kad ši tema reikalauja gilesnės analizės, todėl kyla probleminis klausimas: **kaip organizuoti viešojo ir privataus sektorių bendradarbiavimą kibernetinio saugumo srityje?**

Tyrimo objektas – viešojo ir privataus sektorių partnerystė užtikrinant kibernetinį saugumą Lietuvoje.

Magistro baigiamojo darbo tikslas – ištirti viešojo ir privataus sektorių bendradarbiavimo užtikrinant kibernetinį saugumą situaciją ir plėtros galimybes Lietuvoje.

Darbo tikslui pasiekti, darbe reikia spręsti šiuos **uždavinius**:

1. išanalizuoti viešojo ir privataus sektorių partnerystės sampratą ir įgyvendinimo būdus,
2. išanalizuoti viešojo ir privataus sektorių partnerystės kibernetinio saugumo užtikrinimo srityje teorinius aspektus,
3. palyginti 2016-2018 m. pasitvirtinusių (atsinaujinusių) kibernetinio saugumo strategiją Europos Sąjungos šalių narių praktiką dėl viešojo ir privataus sektorių partnerystės įgyvendinimo kibernetinio saugumo srityje,
4. empirinio tyrimo metu ištirti viešojo ir privataus sektorių bendradarbiavimo kibernetinio saugumo srityje situaciją ir plėtros galimybes Lietuvos Respublikoje.

Darbo uždaviniams pasiekti bus naudojami šie **metodai**:

1. empirinio tyrimo analizės metodu išanalizuoti viešojo ir privataus sektorių partnerystės sampratą ir galimas sąsajas su kibernetinio saugumo užtikrinimu;
2. kokybinės lyginamosios analizės tyrimo metodu palyginti viešojo ir privataus sektorių partnerystės kibernetinio saugumo srityje situaciją bei praktiką pasirinktose užsienio valstybėse;
3. kokybinio tyrimo metodo pusiau struktūruotas interviu su ekspertais.

Tyrimo metodologija. Tyrimo metu naudojama kokybinė tyrimo metodologija siekiant gauti detalią informaciją apie galimą viešojo ir privataus sektorių partnerystės kibernetinio saugumo srityje galimybes, teiginiais pagrįsti jų būtinumą. Analizuojant tarptautinę patirtį, išsiaiškinti, kokios naudojamos formos atitinka keliamą tyrimo problemą.

Ekspertų nuomonės apklausos metu siekiama išsiaiškinti esamą situaciją Lietuvoje ir nešališkai, vengiant subjektyvumo, patikrinti keliamą hipotezę.

Darbe naudojami empiriniai duomenų rinkimo metodai. Teoriniame tyrime bus vykdoma dokumentų analizė tiriant mokslinės literatūros šaltinius bei norminius teisės aktus, siekiant atskleisti svarbius tiriamos problemos aspektus. Kokybinės lyginamosios analizės metodu sugretinama tarptautinė viešojo ir privataus sektorių partnerystės praktika ieškant galimo pritaikymo kibernetinio saugumo Lietuvoje užtikrinimui

pranašumų ir trūkumų. Informacijos ieškoma specializuotose žurnalų ir kitų mokslo leidinių duomenų bazėse.

Atlikta ekspertinė apklausa siekiant gauti informacijos apie gerąsias viešojo ir privataus sektorių partnerystės įgyvendinimo praktikas ir galimas tokios partnerystės apraiškas Lietuvoje.

Darbo struktūra. Darbą sudaro įvadas, dėstomoji, tiriamoji ir baigiamoji dalys. Dėstomojoje dalyje apžvelgiama su tyrimo problema siejama literatūra (moksliniai darbai, ekspertiniai žurnalai, tarptautiniai teisės aktai), nagrinėjamos viešojo ir privataus sektorių bendradarbiavimo kibernetinio saugumo srityje teoriniai aspektai bei analizuojami tokio bendradarbiavimo organizavimo principai. Tiriamojoje dalyje aprašoma tyrimo metodologija, aptariami tyrimo metu gauti rezultatai. Baigiamojoje dalyje pateikiamos išvados ir rekomendacijos.

1. VIEŠOJO IR PRIVATAUS SEKTORIŲ PARTNERYSTĖS TEORINIAI ASPEKTAI

Pirmaisiais XXI amžiaus dešimtmečiais, kai technologijų plėtra ir globalizacija tampa neatsiejama kasdienybe, net besivystančiose pasaulio šalyse viešasis sektorius, nuolat spaudžiamas piliečių teikti efektyvesnes ir kokybiškesnes paslaugas, pagal principą „daryti daugiau su mažiau“, išgyvena reikšmingas permainas. Nors daugeliui viešojo sektoriaus sričių nėra svetimos pertvarkymo reformos (Gudelis ir Rozenbergaitė, 2004), mažinant biurokratinį aparatą ir valstybinį reguliavimą ar privatizuojant viešąsias įmones, kurios paremtos privataus sektoriaus vadybine patirtimi, tačiau vis plačiau naudojamas viešojo ir privataus sektorių partnerystės būdas.

Žvelgiant globaliau, kiekvienas pokytis pasaulyje vienaip ar kitaip įtakoja bet kurios organizacijos dominavimą, kai politiniai, ekonominiai ar socialiniai elementai verčia ją nuolatos peržiūrėti savo viziją, misiją ir tikslus. Ne išimtis ir valdžios institucijos, kurios siekdamos patenkinti visuomeninius poreikius ieško naujų metodų ir priemonių viešųjų paslaugų teikimui ir jų infrastruktūros plėtrai. Rėmimasis partneryste leidžia tarp organizacijų perskirstyti užduotis ir misijas atsižvelgiant į dinamišką aplinką ir ekonomines aktualijas. Šios sinergijos atsiradimas integruoja geriausias viešojo ir privataus sektorių savybes.

1.1. Viešojo ir privataus sektorių partnerystės samprata

E. Skietrys ir prof. dr. A. Raipa (2009) analizuodami viešosios ir privačios partnerystės (bendradarbiavimo) esmę teigia, kad „viešojo ir privataus sektoriaus bendradarbiavimas turi gilias istorines tradicijas“ (p. 11) ir nėra tinkamas „analizuoti atsižvelgiant į naująją viešąją vadybą“ (p. 11), kaip ir pačio reiškinio įvardinimui pasirinkti aiškią ir konkrečią sampratą. M. Dūda (2010) antrina išsakytoms mintims, teigdamas, kad ši „sąvoka nėra vienareikšmiškai aiškinama“ (p. 140) ir remdamasis G. A. Hodge ir C. Greve (2007, p. 547) išskiria bent penkias tokios partnerystės sampratos grupes (Dūda, 2010, p. 140):

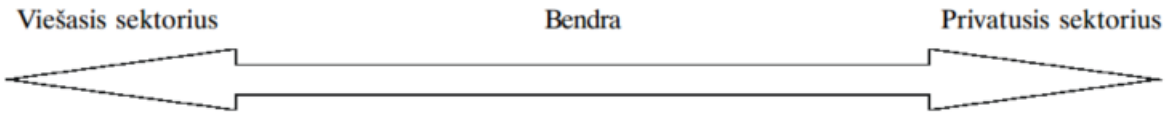
- *viešojo ir privataus sektorių partnerystė kaip institucionalizuotas bendradarbiavimas tarp viešojo ir privataus sektorių, jiems bendrai kuriant viešąsias gėrybes ir dalijantis visą su šia veikla susijusią riziką.*
- *viešojo ir privataus sektorių partnerystė kaip ilgalaikiai infrastruktūros kontraktai, kuriuose nustatyti griežti reikalavimai galutiniams kontrakto rezultatams.*

- *viešojo ir privataus sektorių partnerystė kaip viešosios politikos ir vadybos tinklai, kuriuose akcentuojami laisvi suinteresuotųjų dalyvių savitarpio santykiai.*
- *viešojo ir privataus sektorių partnerystė kaip pilietinės visuomenės ir bendruomeniškumo plėtotė.*
- *viešojo ir privataus sektorių partnerystė kaip miesto atnaujinimas ir ekonominis vystymasis.* Ši sampratos grupė paremta 1980 m. viešojo ir privataus sektorių partnerystės akronimu apibrėžiančiu miestų plėtrą JAV ir JK įtraukiant privatų sektorių.

A. Akintoye siūlo konceptualiai įvardinti viešojo ir privataus sektorių partnerystę kaip viešosios įstaigos ir privataus kapitalo partnerystės sutartį, pagal kurią valdomi bendri ištekliai, rizikų ir naudos pasidalijimas sukuria efektyvias viešąsias paslaugas ir privataus kapitalo produktą (Akintoye, Beck ir Kumaraswamy, 2015). Remdamasis Klijn ir Teisman (2003, p. 137) jam antrina R. Burke (2016) tokį bendradarbiavimą apibrėždamas kaip „ilgalaikį viešojo ir privataus sektorių subjektų bendradarbiavimą, kuriame dalyviai plėtoja savitąsias prekes ir (arba) paslaugas, ir kuriame dalijasi rizika, kaštais ir nauda“ (p. 2).

PPP įgyvendinimo privalumai plačiai aptariami daugelio kitų autorių, išskiriant juos į viešojo finansavimo taupymą, pasinaudojant privataus kapitalo investicijomis (Zhao, Saunoi-Sandgren ir Barnea, 2011), pagal bendradarbiavimo partnerių, partnerystės struktūros ir tipo pasirinkimą (Kavaliauskaitė ir Jucevičius, 2009), projekto įgyvendinimo laiko taupymą ar perkeliant tam tikras rizikas privačiam sektoriui, kurias šis sugeba suvaldyti geriau (Savas, 2000), netgi vienu iš įrankių pasirenkant finansinio poveikio priemones privačiam sektoriui, kai jis nesielgia taip, kaip nori viešasis, bei apdovanojamas papildoma naudos dalimis, jei elgiasi atvirkščiai (S. Harris, cituojamas pagal (Jakutyte, 2012, p. 15)).

M. Dūda (2010), remdamasis daugeliu autorių, įvardina vieną iš esminių stimulų formuoti viešojo ir privataus sektorių partnerystę – „leidžia padalyti rizikas partneriams, kurie jas geba efektyviausiai valdyti“ (p. 141), taip mažinant tokiu bendradarbiavimu paremtų projektų sąnaudas ir kuriant pridėtinę vertę. 2008 m. N. K. Paliulio (2008) vadovautoje studijoje pateikiamas viešojo ir privataus sektorių partnerystės projektams būdingas rizikos pasiskirstymas (1 pav.). Vienareikšmiškai, tai sukuria galimybę viešajam sektoriui, valdant galimas rizikas, pasinaudoti privataus sektoriaus įgūdžiais ir žiniomis.



Diskriminacinė teisinė rizika	Paklausos (apimties) rizika	Detalaus planavimo leidimų gavimas
Bendrojo planavimo leidimų gavimas	Infliacijos rizika	Projektavimas
	Bendra teisinė rizika	Kūrimas
Vykdomos veiklos standartų, kokybės nustatymas	Neįveikiamos aplinkybės (pranc. *force majeure*)	Atidavimas eksploatuoti
		Vykdoma veikla
		Projekto finansavimas
		Technologijos ir moralinis nusidėvėjimas

Šaltinis: Paliulis N. K. ir kt., 2008, p. 31

1 pav. Rizikos pasiskirstymas

Kitas svarbus aspektas partnerystei įgyvendinti – atsakomybės pasidalijimas bei inovacijų diegimas.

Pati partnerystė dar nėra sėkmės garantas ir labai priklauso nuo geros dalyvių sprendimų koordinacijos ir veiksmų. Taip pat svarbus faktorius – skirtingo požiūrio į partnerystę ir jos tikslus suderinimas.

Kaip ir bet kuris egzistuojantis reiškinys, taip ir viešojo ir privataus sektorių partnerystė, pasak E. Skietrio ir A. Raipos (2009), turi „esminius socialinės vertės kūrimo elementus, kurie turėtų būti matuojami“ (p. 13): įeiga, rezultatas, pasekmės ir poveikis. Autorių siūlomas šių dalių interpretavimas (Skietrys ir Raipa, 2009, p. 13):

- *Įeiga – tai resursai, reikalingi, kad kažkas įvyktų. Dažniausiai apskaičiuojami kaip kaštai.*
- *Rezultatas – tai, kas apibrėžta ir įgyvendinta projekto metu.*
- *Pasekmė – pokytis, išryškėjantis per ilgesnį laikotarpį.* Pavyzdžiui, pagerėjusi kibernetinio saugumo būklė arba išaugęs visuomenės sąmoningumas šioje srityje.
- *Poveikis – vertinimas, kuriam didelę įtaką daro lygiagrečiai įgyvendinamos kitos priemonės galinčios padidinti arba sumažinti naudą, kurios tikimasi.* Pavyzdžiui, nekonsoliduotas teisinis reguliavimas su vienas kitam prieštaraujančiais reikalavimais.

M. Buso (2016) teigia, kad viešojo ir privataus sektorių bendradarbiavimas gali pažengti daug toliau už savo tradicines įgyvendinimo formas „kuriant aukštos kokybės viešąsias paslaugas už mažą mokesčių mokėtojų ir naudotojų mokamą kainą“ (p. 3).

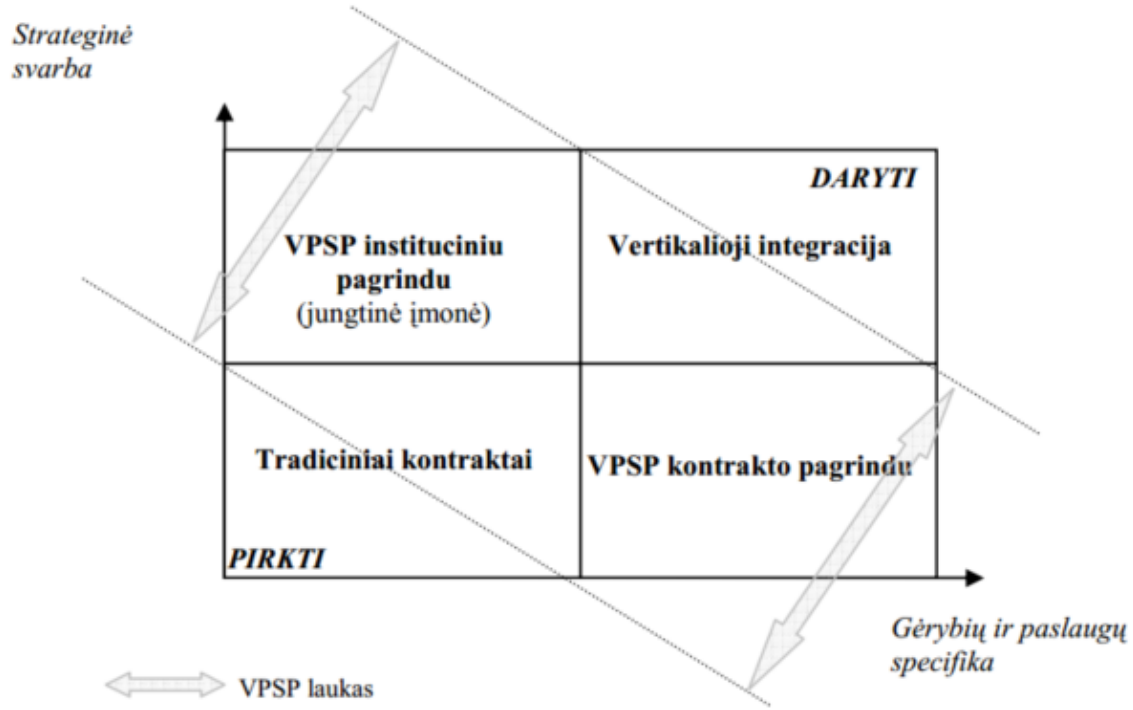
Šio teiginio pagrindimas gali būti 2014 m. užbaigtas 24 mokyklų projektas Atėnuose (Mantzoufas, 2017), kai remiantis Graikijoje priimtu PPP įstatymu Nr. 3389/2005, 2010 m. siekiant išspręsti mokyklų trūkumo ir jų infrastruktūros kokybės problemas užtikrinant švietimo sistemos rezultatus, geresnę šios infrastruktūros priežiūrą visą projekto ciklą, aukščiausius paslaugų standartus ir energijos sąnaudų taupymą, išnaudojant vieną iš PPP metodų - DBFO (angl. *design-build-finance-operation*, kurti-statyti-finansuoti-valdyti), kai privatus sektorius pilnai finansuoja sutarčių vykdymą su nuosavybės teise į sukurtą infrastruktūrą, o viešasis sektorius naudodamasis privataus sektoriaus sukurta viešąja nauda atlieka mėnesinius sutarties apmokėjimus pagal iš anksto nustatytus pateikiamos infrastuktūros kokybės kriterijus. Tokio bendradarbiavimo nauda abipusė – privatus sektorius atgauna investicijas su papildoma finansine grąža, o privatus sektorius naudojasi sutarties sudarymo metu užfiksuota planuojamos naudos įgyvendinimo kaina bei kokybiška ir šiuolaikiška infrastruktūra.

V. Kavaliauskaitė ir R. Jucevičius (2009) analizuodami PPP svarbą realizuojant regiono konkurencinę strategiją, apibendrindami savo tyrimo apimtyje pateikia tokią partnerystės sampratą: „VPP apibūdinama kaip bendradarbiavimas, kai viešojo sektoriaus įstaigos sudaro ilgalaikius susitarimus su privataus sektoriaus institucijomis dėl viešojo sektoriaus infrastruktūros objektų statybos ar valdymo, arba paslaugų teikimo (naudojant infrastruktūros objektus) bendruomenei viešojo sektoriaus institucijos vardu“.

Apibendrinant galime teigti, kad viešojo ir privataus sektorių partnerystė, kaip bendrinis visų tokio reiškinio formų samprata gali būti apibūdinama kaip – bendradarbiavimo instrumentų rinkinys (ekspertinės žinios, infrastruktūra, finansai ir pan.), kuris naudojamas viešojo intereso tikslams pasiekti, skirtas aktyviai į partnerystės kūrimą įtraukti privataus sektoriaus dalyvius pasidalinant rizikomis ir gaunama nauda. Čia tampa ypač svarbus valdymo elementas, kai „valdymas“ suprantamas kaip vaidmenų ir atsakomybių pasidalinimas: „kas turi atlikti“, „kas turi užtikrinti“ ir „kas yra atsakingas“ PPP apimtyje.

1.2. Viešojo ir privataus sektorių partnerystės formos

Analizuojant galimus bendradarbiavimo vienoje ar kitoje srityje aspektus svarbu apsibrėžti tokios partnerystės formas ir mechanizmus. M. Dūda (2010) siūlo viešojo ir privataus sektorių partnerystėje brėžti ribą tarp kontrakto pagrindu ir instituciniu pagrindu įgyvendinamų formų, pabrėždamas strateginę svarbą ir teikiamų viešųjų gėrybių specifiškumo įtaką lemiančius tokį pasirinkimą (2 pav.).

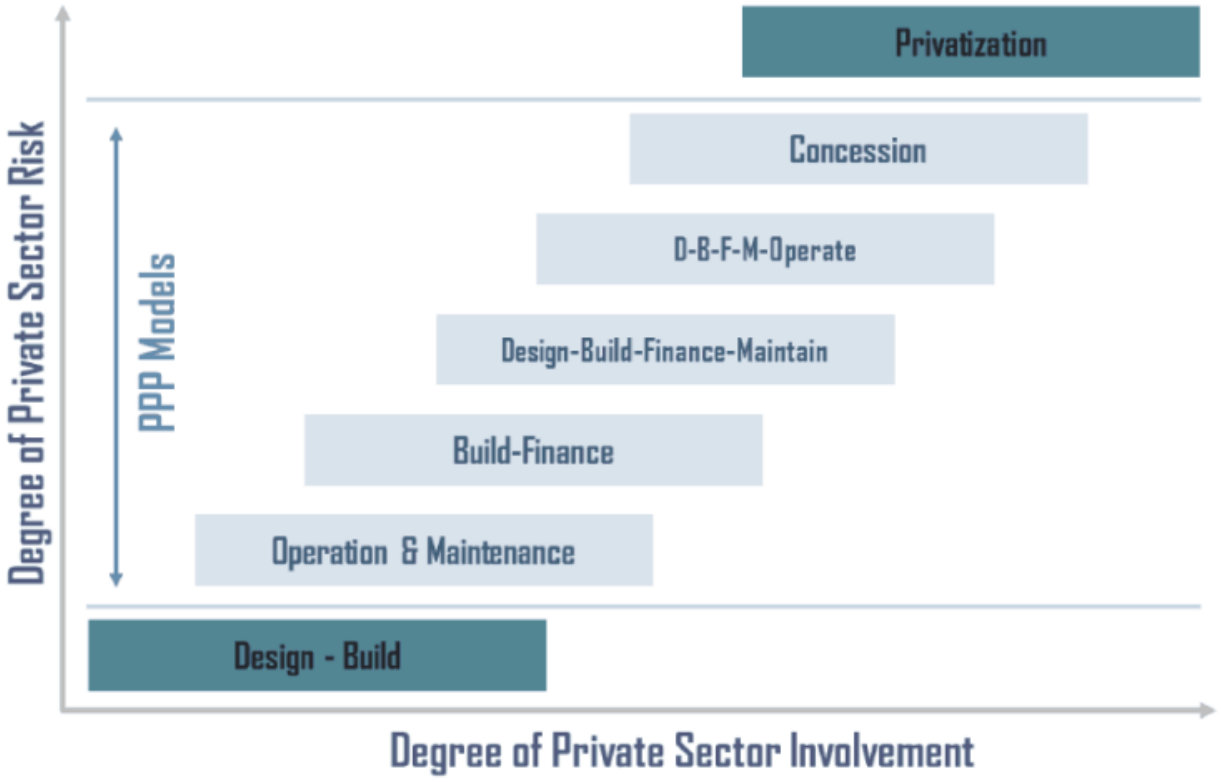


Šaltinis: Dūda, 2010, p. 142

2 pav. Viešojo ir privataus sektoriaus partnerystės formų pasirinkimas

Remiantis 2 paveikslu galime teigti, kad esant žemai gėrybių ir paslaugų specifikai ir aukštai strateginei svarbai, dažniausiai formuojama jungtinė viešojo ir privataus sektoriaus įmonė kaip savarankiškas juridinis asmuo. Tačiau esant nedidelei strateginei svarbai ir aukštam gėrybinių ir paslaugų specifikos poreikiui tokia partnerystė grindžiama kontraktu. Šios dvi formos gali būti papildomai skaidomos į: kontraktus, koncesijas, frančizes (nuomos), jungtines įmones, strategines partnerystes įtraukiant ir privatizaciją, kaip vieną iš galimų sprendimo būdų.

Tuo pačiu pabrėždami, kad PPP priklauso nuo rizikos perkėlimo lygio tarp viešojo ir privataus sektorių ir privataus sektoriaus įsitraukimo, galime teigti, kad didėjant PPP projektams privatus sektorius ne visada nori prisiimti dideles rizikas nepriklausomai nuo būsimos potencialiai didelės naudos ir visiška privatizacija ne visada tampa tinkamu sprendimu. 3 paveiksle pateikiama privataus sektoriaus prisiimamos rizikos ir įsitraukimo lygis atsižvelgiant į partnerystės sudėtingumą.



Šaltinis: transportgeography.org

3 pav. Rizikų perkėlimas ir privataus sektoriaus įsitraukimas PPP

Pagal privataus sektoriaus įsitraukimą PPP kategorizuoti siūlo E. Savas (2000), o pagal rizikas ir atsakomybes – McGraw-Hill (2009) . Tuo tarpu papildomai PPP galima būtų suskirstyti pagal turto būklę (Transportation Research Board, 2018) gaunant bendrą kokybišką naudą, nuosavybės perdavimą (National Cooperative Highway Research Program, 2009), finansinius susitarimus (United States Government Accountability Office, 2008) ar kompensavimo privačiam sektoriui būdus (McGraw Hill Construction, 2009).

E. Savas (2000) PPP formas išdėsto viešumo privatumo skalėje formuodamas ją nuo visiško tik viešojo sektoriaus dalyvavimo su minimaliomis partnerystės apraiškomis per paslaugų sutartis iki aktyvaus privataus sektoriaus dalyvavimo visapusiškai privatizuojant viešąją nuosavybę. Skalės viduryje atsiduria esminiai PPP modeliai: nuoma ir valdymas, kooperatyvas, LBO (nuoma, statymas ir valdymas), BTO (statymas, perdavimas ir valdymas), BBO (pirkimas, statymas ir valdymas) bei BOO (statymas, nuosavybė ir valdymas).

Remiantis greitkelio infrastruktūros įgyvendinimu (Transportation Research Board, 2009), kaip pavyzdžiu, galime apibrėžti privataus sektoriaus įsitraukimą nuo mažiausio iki didžiausio (žr. 1 lent.).

Pirmasis, DBB (projektavimas ir statymas), yra tradicinis projektų įgyvendinimo metodas, tuo tarpu paskutiniai du įvardinami kaip visiška privatizacija.

Pasak A. Akintoye (Akintoye, Beck ir Kumaraswamy, 2015) „privataus sektoriaus dalyvavimo forma partnerystėje gali apimti nuo paslaugų teikimo iki viešajam sektoriui priskiriamų išteklių nuosavybės valdymo“. Taigi, galime išskirti šiuos pagrindinius bendradarbiavimo formų apibūdinimus, kurie vienaip ar kitaip skirtingose teorijose išryškėja kaip esminiai:

- Technologijų perdavimas: viešasis sektorius > privatus sektorius,
- Gerųjų praktikų ir procesų iš privataus sektoriaus perėmimas,
- Mentorystė,
- „Donorų pasirinkimas“,
- Privataus sektoriaus remiami universitetiniai tyrimai,
- Universiteto ruošiami specialistai užpildantys privataus sektoriaus profesionalų poreikį.

Atsižvelgiant į aukščiau išvardintas prielaidas ir apibūdinimus galime partnerystę suskirstyti į kelias pagrindines rūšis (iš viešojo sektoriaus papildomai išskiriant mokslo sektorių, kuris gali būti taip pat ir privataus sektoriaus dalimi):

1. Viešojo ir privataus sektorių bendradarbiavimas,
2. Viešojo ir viešojo sektorių bendradarbiavimas,
3. Privataus ir mokslo sektorių bendradarbiavimas,
4. Mokslo ir privataus sektorių bendradarbiavimas,
5. Mokslo ir viešojo sektorių bendradarbiavimas.

Atitinkamai pagal privataus sektoriaus turimų išteklių ar įsitraukimo lygį, taip pat rizikų perkėlimą ir atsakomybių delegavimą, galime išskirti šiuos pagrindinius viešojo ir privataus sektorių bendradarbiavimo formas pavaizduotas 1 lentelėje.

1 lentelė. Partnerių nuosavybės, atsakomybių ir įsitraukimo lygis

Partnerystės rūšis	Partnerystės forma	Apibūdinimas
Ne partnerystė (tradicinė prieiga)	DBB (Design-Bid-Built) – projektavimas, susitarimas ir statymas	Tradicinis projekto įgyvendinimo būdas, kai viešasis sektorius perka iš privačių bendrovių įvairias prekes, viešąsias paslaugas ar darbus.
Privataus ir viešojo sektorių partnerystė – finansuoja viešasis sektorius	DB (Design-Build) – projektavimas ir statyba	Projektavimo ir statybos dalys apjungiamos vienu susitarimu. Toks suliejimas taupo projekto įgyvendinimo laiką ir finansavimo biudžetą didinant kokybę.

1 lentelės tęsinys kitame puslapyje

Partnerystės rūšis	Partnerystės forma	Apibūdinimas
	O&M (Operation and Maintenance) – nuoma ir valdymas	Privatus sektorius naudoja ir prižiūri viešojo sektoriaus valdomą turtą, kurio priežiūra finansuojama iš viešojo sektoriaus lėšų.
	DBOM (Design-Build-Operate-Management) – projektavimas, statyba, naudojimasis ir valdymas	Privatus sektorius įgyvendinęs projektą tam tikrą laiką juo disponuoja užtikrindamas iš anksto susitartus paslaugos kokybės parametrus už kurių išlaikymą (paslaugų pateikiamumas kaip viešoji nauda) jam kompensuoja viešasis sektorius.
Privataus ir viešojo sektorių partnerystė – finansuoja privatus sektorius	LBO (Lease-Build-Operate) – nuoma, statyba ir valdymas	Privačiam sektoriui suteikta ilgalaikė nuoma koncesijos pagrindu valdyti plečiant ar investuojant papildomai. Privataus sektoriaus investicijos susigrąžinamos per mokesčius, tačiau nuosavybės teisė priklauso viešajam sektoriui.
	DBF (Design-Build-Finance) – projektavimas, statyba ir finansavimas	Privatus sektorius tampa dalininiu rėmėju susigrąžindamas indėlius iš viešųjų fondų, kai yra visiškas dotacijos susitarimas, tačiau finansai atsiranda vėliau nei įvyksta statyba. Santykiai dažniausiai trumpalaikiai.
	BOT (Build-Operate-Transfer) – statymas, naudojimasis ir perdavimas	Privatus sektorius, frančizės pagrindu, finansuoja, stato ir nuosavybės teise valdo rinkdamas mokesčius iš naudotojų, o po tam tikro laiko perleidžia nuosavybę viešajam sektoriui.
	BTO (Build-Transfer-Operate) – statymas, perdavimas, valdymas	Privataus sektoriaus vystytojas finansuoja ir stato ir po to perleidžia nuosavybės teisę viešajam sektoriui. Tačiau privatus sektoriui paliekama teisė valdyti renkant mokesčius su tikslu susigrąžinti investicijas ir gauti pelną.
Privatizacija	BOO (Build-Own-Operate) – statymas, nuosavybė ir valdymas	Privatus vystytojas, frančizės pagrindu, finansuoja, stato, nuosavybės teise valdo, tačiau yra ribojamas reguliuojamos veiklos. Andalogiška situacija kaip ir BOT atveju, tik po tam tikro laiko turtas nėra perleidžiamas viešajam sektoriui.
	BBO (Buy-Build-Operate) – įsigijimas, statymas ir valdymas	Esama viešojo sektoriaus nuosavybė, frančizės pagrindu, perduodama privačiam sektoriui,

1 lentelės tęsinys kitame puslapyje

1 lentelės tęsinys

Partnerystės rūšis	Partnerystės forma	Apibūdinimas
		kuris modernizuoja, vykdo plėtrą ir valdo.
Ištekliaus pardavimas		Viešas sektorius pilnai atiduota savininko teises viešai finansuojamo ištekliaus privačiam sektoriui valdyti

Šaltinis: adaptuota pagal United States Government Accountability Office, 2009, p. 8

Remiantis K. Paliuliu ir kt. (2008) „dabartiniu metu sėkmingiausia PPP forma yra laikoma taip vadinama privačioji finansinė iniciatyva (angl. *Private Finance Initiative* – PFI), pagal kurią privatus sektorius [...] investuoja [...], o viešas sektorius atsiskaito už tai [...] mokėdamas privačiai kompanijai dalimis“ (p. 28).

Apibendrinant galime teigti, kad pagrindinės PPP įgyvendinimo formos yra[1]:

- Sutartinė
  - Kontraktas (pvz. projektavimas, statyba – DB; nuoma ir valdymas – OM),
  - Koncesija (pvz. statyba, perdavimas ir valdymas – BTO),
  - Franšizė (pvz. pirkimas, statyba ir valdymas – BBO; statyba, nuosavybė ir valdymas – BOO),
  - Kooperacija
- Institucinė
  - Jungtinė įmonė
- Strateginė partnerystė

Nepaisant kritikos partnerystei, per paskutinius dešimtmečius, vyriausybės aktyviai naudodamos įvairias aukščiau išvardintas formas sėkmingai įgyvendino svarbiausius infrastruktūrinius projektus, tokius kaip mokami keliai, oro uostai, mokyklos ir ligoninės, aprūpinimas vandeniu ar nuotėkų valymo įrenginių statyba tiek nacionaliniu, tiek savivaldybių mastu pasinaudojant viešaisiais finansais ar privatizacijos galimybėmis pasidalinant kylančiomis rizikomis.

1.3. Viešojo ir privataus sektorių partnerystės įgyvendinimas

Nepriklausomai nuo privataus sektoriaus poreikių ir siekiamų rezultatų, vis vien išlieka viešojo sektoriaus, kaip vedančiojo, svarbus vaidmuo, kuris, remiantis teisiniu reglamentavimu, gali paskatinti arba nuslopinti partnerystės iniciatyvas (Dūda, 2010). Ypatingai uolus reglamentuojančių teisinių įrankių

[1] Sutrumpinimai pateikiami nuo angliško formos įvardinimo pirmųjų raidžių

atsiradimas gali pastūmėti motyvacijos tokiai partnerystei sumažėjimą, o nepakankamas – kelia piktnaudžiavimo grėsmes.

Kaip ir kiekvieno aiškaus projekto įgyvendinimas, taip ir partnerystės atsiradimo kertinis elementas yra poreikis. Jo atsiradimas, jei laikytume, kad iniciatyva priklauso viešajam sektoriui, turi būti paremtas ekonomine arba teisinės aplinkos analize. Tačiau kiti autoriai kelia efektyvumo leitmotyvą partnerystei pagrįsti, kuris paskui save veda ideologiją-politiką ir ekspertinės kompetencijos trūkumus (Bel, Brown ir Marques, 2016).

Kaip teigia M. Dūda, viešojo sektoriaus valdžios institucijos, inicijuojančios partnerystės projektus, privalo atsakyti į esminius klausimus (Dūda, 2010):

- ar partnerystė leis viešajam sektoriui pasiekti užsibrėžtus tikslus?
- ar partnerystė yra finansiškai pigesnė alternatyva, nei tradicinis viešųjų paslaugų teikimo būdas?
- kokia papildoma ekonominė ir (ar) socialinė vertė bus sukurta?

T. Liu, Y. Wang ir S. Wilkinson (2016) analizuodami kritinius viešojo ir privataus sektorių bendradarbiavimo faktorius įtakojančius efektyvumą Australijoje ir Kinijoje teigia, kad nenusisekę tokio bendradarbiavimo pavyzdžiai grindžiami neefektyviais ir neproduktyviais įgyvendinimo procesais: nepamatuoti įgyvendinimo terminai, dideli kaštai, kompetencijos (žinių spragos) ir skaidrumo stoka, neišnaudotos viešųjų pirkimų galimybės – tiesioginės ar konkurencingumą skatinančios derybos ir pan. Autoriai, remdamiesi A.P.C. Chan, išskiria 5 kritinius šio bendradarbiavimo sėkmės faktorius (Liu, Wang ir Wilkinson, 2016, p. 703):

1. makroekonominė aplinka,
2. atsakomybės tarp viešojo ir privataus sektorių pasidalinimas,
3. skaidrus ir efektyvus viešųjų pirkimų įgyvendinimas,
4. stabili politinė ir socialinė aplinka,
5. protinga vyriausybinė kontrolė.

C. Skelcher (2010), kaip svarbų PPP įgyvendinimo elementą įvardina pačios partnerystės valdymą, išskirdamas keturis tokio valdymo tipus:

- Teisinis valdymas,
- Reguliuojamasis valdymas,
- Demokratinis valdymas,
- Organizacinis valdymas.

Teisinis valdymas. Šis valdymo tipas labai priklauso nuo konkrečios šalies teisinės bazės ir konstitucinių normų su atitinkamomis jurisdikcijomis, kai viešasis sektorius įtvirtina teisinius pagrindus

partnerystei taip sukurdamas stiprius ryšius su valstybe siekiant naudos visuomenės interesui. Šioje apimtyje, kai kuriais atvejais, galime kalbėti ir apie steigiamas bendrines organizacijas, kuriančias vienokią ar kitokią vertę, kurių dalininkais tampa abi partnerystės pusės. Tokių bendrinių organizacijų steigimas ir jų kuriamos naudos bendradarbiaujant akademiniam, privačiam ir viešajam sektoriams galėtų būti kibernetinio saugumo priemonių kūrimas eliminuojant tokių priemonių įsigijimą už valstybės ribų, taip apsaugant ne tik rinką, tačiau ir užtikrinant šias kibernetinio saugumo priemones naudosiančius vartotojus, t.y., pavyzdžiui, dalinai apsaugant tiekimo grandinę nuo galimai kenkėjiškos programinės įrangos. Tokio bendradarbiavimo minusai yra bendrinių organizacijų atliktų finansinių injekcijų nuvertėjimai arba dalininkų pasikeitimai.

Reguliuojamasis valdymas. Šio tipo valdymo esmė yra taisyklių rinkinys, kurio dėka partnerystė „pririšama“ prie viešojo sektoriaus kaip kliento. Tai apima teisinius ir sutartinius santykius bei procedūras, kuriomis vadovaujasi abi bendradarbiaujančios pusės. Fundamentaliu aspektu tokio tipo valdymas remiasi teisinių reikalavimų viešajam klientui dėl procesų, kurių reikia laikytis, taikymu ir privataus sektoriaus dalyvavimo partnerystėje kriterijais dėl viešųjų pirkimų organizavimo. Visiems neigiamiems tokios valdymo formos atvejams eliminuoti vyriausybė gali pasinaudoti privataus sektoriaus žiniomis ir patirtimi (pvz. dalyvaujant viešuosiuose pirkimuose).

Demokratinis valdymas. Tokio valdymo poreikis atsiranda visada, kai tik valstybė perkelia viešojo sektoriaus atsakomybes ar įtvirtina bendradarbiavimą su trečiosiomis šalimis ir atsiranda tokios atsakomybės paskirstymo elementas.

Organizacinis valdymas. Esminis tokio valdymo tikslas yra užtikrinti, kad partnerystė (bet kokia jos forma – sutartinis bendradarbiavimas, bendra organizacija ir pan.) valdoma taip, jog verslo ir investuotojų lėšų ateitis nėra pernelyg pasiduodanti rizikoms.

Įgyvendinimą galime išskirti į tris pagrindinius lygius:

- Valstybinis lygis,
- Savivaldos lygis,
- Tarpvalstybinis lygis.

Įgyvendinant viešojo ir privataus sektorių partnerystę svarbūs aspektai tampa teisingas tikslo pasirinkimas, kaštų nusistatymas ir biudžeto plano laikymasis, atsakomybių ir vaidmenų pasiskirstymas, dalyvių kompetencijos, partnerystės skaidrumas, viešųjų pirkimų reglamentavimo orientacija į bendradarbiavimo procesus, protinga vyriausybės kontrolė bei teisingo valdymo parinkimas.

1.4. Viešojo ir privataus sektorių partnerystė kibernetinio saugumo srityje

Kibernetinės atakos kelia unikalias grėsmes daugeliui: nuo elektros energijos tiekimo sutrikdymo energetikos sektoriuje iki konfidencialios informacijos nutekėjimo finansų institucijose. Tai sukuria aiškų kibernetinio saugumo prioretizavimą privačiame ir viešajame sektoriuose. Daugelio valstybių įstatymų leidžiamoji valdžia aiškiai simpatizuoja viešojo ir privataus sektorių partnerystės svarbai siekiant apginti kritinę infrastruktūrą, kelti gyventojų sąmoningumo lygį ir užtikrinti duomenų perdavimo tinklų vientisumą.

Didžioji dalis kritinės infrastruktūros pasaulyje priklauso privačiam kapitalui, todėl daugelis kompanijų jau turi įsidiegę įvairias kibernetinio saugumo programas su unikaliomis ekspertinėmis kompetencijomis ir išugdyta patirtimi kylančioms grėsmėms. Tuo tarpu viešasis sektorius sukoncentraves tyrimų ir teisinio kibernetinių nusikaltėlių persekiojimo pajėgumus.

Daugeliui kibernetinio saugumo grėsmių užkardyti ne maža dalis valstybių savo kibernetinio saugumo strategijose kaip pagrindinį „ginklą“ nurodo bendradarbiavimą. Informacijos apie grėsmes dalybos, sąmoningumo skatinimas – visa tai pasiekiama per du esminius įrankius: informacijos dalinimosi ir analizavimo institucijas bei viešojo ir privataus sektorių bendradarbiavimo vystymą.

Pati bendradarbiavimo apimties sąvoka užtikrinant kibernetinį saugumą nuo klasikinės viešojo ir privataus sektorių partnerystės skiriasi. Jei standartinėje PPP apimtyje kalbame apie tai, kad viešasis sektorius iškelia uždavinį, privatus jį įgyvendina, o paskui viešasis sektorius įsipareigoja to uždavinio rezultatus įsigyti ar naudoti, tai kibernetinio saugumo srityje, remiantis K. Bechkoum ir kt. (2017) atliktu tyrimu, kalbame apie „bendradarbiavimo susitarimą, pagal kurį vyriausybės ar viešosios organizacijos bendradarbiauja su pramonės ar akademine bendruomene, siekdamos sušvelninti kibernetinio saugumo riziką stiprindamos kibernetinės gynybos pajėgumus, bendradarbiaudamos ir keisdamosi informacija“ (p. 8). Tuo tarpu Europos Sąjungos ryšių ir informacijos agentūra apibrėždama CSP3 kibernetinio saugumo srityje nurodo, kad „viešojo ir privataus sektorių partnerystė yra istoriškai susiklostęs ilgalaikis susitarimas ar bendradarbiavimas tarp dviejų ar daugiau viešojo ir privataus sektorių sričių“ (ENISA, 2017, p. 7). Tarp kitų tokio bendradarbiavimo sudėtinių dalių K. Bechkoum ir kt. (2017) įvardina pasitikėjimą tarp partnerių ir vaidmenų bei atsakomybių (įsipareigojimų) aiškumą.

ENISA (2017) viešojo ir privataus sektorių partnerystės bendradarbiavimo modelių pristatyme išskyrė šiuos būtinus analizuoti aspektus (p. 5):

- *Nepakankami žmogiškieji ištekliai abiejose bendradarbiavimo pusėse,*
- *Nepakankamas viešojo sektoriaus finansavimas ir turimi resursai, kurie neatitinka privataus sektoriaus lūkesčių,*

- *Viešojo ir privataus sektorių dialogo ir suvokimo lygio nustatymas,*
- *Viešojo ir privataus sektorių bendradarbiavimo minties sklaida tarp mažojo ir vidutinio verslo,*
- *Nepakankama lyderystė ir teisinė bazė.*

Nepakankami žmogiškieji ištekliai abiejuose partnerystės pusėse. Valstybės dažniausiai neskiria tinkamo dėmesio skiriant žmogiškuosius išteklius siekiant užtikrinti kibernetinį atsparumą, tuo labiau nelaiko CSP3 pakankamu prioritetu šiam atsparumui įgyti. Tuo tarpu privačiuose sektoriuose kibernetinio saugumo specialistai dažniausiai užimti kasdienėmis užduotimis. I. Namavičiūtė (2018) siūlo tarpsektorinį bendradarbiavimą pradėti kibernetinio saugumo švietimo srityje, kai iniciatyvos ėmęsis viešasis sektorius kviestu verslo ir akademijos atstovus aptarti bendrus iššūkius ir ieškotų sprendimų drauge į šį procesą įtraukiant švietimo bei mokslo sričių specialistus siekiant, visų pirma, sukurti kibernetinio saugumo kompetencijų žemėlapį, kurio pagrindu, turint suvokimą kiek ir kokių specialistų reikia, būtų ugdomi srities talentai. Autorė taip pat įvardina specialistų ir darbuotojų perkvalifikavimo svarbą bei kibernetinio saugumo žinių trūkumo eliminavimo pasiūlymus įtraukiant srities temas į mokymų programas ar papildomai remtis trumpalaikėmis iniciatyvomis, pvz.: vasaros stovyklos vaikams, mergaičių sudominimas į kibernetinio saugumo sritimi, įvairūs vietinės reikšmės ir tarpmokykliniai konkursai. Tačiau šios iniciatyvos reikalauja viešojo sektoriaus lyderystės – teisinės bazės dėl kibernetinio saugumo švietimo organizavimo, įtraukimo į įvairialypį ugdymą ar aukštojo mokslo studijų programas. Be abejo, siekiant tikslo, šios iniciatyvos (moderuojamos akademinės visuomenės) turėtų panaikinti privataus ir viešojo sektoriaus abejones kibernetinio saugumo programų kokybe.

Nepakankami ir neatitinkantys privataus sektoriaus lūkesčių viešojo sektoriaus finansiniai resursai. Vyriausybės dažniausiai neskiria pakankamo valstybinio biudžeto dalies, kuris būtinas CSP3 plėtrai, taip pat neatlieka tinkamo planavimo ankstyvosiose biudžeto formavimo stadijose. Nepaisant to, viešasis sektorius atlieka ilgalaikės perspektyvos planavimą kuriant strategijas ir veiksmų planus skirtus CSP3 įgyvendinimui. Kai tuo tarpu privatus sektorius egzistuoja dinaminėje aplinkoje ir ilgalaikės strategijos apima ne ilgesnius kaip kelerių metų periodus. Prie šio aspekto prisideda ir tai, kad viešasis sektorius priekaištaudamas privačiam sektoriui dėl nepakankamo įsitraukimo į kibernetinio saugumo strategijos kūrimą ar įgyvendinimą sulaukia kontrargumentų dėl nepakankamo grėsmių švelninimo investicijų pagrindimo šios strategijos įgyvendinimo biudžetui (Carr, 2016). Čia kyla viena iš esminių CSP3 problemų: viešojo sektoriaus lūkestis, kad privatus sektorius investuos į kibernetinį saugumą nekreipdamas dėmesio į savo sąnaudų-naudos analizę ir taip pilnai patenkins viešąjį interesą – kitaip sakant, užtikrins nacionalinį saugumą.

Viešojo ir privataus sektorių dialogo ir suvokimo lygio nustatymas. Standartizuoti ir nustatyti vienodą komunikaciją abiejuose CSP3 pusėse tai pat yra nelengvas uždavinys dalyviams. Ypač aiškios komunikacijos nebuvimo barjeras dar labiau pasunkina ir taip sudėtingą CSP3. Tai sukuria nesusipratimus abiejose pusėse: viešojo ir privataus sektorių darbo ypatumai ir skirtumai, strateginis ir techninis suvokimas, darbo kultūros skirtumai ir t.t.

Partnerystės minties sklaida įtraukiant ir mažąjį bei vidutinį privačius kapitalus. Nedidelio kapitalo privatus sektorius dažniausiai neturi patirties dalyvaujant CSP3. Toks bendradarbiavimas sukuria abipusę naudą: „mažieji“ mokosi iš „didžiųjų“, viešasis sektorius užsitikriną visapusišką kibernetinį atsparumą valstybiniu lygmeniu. A. D. Givens ir N. Busch (2013) teigia, kad „individualus pasiruošimas gali būti transformuotas į visuomeninį pasirengimą“ (p. 41), kai kiekvienas mažas valstybės elementas tampa visuomenės evoliucijos iš kibernetinio saugumo į kibernetinį atsparumą dalimi siekiant suvaldyti įvairias grėsmes iki joms vienaip ar kitaip materializuojantis.

Nepakankama lyderystė ir teisinė bazė. Viešojo sektoriaus dvejonės dėl lyderystės partnerystėje prisiėmimo įneša tam tikrų abejonių privataus sektoriaus dalyvavimui. Žinių ir patirties dalybos, taip pat aktyvus dalyvavimas diskusijose ir CSP3 veikloje didina šio reiškinio efektyvumą, tačiau tam reikalinga tvirta lyderystė ar moderatoriaus rolės prisiėmimas. Tuo tarpu ginčai ar nesutarimai bei nuomonių skirtumai tarp paties viešojo sektoriaus elementų labai mažina privataus sektoriaus pasitikėjimą CSP3. Dažniausiai verslas tikisi tvirtų valdžios veiksmų ir užtikrintumo rytdiena. Tinkama teisinė bazė nustatanti dalyvių atsakomybes ir vaidmenis sustiprina partnerystę ir apibrėžia konkrečius reikalavimus (įnašą) ir siekiamus tikslus (naudą). Reikėtų eliminuoti viešojo sektoriaus nuostatą – atidžiai stebėti ir kontroliuoti, keičiant ją norimo tikslo siekimo koordinavimu bei motyvavimo instrumentų parinkimu (Carr, 2016, p. 60).

Šalia šių aspektų dar galime paminėti keletą esminių: privataus sektoriaus motyvacija dalyvauti projektuose, dalyvių bendradarbiavimo sutarimas dėl teisinės bazės kūrimo (pavyzdžiui, viešojo sektoriaus atstovų dalyvavimas atsakingo informacijos atskleidimo susitarimų sąlygomis (angl. *responsible discloser* arba *non-disclosure agreement*)), viešojo sektoriaus lyderystė, mažojo ir vidutinio verslo įtraukimas ir pan.

Efektyvių bendradarbiavimo tarp viešojo ir privataus sektorių modelių tyrimo ataskaitoje ENISA (2011) išskiria šias pagrindines tokio bendradarbiavimo karkaso sudarymo dalis:

- vaidmenų ir atsakomybių apibrėžimas,
- tarpusavio ryšių apibrėžimas,
- bendradarbiavimo sričių apibrėžimas.

Dar 2013 m. JAV prezidentas B. Obama, nusivylęs JAV Kongreso nesugebėjimu priimti visapusiško kibernetinio saugumo įstatymo, išleidžia nurodymą Nr. 13636, kuriame įgalioja NIST išplėtoti savanoriško

viešojo ir privataus bendradarbiavimo gaires (kurios labiau orientuotos į kritinę infrastruktūrą valdančias organizacijas, tačiau tai niekaip jų neatitolina ir nuo kitų privataus sektoriaus dalyvių). Daugeliu atveju kalbant apie partnerystę yra laikoma, kad valstybė yra atsakinga už saugumą, ypač nacionalinį, tuo labiau kai visa tai suvedama į kritinę infrastruktūrą, nors kibernetine erdve naudojasi visi, todėl atsakomybė už kibernetinį saugumą gula ant visų valstybės piliečių pečių.

Privatus sektorius kibernetinio saugumo iššūkį suvokia kaip finansinių ir grėsmių reputacijai rinkinį, o ne kaip grėsmes bendrai viešajai naudai, kas yra kibernetinio saugumo užtikrinimo tikslas valstybės požiūriu.

Privatus sektorius prisiima atsakomybę už savo sistemų saugumą iki lygio, kuris yra pelningas, t.y. iki tol kol prevencinės priemonės neviršija patiriamos prastovos nuostolių ir orientuojasi į „žemo lygio“ grėsmes, tokias kaip haktivizmas, hakeriai kitas kibernetinis „triukšmas“. Tuo pačiu privatus sektorius tikisi, kad didesnes grėsmes (organizuotas nusikalstamumas, terorizmas, priešiškų valstybių remiami hakeriai ir pan.) suvaldys valstybė. Deja, puikus tokio nebendradarbiavimo ir neefektyvaus atsakomybių pasiskirstymo – viešojo ir privataus sektorių dialogo ir suvokimo lygio neegzistavimo – pavyzdys yra 2014 m. kibernetinė Sony Picture ataka, kai valstybės remiami kompiuteriniai įsilaužėliai atakavo privataus kapitalo įmonę taip atsakydami į vieno iš kompanijos kuriamų filmų išleidimą į apyvartą, kuriame nepagarbiai atsiliepiama apie ataką organizavusios valstybės vadovą (Zetter, 2014), kai tuo tarpu atlaikyti valstybinio lygio ataką privačiam sektoriui nėra jokių galimybių ir čia atsakomybės pasidalijimas su viešuoju sektoriumi (krizės valdyme) ar žvalgybinės informacijos atskleidimas privačiam sektoriui būtų sąlyginai sumažinęs patiriamo sutrikimo mastą.

Pirmi žingsniai CSP3 kryptimi ES mastu įvyko 2012 m., kai ENISA išleido geruųjų praktikų gaires siekiant partnerystės. Praėjus tam tikram laikui Europos komisija atsižvelgdama į 2015 m. priimtą Skaitmeninę strategiją 2016 m. patvirtino viešojo ir privataus sektorių bendradarbiavimo įtraukimą į bendrą Europos kibernetinio atsparumo sistemą bei tokio bendradarbiavimo poreikį kibernetinio saugumo inovacijų pramonėje[2]. Šio dokumento pagrindu sukurtas „Horizon 2020“ programos karkasas, kurio esmė paremta sutartiniais santykiais tarp partnerystėje dalyvaujančių šalių įsipareigojimu remti ES konkurencingumo ir pramonės lyderystės strateginės svarbos mokslinius tyrimus ir inovacijų veiklos plėtrą bei įgyvendinimą.

Europos Komisija (2016) darbiniame dokumente dėl viešojo ir privataus sektorių partnerystės kibernetinio saugumo srityje sutartinės sutarties teigiama, kad CSP3 yra „mokslinių tyrimų ir inovacijų srities priemonė padedanti siekti pasiūlos ir paklausos tikslų“ (p. 18), taip pat instrumentas struktūrizuojant

[2] http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=16545 Prieiga per internetą 2018 m. spalio mėn. 8 d.

ir koordinuojant skaitmeninės pramonės saugą „maksimizuojant prieinamų resursų geresnę koordinaciją tarp šalių narių fokusuojantis į kelis techninius prioritetus“ (p. 17). Toks instrumentas turi būti naudojamas:

- siekiant sutelkti privataus ir viešojo sektorių resursus siekiant sustiprinti pramonės sektorių kibernetinį saugumą koncentruojantis į inovacijas ir siekiant bendrai sutartų strateginių tyrimų ir inovacijų plėtros tikslų,
- padėti stiprinti pasitikėjimą tarp valstybių narių ir pramonės subjektų, skatinant bendradarbiavimą "iš apačios į viršų" mokslinių tyrimų ir inovacijų srityje (European Commision, 2016, p. 18),
- skatinti kibernetinio saugumo pramonę, derinant kibernetinio saugumo produktų ir paslaugų paklausą ir pasiūlą, taip pat leisti pramonei veiksmingai apibrėžti būsimus galutinių vartotojų poreikius (European Commision, 2016, p. 18),
- panaudojant "Horizon 2020"[3] finansavimą ir didinant turimų pramonės fondų poveikį geriau koordinuoti ir labiau susitelkti į kelis techninius prioritetus,
- užtikrinti Europos kibernetinio saugumo ir privatumo elektroninėje erdvėje kompetencijas.

Remdamiesi ENISA (2017, p. 11) pateiktais bendradarbiavimo modeliais galime išskirti kelias varomąsias jėgas privataus ir viešojo sektorių partnerystės atsiradimui:

1. Ekonominiai interesai – natūrali privataus sektoriaus dalyvavimo partnerystėje motyvacija.
2. Teisinis reglamentavimas – partnerystė sukuriama kaip specifinių įstatymų įgyvendinimas apsprendus to pagrįstumą (pvz. kritinių situacijų ir krizių valdymas).
3. Ryšiai su viešuoju sektoriumi – kai valstybė leidžia privačiam sektoriui dalyvauti teisinės bazės kūrime, taip sudarant galimybes dalintis tarpusavio žiniomis.
4. Socialiniai interesai – tikslas iškelti kibernetinį saugumą į aukštą politinį lygmenį tam, kad užtikrintas kibernetinis atsparumas leistų veikti be reikšmingų pertrūkių.
5. Kiti interesai – teisinio reguliavimo įgyvendinimas suteikiant viešojo ir privataus sektorių partnerystės galimybes ir pan.

Esmine PPP atsiradimo priežastimi, kaip bendrą abiejų dalyvaujančių pusių tikslą, galime laikyti kibernetinio saugumo lygio kėlimą.

ENISA (2017) atliktame tyrime įvardina apibendrintas šio tikslo siekimo priežastis nurodytas 2 lentelėje.

[3] https://ec.europa.eu/programmes/horizon2020/what-horizon-2020

2 lentelė. Dalyvavimo partnerystės veikloje bendriniai tikslai

Privatus sektorius	**Viešas sektorius**
Galimybė gauti prieigą prie viešųjų išteklių	Geresnis kritinės infrastruktūros (kaip vieno iš esminių šių laikų valstybės egzistavimą užtikrinančio elemento) gynybos suvokimas
Galimybė įtakoti teisinį reguliavimą ar teisės aktų kūrimą	Galimybė sukurti sinergiją tarp skirtingų privataus sektoriaus iniciatyvų
Prieiga prie viešojo sektoriaus valdomų žinių ir žvalgybinės informacijos	Prieiga prie privataus sektoriaus išteklių (pvz. ekspertų)
Galimybė užsitikrinti tiekiamos produkcijos kokybę, kurią savo garantijomis patvirtina valstybė	
Dalinimasis žiniomis, ekspertine nuomone ir gerosiomis praktikomis	
Tarpusavio pagalba kibernetinio atsparumo stiprinime	
Augantis pasitikėjimas tarp viešo-viešo, privataus-privataus, viešo-privataus sektorių siekiant operatyvumo ir proaktyvumo kritinėse situacijose ir krizės akivaizdoje.	
Tiesioginis ir patikimas kontaktas su kitomis organizacijomis	

Šaltinis: ENISA, 2017, p. 13

J. Bakster pagrindinį CSP3 atsiradimo tikslą, siekiant bendradarbiavimo efektyvumo, skaido į tris būtinus kibernetiniam saugumui elementus (Baxter, et al., 2009, p. 8):

1. *Detektavimas: partnerystė turi apsibrėžti, identifikuoti ir stebėti nerimą keliančius reiškinius (įvairias kibernetinio saugumo anomalijas).*
2. *Apsauga: turi būti užtikrinta atitiktis bendriems saugumo standartams skiriant atitinkamas sankcijas nesilaikantiems susitarimų*
3. *Atsakas: turi būti suteikiamos priemonės atlikti kibernetinių incidentų tyrimus, analizuoti pažeidžiamumus, diegti trumpalaikius saugumo pataisymus ir efektyviai identifikuoti tikrąsias priežastis ir jų sukėlėjus*.

Nepaisant išsakomų argumentų ar tiriamųjų darbų analizės bei keliamų tikslų, galime teigti, kad pagrindiniai PPP elementai kibernetinio saugumo srityje susideda iš:

1. Atsakomybių paskirstymo,
2. Suteikiamos ar gaunamos naudos (žinios, patirtis, garantijos, dalyvavimas teisinės bazės kūrime ar specialistų ruošime, prieigos prie valdomų išteklių ir pan.),
3. Ryšių palaikymo (tame tarpe pasitikėjimo ugdymo ar bendradarbiavimo krizės akivaizdoje).

ENISA (2017) publikacijoje teigiama, kad PPP kibernetinio saugumo srityje modelius galime suskirstyti į keturias pagrindines grupes pavaizduotas 4 paveiksle.

Institucinis bendradarbiavimas, kaip teigia ENISA (2017), orientuotas į kritinę infrastruktūrą ir jos veiklos palaikymą. Svarbus niuansas – partnerystėje dalyvaujantis viešasis sektorius įgalinamas būti labiau orientuotas į privataus sektoriaus poreikius. Remiantis tokiu bendradarbiavimo modeliu siekiama užtikrinti aukštą kibernetinį infrastruktūros saugumą ir tinkamą teisinių reikalavimų įgyvendinimą. Tokio bendradarbiavimo pavyzdys galėtų būti Lenkijos vyriausybės saugumo centras[4] (angl. *The Government Centre for Security*).

Šaltinis: ENISA, 2017, p. 20

4 pav. Partnerystės modeliai užtikrinant kibernetinį saugumą

Į tikslą orientuotas bendradarbiavimas modeliuojamas tokiu atveju, kai kibernetinis saugumas suvokiamas kaip neatsiejama ekonominių veiklų dalis ir reikalauja tik papildomo palaikymo bei susidomėjimo iš viešojo sektoriaus. Partnerystės rezultatas – strateginiai sprendimai remiantys IT sritį ir sukuriantys prielaidas kibernetinio saugumo srities vystymui šalyje. Šio bendradarbiavimo modelis įgyvendintas Nyderlandų Karalystėje kaip Kibernetinio saugumo taryba[5].

Kibernetinio saugumo užsakomųjų paslaugų teikimu (angl. *Outsourcing*) grįsta partnerystė atsiranda tuomet, kai viešasis sektorius identifikuoja privataus sektoriaus poreikį, tačiau jo patenkinti nėra galimybių. Tokiu atveju CSP3 tampa savarankiška organizacija siūlanti paslaugas. Tačiau, vėlgi, pagrindinis tokios

[4] http://www.antyterroryzm.gov.pl/eng/anti-terrorism/institutions-and-servi/the-government-centre/662,dok.html
[5] https://www.cybersecurityraad.nl/index-english.aspx

organizacijos tikslas tampa kibernetinio saugumo lygio ir sąmoningumo ugdymo tarp partnerystės dalyvių didinimas. Kitaip tariant, informacijos ir profesinių žinių bei konsultavimo paslaugų įgyvendinimas. Kaip užsakomosiomis paslaugomis grįsta partnerystė gali būti įvardinta Vokietijos UP KRITIS[6] apimtyje.

Hibridinė partnerystė paremta užsakomųjų paslaugų teikimu ir instituciniu bendradarbiavimu. Tokia forma efektyvi tuomet, kai viešasis sektorius, kuris visada įvardinamas kaip esminis naudos gavėjas, neturi pakankamai resursų įgyvendinti kibernetinį saugumą nacionaliniu lygmeniu ir pasitelkdamas privataus sektoriaus dalyvius naudojasi jų pateikiamomis naudomis (žiniomis, ekspertize ir pan.). Kibernetinio saugumo srityje tokio bendradarbiavimo pavyzdys – bendrai kuriami CSIRT (angl. *Computer Security Incident Response Team*).

Apibendrinant galime teigti, kad PPP kibernetinio saugumo srityje taip pat remiasi atsakomybių ir rizikų paskirstymu bei ryšių tarp dalyvaujančių šalių palaikymu, tačiau patys įgyvendinimo modeliai dažniausiai nesiremia klasikinėmis PPP formomis ir apsiriboja informacijos dalybomis, ekspertinių žinių palaikymu, tam tikrų kibernetinio saugumo paslaugų tarpsektoriniu perkėlimu ar orientacija į keliamus tikslus (krizių valdymas, sąmoningumo ugdymas, rizikų mažinimas, bendra nauda ir pan.). Taip pat CSP3 apimtyje svarbūs aspektai tampa pasitikėjimas, aiškus vaidmenų ir atsakomybių pasidalinimas bei komunikacijos kanalas.

Apjungus visus išanalizuotus galimus tokios partnerystės sudėtinius elementus CSP3 apibūdinama kaip ilgalaikis susitarimas/bendradarbiavimas/parama tarp dviejų ar daugiau viešojo ir privataus sektorių dalyvių paremtas pasitikėjimu, informacijos, resursų ir žinių dalybomis bei atsakomybių ir rizikų pasiskirstymu siekiant kibernetinio atsparumo, kaip bendros naudos. Ši samprata ir bus naudojama toliau šiame darbe.

[6] https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/UP%20KRITIS.pdf?__blob=publicationFile

2. VIEŠOJO IR PRIVATAUS SEKTORIŲ PARTNERYSTĖS KIBERNETINIO SAUGUMO SRITYJE PRAKTIKA

Įvairių informacinių sistemų atsiradimo poveikis visuose sektoriuose ir žmonių kasdieniniame gyvenime atveria kelią įvairiausių tipų kibernetinėms rizikos, kurių daroma įtaka jau seniai peržengė skaitmeninio pasaulio ribas.

Kibernetinis saugumas jau seniai tapo fundamentalus ir esminis pasitikėjimo kūrimo elementas, kuris yra būtinas skaitmeninės ekonomikos pranašumui išnaudoti. „Išorinio ir vidinio bendradarbiavimo kontekste visos bendradarbiaujančios grandys yra tarpusavyje priklausomos, todėl privalo derinti savo interesus“ (Štitilis, Pakutinskas, Laurinaitis ir Malinauskaitė-van de Castel, 2017, p. 35).

Europos Sąjungos komisija (2015) savo iniciatyva priimtoje rezoliucijoje paragino plėtoti pramoninius ir technologinius išteklius, būtinus siekiant pagerinti kibernetinį saugumą, o jau 2016 m. sausio 19 d. Europos parlamento (2016) rezoliucijoje nurodytas poreikis didinti išteklius būtinus bendradarbiauti tarp kibernetinio saugumo pramonės, viešojo ir privataus sektoriaus, ypač vykdant bendradarbiavimą mokslinių tyrimų srityje, ir plėsti viešojo ir privataus sektorių partnerystę.

Bendradarbiavimas tarp skirtingų sektorių kibernetinio saugumo srityje daugeliu atveju remiasi tomis pačiomis prielaidomis: rizikų pasiskirstymas, sutartimis paremtais santykiais, instituciniu pagrindu.

2.1. Užsienio šalių praktikos apžvalga

Grėsmių modeliavimas leidžia taikyti struktūrizuotą požiūrį į kibernetinį saugumą vertinant didžiausias grėsmes galinčias turėti įtakos veiklos procesams. Teisingas didžiausią riziką keliančių grėsmių nustatymas ir įvertinimas gali tapti tvirtu įrankiu taikant tinkamas atsakomąsias priemones.

Viešojo ir privataus sektorių partnerystė, daugelyje šalių turėdama ilgą istoriją, tik paskutiniais dešimtmečiais tapo svarbesne dalimi viešosios naudos gavyboje. Kibernetinio saugumo aspektu ši nauda apima kibernetinį tautos atsparumą. Pačios CSP3 įgyvendinimas ir jos aspektai dažniausiai „gula“ į įvairias šalių kibernetinio saugumo strategijas.

2011 m. Europos tinklų ir informacijos apsaugos agentūra paskelbė Bendradarbiavimo modelių įgyvendinant CSP3 gerųjų praktikų gaires ir tyrimo rezultatus. Dokumentas pateikia 36-ias rekomendacijas kaip sėkmingai įgyvendinti CSP3 siekiant įgyti atsparumą kibernetinėms atakoms ir pagelbėti identifikuoti reikalingą pagalbą ES narėms, kurios šią kibernetinio saugumo užtikrinimo dalį bando įdiegti pirmą kartą.

Atsižvelgiant į tai, kad daugeliu atveju pačios PPP įgyvendinimas kibernetinio saugumo srityje remiasi strateginio lygmens įgyvendinimu, todėl šioje palyginamoje analizėje lyginant skirtumus ir panašumus remiamasi šiais pagrindiniais aspektais:

- CSP3 reikšmė šalims ar jų atstovaujamoms organizacijoms
- CSP3 įgyvendinimo spektras
- Ryšys tarp CSP3 dalyvių
- CSP3 tikslai ir numatomi rezultatai

Bet kokia nacionalinio lygmens strategija skirta suderinti valdymo visumą, koordinuoti viešojo ir privataus sektorių veiklas per atsakomybes santykiuose tarp suinteresuotų šalių, bei perteikti nacionalinius ketinimus kitų šalių atžvilgiu (Luiijf, Besseling ir de Graaf, 2013).

Šioje dalyje koncentruojamasi į Europos žemyno šalis siekiant įvertinti to paties požiūrio ar kultūrinio suvokimo ryšiais susaistytų senojo žemyno tautas, eliminuojant pastebimus skirtumus, tarkime, tarp Europos valstybių, Azijos šalių ar Amerikos pasaulėžiūros, kai radikalūs neatitikimai labai tikėtini. Svarbus aspektas – strategijos „šviežumas“, kai atsiranda galimybė nekartoti anksčiau priimtų strategijų klaidų ar sekti geriausio pavyzdžio pėdomis. Strategijų analizės imtis – strategijos patvirtintos ar atnaujintos laikotarpyje tarp 2016 ir 2018 m.

3 lentelė. Partnerystės šalių strategijose palyginimas

ES valstybė ir strategijos priėmimo/atnaujinimo data	**Vokietija (2016)**	**Jungtinė Karalystė (2016)**	**Graikija (2017)**	**Lenkija (2017)**	**Švedija (2017)**	**Nyderlandų Karalystė (2018)**
CSP3 forma	Viešas-viešas, viešas-privatus, viešas-akademinis	Viešas-privatus	Viešas-privatus, viešas-akademinis	Viešas-privatus	Privatus-viešas, privatus-akademinis, viešas-akademinis	Viešas-privatus, Viešas-akademinis, viešas-viešas
Pagrindiniai įgyvendinimo aspektai	Informacijos dalybos (programinės įrangos pažeidžiamumai ir silpnosios vietos, atakos profiliai), krizių valdymas ir bendradarbia		Informacijos keitimasis, krizių valdymas,	Krizių valdymas, kibernetinio saugumo specialistų ruošimas, mokslinė tiriamoji veikla, informacijos dalybos	Bendradarbiavimas ir informacijos dalinimasis, krizių valdymas, parama mokslinei tiriamajai veiklai ir švietimui	Reagavimas į incidentus, išankstinio perspėjimo kanalai, praktiniai seminarai, viešieji ryšiai (sąmoningumo ugdymas).

3 lentelės tęsinys kitame puslapyje

3 lentelės tęsinys

ES valstybė ir strategijos priėmimo/atnaujinimo data	Vokietija (2016)	Jungtinė Karalystė (2016)	Graikija (2017)	Lenkija (2017)	Švedija (2017)	Nyderlandų Karalystė (2018)
	vimas jų metu.					
CSP3 tikslai	Atskirai CSP3 strategijoje nėra apibrėžiama	CSP3 kaip sudėtinė dalis visų strategijoje numatytų tikslų	Atskirai CSP3 strategijoje nėra apibrėžiama	Efektyvi CSP3 pagrįsta pasitikėjimu ir pasidalinta atsakomybe už saugumą kibernetinėje erdvėje plėtojant viešojo sektoriaus gebėjimus bei įsitraukiant į bendrą ES CSP3. Remti mokslinę tiriamąją veiklas kibernetinio saugumo srityje tarp akademinio ir privačių sektorių.	Atskirai CSP3 strategijoje nėra apibrėžiama	CSP3 kaip strategijos pagrindas užtikrinantis vaidmenis ir atsakomybes, tiekimo grandinės patikimumą ir rinkos organizavimą.
CSP3 viešojo sektoriaus dalyviai ir vaidmuo	Federalinės vyriausybės informacinių technologijų komisaras, Nacionalinė kibernetinio saugumo tarnyba	Nacionalinis kibernetinio saugumo centras			Vyriausybė – kontroliuojanti įgyvendinimą institucija.	Vyriausybės paskirtas CSP3 įgyvendintojas – Nacionalinis saugumo ir kovos su terorizmu koordinatorius.

Šaltinis: parengta autoriaus

Europos sąjungos mastu stiprius žingsnius PPP plėtojime kibernetinio saugumo srityje paskutiniu metu žengia **Jungtinė Karalystė** kaip vieną iš tokios partnerystės valdymo įrankių pasitelkdama Nacionalinį kibernetinio saugumo centrą. Daugeliu atveju Jungtinė Karalystė CSP3 patirtį perėmė iš glaudaus bendradarbiavimo su JAV, kai du vienodi požiūriai, kibernetinio saugumo kultūros ir analogiškos

žvalgybinės patirties bendruomenės, komerciniai sektoriai bei gynybiniai ryšiai išlaiko tik subtilius skirtumus (Carr, 2016).

Nyderlandų karalystė. Lyderio pozicijos įgyvendinant PPP (valdžios institucijomis, verslo bendruomene, mokslu, pilietine visuomene) kibernetinio saugumo apimtyje Nyderlanduose paskirtos Nacionaliniam saugumo ir kovos su terorizmu koordinatoriui (NCTV). Šios institucijos dalimi yra Nacionalinis kibernetinio saugumo centras (NCSC) esantis Kibernetinio saugumo departamente (DCS), kurio apimtyje užtikrinti kibernetinio saugumo stiprinimas ir rūpinimasis PPP koordinavimu tiek strateginiu, tiek operatyviniu lygiu. Išskiriamos 3 esminės CSP3 įgyvendinimo sritys NCSC[7] apimtyje (žr. 5 pav.):

1. Bendradarbiavimo tarp viešojo ir privataus sektorių kibernetinio saugumo apimtyje organizavimas per informacijos dalinimosi ir analizės centrus ir ryšių palaikymo įgaliotinius (viešojo ir privataus sektorių deleguotus atstovus);
2. Pasitikėjimo kūrimas su visais suinteresuotaisiais subjektais įtraukiant ryšių palaikymą strateginiame, taktiniame ir operatyviniame lygiuose identifikuojant tendencijas, pokyčius ir naujus dalyvius kibernetinio saugumo srityje;
3. Pasiruošimas ir krizių valdymo koordinavimas apimant visą kibernetinio saugumo grandinę užtikrinant viešojo ir privataus sektorių vaidmenis, galimybes ir atsakomybes.

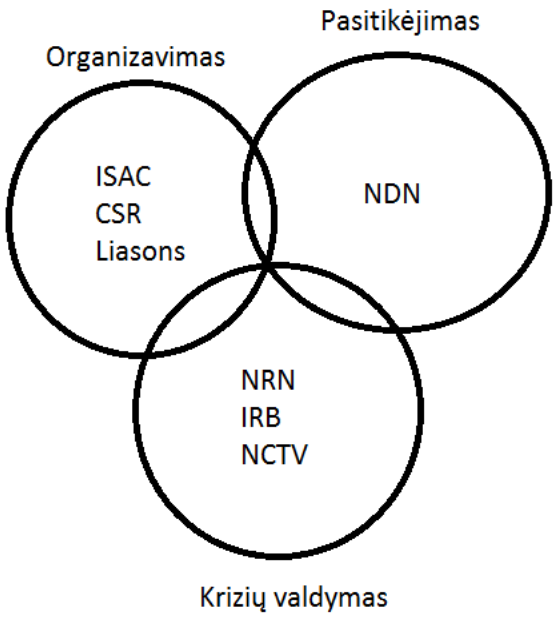
Papildomai bendradarbiavimo tikslui pasiekti 2014 m. įkurtas Nacionalinis atsako tinklas (angl. *National Response Network (NRN)*). Jo pagalba viešas ir privatus sektoriai gali dalintis žiniomis ir patirtimi bei teikti pagalbą kibernetinio atsako metu[8].

Nacionalinis aptikimo tinklas (angl. *National Detection Network (NDN)*) skirtas informacijos dalinimuisi apie grėsmes ir rizikas siekiant užkardyti arba apriboti tikėtiną žalą[9]. Tinklo tikslas – su dalyvaujančiais projekte dalintis esminiais atakos indikatoriais (angl. *Indicators of Compromise*), kurių dėka galima identifikuoti kenkėjišką veiklą informacinėse sistemose ar duomenų perdavimo tinkluose. 2018 m. Nyderlandų kibernetinio saugumo ataskaitoje (NCSC, 2018) teigiama, kad per nurodytus metus Nacionaliniu aptikimo tinklu buvo pasidalinta 25049 esminiais atakos indikatoriais, kas įrodo šio CSP3 efektyvumą ir naudą.

Pasinaudojant ryšių palaikymo „įgaliotiniais“[10] (angl. *Liaison officers*) Nyderlanduose siekiama sukurti stiprų tarpusavio komunikacijos kanalą, kurio vystymas taikos metu užtikrina reikiamą greitą

[7] https://www.ncsc.nl/english/Cooperation/public-private-partnership.html
[8] https://www.ncsc.nl/english/Cooperation/national-response-network.html Žiūrėta: 2018 m. rugpjūčio 18 d.
[9] https://www.ncsc.nl/english/Cooperation/national-detection-network.html Žiūrėta: 2018 m. rugpjūčio 18 d.
[10] https://www.ncsc.nl/english/Cooperation/liaisons.html Žiūrėta: 2018 m. rugpjūčio 18 d.

palaikymą (ekspertinį bendradarbiavimą) krizės akivaizdoje. Didelio masto kibernetinio incidento atveju CSP3 apimtyje situaciją analizuoja ir informacijos dalinimąsi koordinuoja IT atsako taryba[11] (angl. *ICT Response Board* (IRB)), kurią sudaro IT ekspertai iš svarbių sektorių (telekomunikacijos, energetika, finansai ir t.t.) bei vyriausybinių organizacijų.



Šaltinis: sudaryta autoriaus

5 pav. Bendradarbiavimas kibernetinio saugumo srityje Nyderlanduose

Pasinaudojant ryšių palaikymo „įgaliotiniais“[12] (angl. *Liaison officers*) Nyderlanduose siekiama sukurti stiprų tarpusavio komunikacijos kanalą, kurio vystymas taikos metu užtikrina reikiamą greitą palaikymą (ekspertinį bendradarbiavimą) krizės akivaizdoje. Didelio masto kibernetinio incidento atveju CSP3 apimtyje situaciją analizuoja ir informacijos dalinimąsi koordinuoja IT atsako taryba[13] (angl. *ICT Response Board* (IRB)), kurią sudaro IT ekspertai iš svarbių sektorių (telekomunikacijos, energetika, finansai ir t.t.) bei vyriausybinių organizacijų.

Siekiant palaikyti kibernetinį atsparumą NCSC taip pat atlieka ekspertinių žinių konsultanto vaidmenį tiek viešam, tiek privačiam sektoriams. Esminiai tokio patarėjo vaidmens pavyzdžiai yra[14]:

[11] https://www.ncsc.nl/english/Cooperation/ict-response-board.html Žiūrėta: 2018 m. rugpjūčio 18 d.
[12] https://www.ncsc.nl/english/Cooperation/liaisons.html Žiūrėta: 2018 m. rugpjūčio 18 d.
[13] https://www.ncsc.nl/english/Cooperation/ict-response-board.html Žiūrėta: 2018 m. rugpjūčio 18 d.
[14] https://www.ncsc.nl/english/expertise—advice Žiūrėta: 2018 m. rugpjūčio 18 d.

- patarimai dėl saugios tiekimo grandinės procesų užtikrinimo;
- informacijos saugos politikos peržvalga;
- patarimai dėl duomenų tinklo stebėjimo ir žurnalinių įrašų sistemų projektavimo;
- ekspertinių žinių indėlis įvairiose informacijos ir kibernetinio saugumo platformose valstybės mastu;
- patarimai dėl saugumo skenavimų ir pažeidžiamumų vertinimo esminiuose sektoriuose organizavimo;
- CERT veiklos ir incidentų valdymo plano peržiūra.

Pagal ENISA (2017), Nyderlanduose veikianti nepriklausoma Nacionalinė kibernetinio saugumo taryba yra puikus į tikslą orientuoto bendradarbiavimo formos pavyzdys. Tarybai keliami sekantys uždaviniai siekiant pasiekti patariamosios ir tiriamosios veiklos tikslus:

- Pagal užsakymus ir savarankiškai vyriausybei bei verslui teikti konsultacijas strateginiais kibernetinio saugumo klausimais;
- Stebėti naujas kibernetinio saugumo tendencijas ir technologinius pokyčius bei inovacijas transformuojant jas į galimas kibernetinio saugumo rizikų mažinimo priemones bei ekonominio potencialo didinimo galimybes;
- Inicijuoti iniciatyvas šalyje ir už jos ribų, kurios akivaizdžiai padeda kelti kibernetinio saugumo lygį Nyderlanduose.

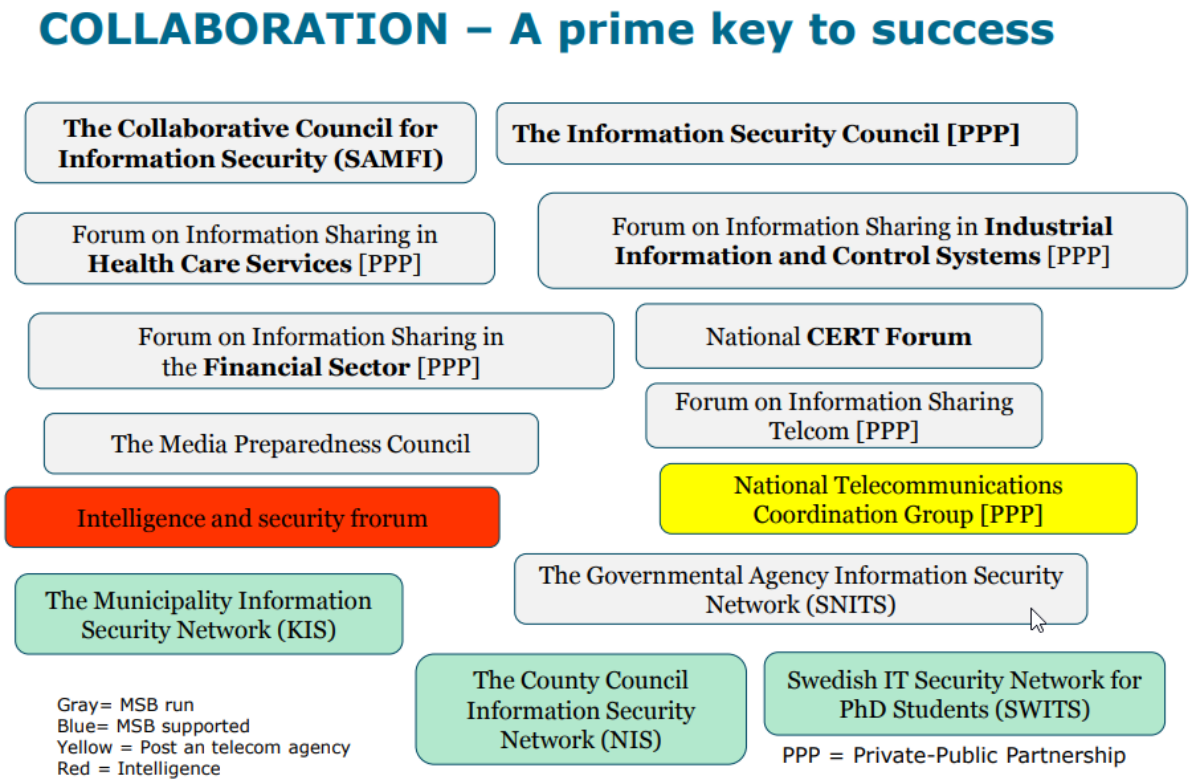
Apžvelgus galime teigti, kad esminiai PPP įgyvendinimo užtikrinant kibernetinį saugumą Nyderlanduose indikatoriai remiasi ekspertinių žinių, esminių kenkėjiškos veiklos indikatorių dalybomis, tarpsektorinio komunikacijos kanalo palaikymu ar viešojo sektoriaus pagalba kibernetinio incidento metu.

Švedija. Siekdama užtikrinti nacionalinėje saugumo ir skaitmeninės transformacijos strategijose įtvirtintas nuostatas Švedija kibernetinio saugumo strategijoje kaip vieną iš tikslų nurodo aukštojo mokslo ir tyrimų plėtojimą. CSP3 užuomazgomis galime laikyti partnerystės stiprinimą tarp aukštojo mokslo institucijų, pramoninių tyrimų institutų bei privataus ir viešojo sektorių siekiant pilnai išnaudoti turimą potencialą ir inovacijas kibernetinio saugumo srityje. Taip pat tikslo įgyvendinimui keliamas ir kibernetinio saugumo integravimo į visas strateginių inovacijų bendradarbiavimo programas, kurių penkias, skirtas socialiniams iššūkiams įveikti, vyriausybė pristatė 2016 m. Inovacijos programų tikslas, tuo pačiu ir jas palaikančios CSP3, užtikrinti Švedijos konkurencingumą stimuliuojant skaitmeninę transformaciją ir mobilizaciją jai tarp suinteresuotųjų viešojo ir privataus sektorių šalių.

CSP3 Švedijoje remiasi informacijos dalybomis įvairiose partnerystės rūšyse, tame tarpe viešųjų sektorių partnerystė: Informacijos saugos bendradarbiavimo grupė (angl. *The Cooperation Group for*

Information Security (SAMFI)), kuri apjungia viešojo sektoriaus dalyvius (Švedijos ginkluotosios pajėgos, Policija ir pan.); Bendradarbiavimo forumas (angl. *National Cooperative Council against Seriuos IT Threats* (NSIT) analizuojantis grėsmes ir pažeidžiamumus galinčius turėti įtakos nacionaliniams interesams. Forumas apjungia valstybinės žvalgybines organizacijas.

Švedijos kibernetinio saugumo strategijoje CSP3 nustatoma kaip savanoriškas, susitarimais pagrįstas bendradarbiavimas[15]. Šios rūšies partnerystei sukurtos kelios bendradarbiavimo platformos, tokios kaip Švedijos krizių valdymo agentūra (angl. *Swedish Civil Contingencies Agency* (MSB)), Nacionalinė telekomunikacijų koordinavimo grupė (angl. *National Telecommunications Coordination Group* (NTSG)) – savanoriškas forumas skirtas bendradarbiauti nacionalinės infrastruktūros atkūrimo kritinėse situacijose metu. MSB apimtyje sukurti keli informacijos dalinimosi forumai įvairiuose sektoriuose: telekomunikacija, CERT, finansai, sveikatos ir socialinė apsauga, SCADA (angl. *Supervisory control and data acquisition*).



Šaltinis: R. Oehme, 2007, p. 12

6 pav. Partnerystės schema Švedijoje

[15] https://www.government.se/information-material/2017/07/a-national-cyber-security-strategy/ Žiūrėta: 2018 m. rugsėjo 12 d.

Bendradarbiavimo užtikrinimo atsakomybė paskirta vyriausybei, kuri turi skatinti kolaboravimą tarp skirtingų institucijų, turinčių atskiras užduotis kibernetinio saugumo užtikrinime, taip pat užtikrinti tinkamą informacijos ir ekspertinės patirties dalinimosi tarp CSP3 dalyvių.

Šalies strategijoje apibrėžtas unikalus reikalavimas (susijęs su viešųjų sektorių partneryste) užtikrinti viešųjų pirkimų efektyvumą siekiant pagerinti veiklos pasiekiamumą pašto ir telekomunikacijų infrastruktūros palaikymo srityje per ekspertines konsultacijas, kurios pavestos Švedijos pašto ir telekomunikacijų priežiūros tarnybai pasinaudojant aukščiau minėtais bendradarbiavimo per forumus būdais. Sukuriamas savotiškas tarpininkavimo tarp infrastruktūros savininkų ir Nacionalinės viešųjų pirkimų agentūros metodas užtikrinantis ir tiekimo grandinės saugumą.

PPP kibernetinio saugumo srityje Švedijoje, analogiškai kaip ir Nyderlanduose, remiasi informacijos ir ekspertinės patirties dalinimosi projektais, kuriuos koordinuoja Informacijos saugumo taryba (angl. *The Information Security Council*). Detali partnerystės, remiantis R. Oehme (2015), schema pateikta 5 paveiksle.

Lenkija. Strategijoje keliamas tikslas ir atsakomybė vyriausybei sukurti viešojo ir privataus sektorių kooperavimo mechanizmus paremtus pasitikėjimu ir pasidalinta atsakomybe. Tuo pat metu viešasis sektorius turėtų didinti patariamojo balso pajėgumus visiems ekonominiams sektoriams. Bendradarbiavimo formose išskiriami piliečiai kaip atskiras vienetas. Svarbus strateginis aspektas liečia ir kibernetinio saugumo projektų plėtojimą viešajam sektoriui kooperuojantis su akademiniu ir privačiu sektoriais. Šio uždavinio įgyvendinimui sukurtas Nacionalinis tyrimų ir plėtros centras prie Švietimo ir aukštojo mokslo ministerijos. Bendradarbiavimas kibernetinio saugumo tyrimų srityje pasiekiamas per unikalius įgūdžius turinčių specialistų įtraukimą įvairiuose tyrimuose ir analizės centruose sprendžiant kompleksines kibernetinio saugumo problemas.

Siekiant viešojo ir akademinių sektorių partnerystės aukštojo mokslo institucijos įpareigojamos vystyti tarpdisciplinines specializacijas, tokias kaip informacijos saugos valdymas, asmens duomenų apsauga, intelektinės nuosavybės apsauga internete ir kt. naujų technologijų inovacijos. Tame tarpe didelis dėmesys skiriamas kibernetinių nusikaltimų tyrimų ekspertų ugdymui taip stiprinant teisėsaugos pajėgumus.

Nors kibernetinio saugumo strategijoje nėra konkrečių nuorodų į viešojo ir privataus sektorių partnerystę, Lenkija turi Nacionalinį kibernetinio saugumo centrą, kuriam pavesta atsakomybė už tarpusavio bendradarbiavimą tarp sektorių, tačiau koordinuojanti institucija yra valstybinis tyrimų institutas – NASK[16], kurio viena iš veiklos krypčių – „sukurti bendradarbiavimo ir keitimosi informacija tarp privataus ir viešojo sektorių platformą“.

[16] http://eng.nask.pl/en/activities/cyber-security/283,Cyber-security.html Žiūrėta: 2018 m. rugsėjo mėn. 12 d.

ENISA (2017) tyrimas nurodo, kad institucinio bendradarbiavimo forma Lenkijoje įgyvendinama Vyriausybinio saugumo centro (lenk. *Rządowe Centrum Bezpieczeństwa*) apimtyje užtikrinant krizių valdymą. Kaip ir teigiama tyrime, šios formos partnerystės apimtyje centro veikla nukreipta į kritinę infrastruktūrą.

Graikija. Kibernetinio saugumo strategijos viena iš krypčių – paskirti atsakingą kibernetinio saugumo instituciją už tarpusavio santykių tarp viešojo ir privataus sektorių vystymą. Esminė viešojo sektoriaus siekiamybė, kaip viešoji nauda – skaitmeninių technologijų panaudojimas įvairių paslaugų gerinimui ir kibernetinio saugumo kultūros stiprinimas išnaudojant akademinę bendruomenę bei viešą ir privatų sektorius.

The Software Alliance[17] paruoštame 2015 m. ES kibernetinio saugumo brandos žemėlapyje nurodoma, kad Graikija neturi ir artimiausiu metu neplanuoja reglamentuoti PPP kibernetinio saugumo srityje, tame tarpe organizuoti įvairias sektorių bendradarbiavimo tarybas.

Vokietija. Prioretizuojant kritinę infrastruktūrą Vokietijos kibernetinio saugumo strategijoje UP KRITIS yra viešojo ir privačiojo sektorių bendradarbiavimo iniciatyva tarp ypatingos svarbos infrastruktūros objektų operatorių, jų profesinių asociacijų ir atitinkamų vyriausybinių agentūrų. Šio bendradarbiavimo tikslas yra palaikyti ypatingos svarbos infrastruktūros paslaugų teikimą šalyje. Plačiau bendradarbiavimas apibrėžiamas 2011 m. patvirtintoje Nacionalinėje kritinės infrastruktūros saugumo strategijoje kai tikslams pasiekti reikia „gerai veikiančios bendradarbiavimo schemos ir partnerystės tarp įvairių lygių valdžios institucijų, priklausančių skirtingiems departamentams, infrastruktūros operatorių, daugeliu atvejų priklausančių privačiam sektoriui, bei įvairių asociacijų, kaip tarpininkų“ (Federal Ministry of the Interior, 2009).

Šiuo atveju vėl pastebime CSP3 įgyvendinimo tendenciją apsiribojančia keitimąsi informacija ir įvairių krizės valdymo planų kūrimu (Federal Ministry of the Interior, 2009). Vokietija, kaip pasiekimus CSP3 kritinės infrastruktūros kibernetinio saugumo rėmuose įvardina:

- ekspertinių žinių dalybas tarp įvairių sektorių,
- pasitikėjimo tinklo sukūrimą tarp UP KRITIS narių,
- bendrai sutartų rekomendacijų įgyvendinimą (reguliarių bendrų kibernetinio saugumo pratybų organizavimas, kritinių procesų identifikavimas ir tarpusavio ryšių nustatymas).

Esminė UP KRITIS įgyvendinamos CSP3 kryptis iki 2013 m. buvo užtikrinti kritinės infrastruktūros savininkų atsakomybę ir savarankiškumą siekiant vyriausybės nustatytų kibernetinio saugumo reikalavimų šiai infrastruktūrai, tuo pačiu bendradarbiaujant analizuoti, kurti gerąsias praktikas ir specifikacijas, bendrai

[17] http://cybersecurity.bsa.org/index.html Žiūrėta: 2018 m. rugsėjo mėn. 18 d.

vertinti situaciją ir koordinuotai valdyti krizes nuolatos tobulinantis pratybose ugdant tarpusavio pasitikėjimą. Vėliau bendradarbiavimui įgijus naują prasmę veiklos diapazonas perlipo kritinės infrastruktūros dalyvius ir buvo išplėstas iki 500 privataus ir viešojo sektoriaus organizacijų visoje Vokietijoje.

Pagal ENISA (2017) įvardintas PPP formas kibernetinio saugumo srityje Vokietijos UP KRITIS partnerystė vyksta kibernetinio saugumo užsakomųjų paslaugų teikimo būdu, kai iniciatyva finansuojama iš valstybės biudžeto ir dalinai pasitelkiant privatų sektorių naudos gavimui visiems projekto dalyviams – ilgalaikės bendruomenės dirbančios su specifinėmis grėsmėmis ir kitais kibernetinio saugumo iššūkiais.

Jungtinė Karalystė. 2016-2021 m. strategija numato paskatas ir svertus privačiam sektoriui pagrįstus šalies vyriausybės investicijomis, kuriomis siekiama didinti novatoriškos valstybės kibernetinės erdvės potencialą. Taip pat skiriama daug dėmesio vyriausybės vaidmeniui konsultuojant ir užmezgant partnerystės ryšius su privataus kapitalo įmonėmis siekiant nustatytų kibernetinio saugumo tikslų (HM Government, 2016):

- užtikrinti, kad privatus sektorius imsis neatidėliotinų veiksmų siekiant apsaugoti save ir savo klientus nuo kibernetinių atakų pasinaudojant patarimais ir lengvai įdiegiamais įrankiais;
- dirbti su rinkos dalyviais (draudikais, reguliuotojais ir investuotojais) siekiant pabrėžti aiškias naudas verslui įvertinant rizikų kaštus efektyviam rizikų valdymui,
- kurti partnerystę paremtą profesiniais standartais pereinant prie sąmoningumo didinimo, siekiant įtikinti verslą imtis veiksmų,
- nustatyti tinkamą kibernetinių rizikų, kurių sektoriai nesugeba spręsti, valdymo reguliavimo sistemą.

Analizuojamu metu veikiančios CSP3 įgyvendinimo kampanijos ir schemos:

- Kibernetinio sąmoningumo kampanija (angl. Cyber Aware campaign (žinoma kaip Cyber Streetwise[18])) – skatina privataus ir viešo sektorių elgsenos kibernetinėje erdvėje pokyčius. Kompanijoje dalyvauja 128 tarpsektoriniai partneriai.
- „Cyber Essentials“ schema skatina 5 pagrindinių techninių kontrolių diegimą siekiant saugotis nuo dažniausiai pasitaikančių internetinių grėsmių.
- „Cyber-Security Information Sharing Partnership (CiSP) yra pramonės ir vyriausybės bendradarbiavimo iniciatyva skirta informacijos apie kibernetines grėsmes dalinimosi, užtikrinant jos saugumą ir konfidencialumą, realiu laiku.

[18] https://www.cyberaware.gov.uk/

Analogiškai, kaip ir Vokietijos atveju, įgyvendinant CSP3 skiriamas dėmesys kritinei infrastruktūrai, ypač telekomunikacijų sektoriui, kur vienas iš esminių strateginių tikslų yra saugios tiekimo grandinės užtikrinimas. Siekiant apsaugoti gyventojus vyriausybė rūpinasi prieigos prie kenkėjiškų interneto resursų per DNS blokavimą pasitelkiant interneto tiekėjus.

Beveik visos ES valstybės (ne tik analizuotos šio darbo imtyje) narės užtikrindamos partnerystę remiasi ir dirba visiems priimtinais metodais orientuojantis į partnerystės formą, įgyvendinimo aspektus, keliamus tikslus ir dalyvių vaidmenis bei atsakomybes. Analizuotoje imtyje galime išskirti kelis unikalius partnerystės įgyvendinimo bruožus:

- Nyderlandų karalystė: bendradarbiavimas organizuojamas per informacijos dalinimosi platformas ir analizės centrus; už ryšių tarp partnerystės dalyvių atsakingas koordinuojantis įgaliotinis; pasitikėjimui kurti partneriai įtraukiami į visus bendradarbiavimo organizavimo lygmenis – strateginį, taktinį ir operatyvinį; partnerystės pasitelkimas krizių valdymui paremtas nustatant dalyvių vaidmenis, galimybes ir atsakomybes.
- Švedija: informacijos dalinimasis tarp įvairių partnerystės rūšių vyksta įtraukiant ir žvalgybos institucijas; bendradarbiavimas grindžiamas savanoriškais susitarimais per įvairias platformas siekiant tai išnaudoti krizių valdymo efektyvumui didinti. Unikalus Švedijos atvejis – strateginiame lygyje įtraukiamas ir viešųjų pirkimų efektyvumo užtikrinimas siekiant gerinti partnerystės veiklos pasiekiamumą.
- Lenkija: didelis dėmesys partnerystės veikloje skiriamas tarpdisciplininių specializacijų palaikymui (kartu su akademiniu sektoriumi) ir įvairioms ekspertinėms kompetencijoms ugdyti.
- Vokietija: istoriškai išliekantis kritinės infrastruktūros prioritetas organizuojant partnerystę, tačiau orientuojantis į šiandienos poreikius vyksta ir užsakomųjų paslaugų finansuojamų iš valstybės biudžeto ir dalinai verslo su „nauda visiems“ principu įgyvendinimas.
- Jungtinė Karalystė: vyriausybei skiriamas esminis vaidmuo konsultuojant partnerystės įgyvendinimo klausimais bei užmezgant bendradarbiavimo ryšius su privačiu sektoriumi; partnerystės apimtyje viena iš siekiamybių yra ir saugios tiekimo grandinės užtikrinimas.

Kadangi daugeliu atveju partnerystės įgyvendinimas kibernetinio saugumo srityje remiasi strateginio lygmens įgyvendinimu, todėl tarp analizuotų per 2016-2018 metus pasitvirtinusių ar atsinaujinusių kibernetinio saugumo strategiją valstybių aiškias lyderio pozicijas viešojo ir privataus sektorių partnerystės užtikrinant kibernetinį saugumą apimtyje užima Jungtinė Karalystė, Nyderlandų karalystė ir Vokietija. Nuo jų neatsilieka Švedija bei Lenkija. Daug labiau pasistengti reikia Graikijai.

2.2.Lietuvos atvejo apžvalga

Atkūrus Lietuvos nepriklausomybę planinę ekonomiką pakeitus rinkos ekonomikai vyko pirmosios privatizavimo reformos. Kaip teigia D. Gudelis ir V. Rozenbergaitė (2004) „viešojo ir privataus sektorių partnerystės plėtros Lietuvoje galimybes lemia teisinės sąlygos.“ (p. 68). Iki šiol nėra vieno bendro tokią partnerystę reglamentuojančio įstatymo Lietuvoje, tačiau šios srities kai kuriomis formomis naudotis leidžia kiti Lietuvos Respublikos įstatymai: koncesijų įstatymas, investicijų įstatymas, viešųjų pirkimų įstatymas, taip pat 2009 m. priimtas Viešojo ir privataus sektorių partnerystės projektų rengimo ir įgyvendinimo taisyklės, kurios nustato reikalavimus partnerystės projektų rengimui, vertinimui, įgyvendinimui ir dalyvaujančių partnerystėje šalių teises, pareigas ir atsakomybes su rizikos paskirstymu. Koordinuojanti PPP veiklą institucija – Lietuvos finansų ministerija: rengia teisinę bazę, dalyvauja kuriant administracinę sistemą ir koordinuoja šios sistemos veiklą, taip pat kaupia proceso praktiką ir ją analizuoja bei skleidžia patirtį. Iki 2009 m. dauguma PPP apraiškos buvo forminamos viešojo ir privataus sektorių sutartimis remiantis Lietuvos įstatyme nustatytu koncesijų būdu. Vėliau išpopuliarėjo ir kitos formos: nuoma, privati finansinė iniciatyva, jungtinė veikla ir t.t.

2010 m. Lietuvos Respublikos Ūkio ministro įsakyme dėl PPP tikslingumo kriterijų nustatymo ir metodinių rekomendacijų dėl PPP taikymo tikslingumo kriterijų nurodoma, kad „viešųjų paslaugų tekimas privačiam sektoriui perduodamas ilgesniam nei 10 metų laikotarpiui“ (Lietuvos Respublikos Ūkio ministerija, 2010), taip pagrindžiant ilgalaikės partnerystės reikalavimą PPP sampratoje.

Per paskutinius kelerius metus Lietuva padarė didelį proveržį kibernetinio saugumo srityje: nuo visiško neapibrėžtumo iki patvirtintos kibernetinio saugumo strategijos ir praktinių įgyvendinimo pavyzdžių. 2018 m. rugpjūčio 13 d. Vyriausybės patvirtinta Nacionalinė kibernetinio saugumo strategija penkerių metų laikotarpiui nustatė svarbiausias nacionalinės kibernetinio saugumo politikos viešajame ir privačiame sektoriuose kryptis perkeliant Europos Sąjungos Tinklų ir informacinių sistemų saugumo (TIS) direktyvos nuostatas.

Strategija parengta įvertinus pastaraisiais metais Lietuvoje didėjanti kibernetinių incidentų kiekį.

Dokumente išskiriamos penkios svarbiausios sritys:

1. valstybės kibernetinio saugumo ir gynybos pajėgumų stiprinimas,
2. nusikalstamų veikų kibernetinėje erdvėje prevencijos, užkardymo ir tyrimų užtikrinimas,
3. kibernetinio saugumo kultūros ir inovacijų plėtros skatinimas,
4. glaudaus viešojo ir privataus sektorių bei mokslo institucijų bendradarbiavimo stiprinimas,
5. tarptautinio bendradarbiavimo kibernetinio saugumo srityje stiprinimas.

Viešojo ir privataus sektorių bei mokslo institucijų bendradarbiavimo stiprinimui strategijoje keliami bendradarbiavimo koordinavimo, technologinių priemonių diegimo bendradarbiavimui stiprinti ir atsakingo informacinių sistemų saugumo spragų atskleidimo uždaviniai. Šiuos uždavinius apibendrina keliamas tikslas – lygiaverčių partnerių abipusis pasitikėjimas ir nauda.

Pirmam tikslo uždaviniui įgyvendinti vyriausybė planuoja kurti naujus arba tobulinti esamus komunikacijos metodus, procesus ir kitas priemones. Šiuo metu, remiantis Lietuvos Respublikos Vyriausybės 2015 m. balandžio 23 d. nutarimu Nr. 422 „Dėl Kibernetinio saugumo tarybos sudarymo ir jos reglamento patvirtinimo“ yra sudaryta Kibernetinio saugumo taryba, kurios nariais pakviesti ir privataus sektoriaus atstovai – įvairių kompanijų vadovai, rizikų valdymo profesionalai ar informacijos saugos specialistai. Tarybos mandatus gavo ir du mokslo srities atstovai. Tokiu būdu taryba tapo viešojo ir privataus, bei viešojo ir akademijos sektorių bendradarbiavimo formos pavyzdys. Pati taryba yra nuolatinė patariamoji institucija, teikianti pasiūlymus dėl kibernetinio saugumo gerinimo valstybės institucijoms, viešojo administravimo subjektams, tvarkantiems valstybės informacinius išteklius, viešųjų ryšių tinklų, elektroninių paslaugų teikėjams, šios srities įmonėms, mokslo ir studijų institucijoms.

Antruoju tikslo uždaviniu siekiama ugdyti kūrybiškumą, pažangius gebėjimus ir rinkos poreikius atitinkančius kibernetinio saugumo įgūdžius bei kvalifikaciją. Viešasis sektorius aktyviai pritraukdamas privatų ir akademinį sektorius sieks užpildyti kibernetinio saugumo specialistų trūkumą plėtojant mokymų, akreditavimo ir sertifikavimo sistemas, orientuotas į darbo rinkos poreikius. Tame tarpe mokant naujokus ar suteikiant persikvalifikavimo galimybes informacinių technologijų srityje dirbantiems asmenims.

Trečiasis tikslo uždavinys savotiškai papildo antrą uždavinį skatinant įvairių sektorių ir mokslo bendradarbiavimą panaudojant išugdytus specialistus kuriant kibernetinio saugumo srities inovacijas.

Patvirtinta strategija koncentruojasi į tris pagrindines sritis viešojo ir privataus sektorių partnerystės įgyvendinime:

1. viešojo sektoriaus, kaip koordinatoriaus ir konsultanto vaidmuo įtraukiant privatų sektorių į teisėkūrą,
2. pasinaudojant privataus sektoriaus resursais ir akademinio sektoriaus žiniomis specialistų poreikio patenkinimas,
3. kibernetinio saugumo technologijų inovacijų kūrimas pritraukiant akademinį sektorių ir privataus sektoriaus kapitalą.

Visas šias sritis viena ar kita forma galime pastebėti aukščiau išvardintuose strategijos uždaviniuose.

Remdamiesi A. Dūdos iškeltais PPP inicijavimo pagrindimo klausimais 4 lentelėje įvertinkime strategijos uždavinius.

4 lentelė. Partnerystės inicijavimo galimas pagrindimas

	1 uždavinys	**2 uždavinys**	**3 uždavinys**
Ar partnerystė leis viešajam sektoriui pasiekti užsibrėžtus tikslus?	Taip – Tarybos sudėties didžiąją dalį (iš 24) narių sudaro viešojo sektoriaus atstovai – 14, taip pat tik 2 akademinės bendruomenės atstovai ir 8 privataus sektoriaus dalyviai (Lietuvos Respublikos krašto apsaugos ministras, 2018).	Taip – 2018 m. vykdomos 2 antrosios pakopos ir 2 pirmosios pakopos studijų programos susijusios su informacijos ir kibernetiniu saugumu[19].	Ne – papildomai reikalinga inovacijų strategija tiriamosios veiklos plėtrai ir integracijai į partnerystę.
Ar partnerystė yra finansiškai pigesnė alternatyva, nei tradicinis viešųjų paslaugų teikimo būdas?	Panaikinamas poreikis samdyti brangiai apmokamus konsultantus pasinaudojant privataus sektoriaus žiniomis ir kompetencijomis.	Specialistų poreikio mažinimui pasitelkiamos privataus sektoriaus lėšos ir akademinės bendruomenės kompetencija.	Inovacijas finansuoja privatus sektorius, o įgyvendina akademinis sektorius. Viešasis sektorius lieka koordinatoriaus pozicijoje.
Kokia papildoma ekonominė ir (ar) socialinė vertė bus sukurta?	Privataus sektoriaus įtraukimas į reguliacinio proceso kūrimą galimai mažina nepamatuotų kaštų atsiradimą.	Sukuriamos modernios studijų programos kibernetinio saugumo specialistams ruošti. Daugeliu atveju mokslą gali finansuoti privatus sektorius siekdamas kelti savo darbuotojų kvalifikaciją.	Stabdomas „protų nutekėjimas“, užtikrinama technologijų rinkos kaina atsižvelgiant į regioną, apsaugoma vietinė rinka.

Šaltinis: sudaryta autoriaus pagal A. Dūdos iškeltus partnerystės inicijavimo pagrindimo klausimus

Lietuvos Respublikos Vyriausybė 2015 m. balandžio mėn. 23 d. nutarimu Nr. 422 įkuria Kibernetinio saugumo tarybą apibrėždama jos sudėtį – 24 nariai – ir įtraukdama privatų bei akademinį sektorius. Tai galima laikyti viena pirmųjų įteisintų CSP3 apraiškų Lietuvoje: „taryba yra nuolatinė kolegiali institucija, analizuojanti kibernetinio saugumo užtikrinimo būklę Lietuvos Respublikoje ir teikianti [...] pasiūlymus dėl šios būklės gerinimo“ (Lietuvos Respublikos Vyriausybė, 2015).

Remiantis analizuotų užsienio valstybių patirtimi vienas iš esminių partnerystės elementų yra koordinuojančio asmens ar institucijos nuo viešojo sektoriaus paskyrimas. Darbo atlikimo metu Lietuvos kibernetinio saugumo įstatymo pagrindu kibernetinio saugumo politiką formuojančia, įgyvendinimą organizuojančia, kontroliuojančia ir koordinuojančia institucija paskirta Lietuvos Respublikos krašto

[19] lamabpo.lt Žiūrėta: 2018 m. rugsėjo mėn. 29 d.

apsaugos ministerija., tuo tarpu viena iš politiką įgyvendinančių institucijų paskirtas Nacionalinio kibernetinio saugumo centras, kuris vykdo ir kibernetinio saugumo krizių valdymo funkciją.

Kibernetinio saugumo strategija neapibrėžia konkrečių CSP3 įgyvendinimo žingsnių (analizuojamu metu papildomų dokumentų nurodančių partnerystės įgyvendinimo gairių irgi nėra priimta), tačiau kiekvienoje strategijos nubrėžtoje kryptyje galime identifikuoti esminius bendradarbiavimo bruožus: konsultacijos, pasiūlymai, kvalifikacijos kėlimas, inovacijos, žinių dalybos, abipusis pasitikėjimas ir nauda.

3. VIEŠOJO IR PRIVATAUS SEKTORIŲ PARTNERYSTĖS UŽTIKRINANT KIBERNTINĮ SAUGUMĄ LIETUVOJE TYRIMAS

3.1. Tyrimų metodologija

Tyrimo problema. Nepakankamas viešojo ir privataus sektorių bendradarbiavimas didina neracionalių kibernetinį saugumą reglamentuojančių teisės aktų ir reikalavimų atsiradimą, neišnaudojamas kibernetinio saugumo specialistų rengimo potencialas, neatsiranda tarpusavio pasitikėjimo stiprinimo prielaidos ir rizikų pasidalinimas, o tai įtakoja investuojamų kaštų į kibernetinio saugumo užtikrinimą privačioje infrastruktūroje didėjimą ir neišnaudojamos visos įmanomos kibernetinio atsparumo priemonės valstybės mastu siekiant viešojo sektoriaus keliamų tikslų ir pageidaujamų naudų.

Tyrimo objektas. Viešojo ir privataus sektorių partnerystė užtikrinant kibernetinį saugumą Lietuvoje.

Tyrimo tikslas. Nustatyti, kaip informacijos ir kibernetinio saugumo ekspertai iš skirtingų sektorių vertina viešojo ir privataus sektorių partnerystės situacija ir perspektyvą Lietuvoje.

Tyrimo uždaviniai. Empiriniu tyrimo metodu atlikti:

- ekspertų nuomonės tyrimą, kuris padėtų išsiaiškinti požiūrį į viešojo ir privataus sektorių partnerystę užtikrinant kibernetinį saugumą Lietuvoje,
- remiantis ekspertine nuomone, pasiūlyti galimus tokios partnerystės įgyvendinimo būdus ir formas, kurie sustiprintu Lietuvos kibernetinį atsparumą.

Tiriant CSP3 įgyvendinimą užtikrinant kibernetinį saugumą Lietuvoje svarbu tiksliai atlikti ekspertų žinių ir vertinimų tyrimą, nes gilesnei analizei reikalingos respondentų specifinės žinios ir patirtis. Ekspertų apklausos tikslas – patvirtinti arba paneigti darbe formuluojamus ginamuosius teiginius, taip pat iškelti kitus papildomus klausimus, atskleidžiančius naudingas įžvalgas išvadų ir rekomendacijų formulavimui.

Pasak R. Tidikio (2003) „ekspertas – asmuo, kuris dėl savo profesinės arba gyvenimo patirties turi didžiausią kompetenciją ir patikimiausią bei pakankamai išsamią informaciją apie tiriamą problemą“ (p. 467). Tokia tyrėjo orientacija į respondento profesinę, socialinę ir pan. patirtį ir jos raiška pasisakymuose remiasi kokybinio tyrimo fenomenologine strategija.

Kokybinis tyrimas pasirinktas dėl jo interpretacinio požiūrio, kuris pabrėžia tyrėjo siekį interpretuoti reiškinius tomis prasmėmis, kurias jiems suteikia tiriami žmonės (Gall, Gall ir Borg, 2007). Toks atvirumo principas suteikia galimybę į tyrimo objektą žiūrėti visapusiškai ir teoriškai minimaliai. Kokybinis tyrimas atveria galimybę ištraukti autentišką informaciją ir interpretacijos dėka teoriją konstruoti tiesiog iš pačios

realybės. Atsižvelgiant į darbe numatytą tikslą atliktas privačiame ir viešajame sektoriuose dirbančių informacijos ir kibernetinio saugumo srities ekspertų struktūruotas interviu raštu.

Darbo tyrimo objektas apima ne tik socialinio mokslo sritį, tačiau ir techninius aspektus, todėl formuluojant išvadas bei rekomendacijas ekspertų žinių panaudojimas yra būtinas siekiant suprasti tiriamąjį reiškinį sistemingai vertinant situacija natūralioje aplinkoje ir pateikiant interpretacinį bei holistinį, kaip „išgyventą patirtį“, iš situacijos analizės kylantį paaiškinimą. Kadangi tiriamasis reiškinys, kibernetinio saugumo srityje, Lietuvoje dar nėra plačiai paplitęs ir populiarus, todėl interpretuojamos hipotetinių teiginių išvadas bus galima toliau tikrinti kai atsiras poreikis darbo tęstinumui.

Kokybinio tyrimo instrumentu parinktas pusiau struktūruotas interviu, kuriame vyrauja atviri klausimai. Jis buvo išsiųstas pasirinktiems ekspertams elektroninių paštu arba per profesinį socialinį tinklą Linkedin, taip pat kai kurie ekspertai pageidavo bendrauti telefonu. Ekspertai atsakinėjo į paruoštus klausimus neribojant laiko, pertraukų darymo ar pildymo vietos, todėl galėjo geriau apgalvoti atsakymus, juos išreikšti išsamiau, neribojant jų laisvo vertinimo pasitelkiant sukauptas žinias ir intuiciją.

Struktūruotą interviu dalį sudaro 7 viešojo ir privataus sektorių partnerystės klausimai ir 7 bendrojo pobūdžio klausimai, kurie sudaryti remiantis magistrinio darbo teorine dalimi (5 lentelė). Apklausiant ekspertus buvo užduodami papildomi nenumatyti tyrimo plane klausimai siekiant išsiaiškinti gilesnę ekspertinę nuomonę ar gauti atsakymų patikslinimą.

5 lentelė. Struktūruoto interviu klausimai

Nr.	**Klausimas**
Viešojo ir privataus sektorių partnerystė	
1.	Kokias viešojo ir privataus sektorių partnerystės apraiškas užtikrinant kibernetinį saugumą Lietuvoje šiuo metu pastebite?
2.	Ar šiuo metu įgyvendinami viešojo ir privataus sektorių partnerystės kibernetinio saugumo srityje projektai yra efektyvūs?
3.	Kokia ekonominė ir socialinė viešojo ir privataus sektorių partnerystės įgyvendinimo Lietuvoje užtikrinant kibernetinį saugumą vertė?
4.	Kokie būtų pasiūlymai dėl viešojo ir privataus sektorių partnerystės plėtros ar papildomų įgyvendinimo formų siekiant kibernetinio Lietuvos atsparumo?
5.	Ar atskirų sektorių (viešojo ir privataus) įsitraukimas į viešojo ir privataus sektorių partnerystę yra pakankamas su aiškiai apibrėžtomis atsakomybėmis ir rizikomis? Jei nepakankamas, tada ko trūksta ir ką reikėtų tobulinti?
6.	Kokios viešojo ir privataus sektorių partnerystės iniciatyvos nėra įgyvendintos Lietuvoje, nors buvo apie tai galvota, jos buvo inicijuotos arba jau pradėtos? Kokias nešgyvendinimo priežastis galite įvardinti?

5 lentelės tęsinys kitame puslapyje

5 lentelės tęsinys

7.	Kokią gerąją viešojo ir privataus sektorių partnerystės įgyvendinimo praktiką galima panaudoti žvelgiant į užsienio šalis? Kokie tokios gerosios praktikos įgyvendinimo pavyzdžiai ir kodėl jie pasiteisino (priežastys)?
Bendrojo pobūdžio klausimai	
8.	Koks organizacijos, kurioje dirbate, tipas (tarptautinė organizacija, vietinis verslas, valstybinė įstaiga (įmonė ir pan.)?
9.	Koks organizacijos, kurioje dirbate, dydis (0-50, 51-100, 101-400, 401-1000 darbuotojų)?
10.	Kokias atsakomybes ir pareigas (vaidmenis) užimate įvardintoje organizacijoje?
11.	Kiek ilgai jau dirbate šioje organizacijos pozicijoje?
12.	Kokia Jūsų patirtis informacijos ir kibernetinio saugumo srityje?
13.	Ar Jūsų organizacija dalyvauja kokiuose nors kibernetinio saugumo viešojo ir privataus sektorių partnerystės projektuose?
14.	Jei atsakėte teigiama į aukščiau esantį klausimą, prašome įvardinkite kokią Jūsų darbo laiko dalį užima darbas pagal įvairius kibernetinio saugumo viešojo ir privataus sektorių partnerystės projektus?

Šaltinis: parengta autoriaus

Klausimų validavimas buvo atliekamas nusiunčiant suformuluotus klausimus baigiamojo darbo vadovui išmanančiam kibernetinio saugumo situaciją Lietuvoje.

Tyrimas buvo atliekamas pagal žemiau lentelėje pateiktą struktūrą (6 lentelė).

6 lentelė. Kokybinio tyrimo eiga.

Etapas	Etapo veiklos	Etapo tikslas
Parengiamieji darbai 2 savaitės	Sudaromas tyrimo planas ir parenkamas apklausos metodas bei būtini dokumentai. Identifikuojami galimi tyrimo dalyviai remiantis asmenine tyrėjo patirtimi, viešąja nuomone ir kibernetinio saugumo srities specialistų patarimais	Parengti tyrimo planą. Parengti esminius interviu klausimus. Identifikuoti ekspertus struktūruotam interviu.
Įvadas ir prisistatymas 1 savaitė	Atrinktiems dalyviams el. būdu (per profesinį socialinį tinklą Linkedin ir el. paštu) pristatomas tyrimo tikslas, tyrimą atliekantis asmuo, tiriamoji problema bei duomenų rinkimo konfidencialumo aspektai. Nurodoma, kad tyrimo metu surinkti duomenys bus	Sukuriamos aplinkybės, kad tyrimo dalyviai galėtų apmąstyti savo atsakymus, laisvai reikšti įžvalgas, suprastų tyrimo tikslą.

6 lentelės tęsinys kitame puslapyje

6 lentelės tęsinys

Etapas	Etapo veiklos	Etapo tikslas
	pateikiami apibendrintai neįvardinant konkrečių dalyvių. Gaunamas sutikimas dalyvauti interviu.	
Ekspertų pasirinkimo pagrindimo vertinimas	Dalyvių įvedimas į temą užduodant bendrinius klausimus siekiant gauti patvirtinimą dėl ekspertinės patirties pagrindimo, viešojo ar privataus sektorių priskyrimo. Atsakomi patikslinantys klausimai iš tyrimo dalyvių dėl temos suvokimo ir interpretacijų.	Bendrinės informacijos apie tyrimo dalyvius rinkimas.
Ekspertinis vertinimas 2 savaitės	Užduodami tyrimo klausimai nurodyti 5 lentelėje.	Šalinamos galimos klaidos ir prieštaravimai.
Ekspertinio vertinimo duomenų analizė 1 diena	Tyrėjas, gavęs tyrimo dalyvių atsakymus el. paštu, padėkoja už dalyvavimą ir naudingas mintis, kilus neaiškumams, pasiteirauja dėl išsakytų minčių patikslinimo. Pagal situaciją užduoda papildomus tyrimo klausimus neįtrauktus į struktūruotą interviu.	Išlaikomas teigiamas emocinis kontaktas ir profesinis ryšys.
Ataskaitos rengimas	Ataskaitoje aprašomi atsakymai į klausimus, apibendrinamos skirtingos nuomonės ar spontaniškai kilę atsakymai į papildomus klausimus.	Parengti medžiagą kokybinei duomenų analizei. Rezultatų interpretacija, vertinimo rezultatai ir išvados.

Šaltinis: parengta autoriaus

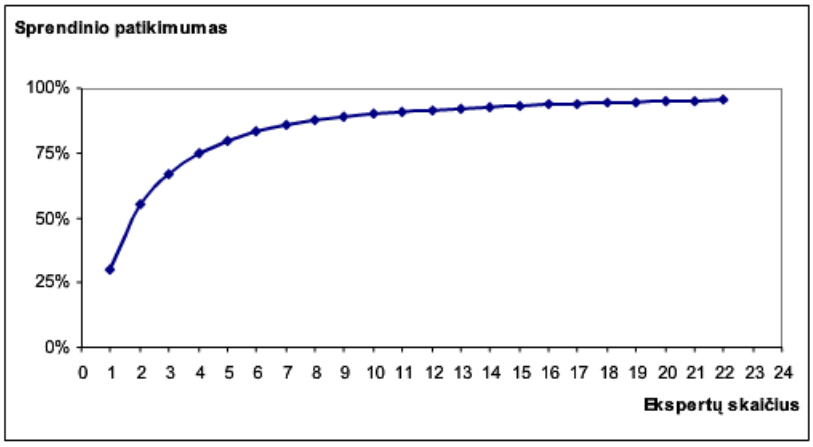
3.2.Ekspertų apklausos analizė

3.2.1. Tyrimo ekspertų charakteristika

Sudarant tyrime dalyvaujančių ekspertų grupės dydį buvo remiamasi dalyvių kvalifikacija ir patirtimi profesinėje srityje (siekiant sumažinti vienodą patirtį turinčių ekspertų kiekį), taip pat subjektyvia tyrimo autoriaus nuomone apie dalyvius ir jų turimas savybes (kūrybiškumą, požiūris į tiriamąją sritį, mąstymo lankstumą, savikritiškumą ir mokėjimą bendradarbiauti).

Pasak A. Augustinaičio ir kt. (2009) „sunku (ir nebūtina) surinkti didesnę grupę aukščiausios kvalifikacijos ekspertų, nes specialistų, galinčių užginčyti ar paneigti jų nuomonę, negali būti daug“ (p. 201). Autorius taip pat teigia, kad „daugelio mokslininkų nuomone, optimalus grupės dydis – nuo 8 iki 10 ekspertų“ (2009, p. 201).

Prielaidos dėl priimtino ekspertų kiekio, kurias suformavo klasikinė testų teorija (Brock ir Hommes, 1997), teigia, „kad agreguotų sprendimų patikimumą ir priimančiųjų (aut. past. ekspertų) sprendimą skaičių sieja greitai slopstantis netiesioginis ryšys“ (Augustinaitis, et al., 2009, p. 202), t.y. didelis ekspertų skaičius – trukdo formuoti bendrą nuomonę, o mažas dalyvių grupės dydis – lemia nepatikimus rezultatus. Galime teigti, kad didesnė nei 10 ekspertų imtis jau nekonstruoja radikalių tyrimo rezultatų pokyčių, tuo tarpu dalyvių skaičius nuo 1 iki 8 gali būti formuojantis nepatikimus rezultatus (žr. 7 pav.).



Šaltinis: Augustinaitis et al., 2009, p. 202

7 pav. Ekspertų skaičiaus įtaka vertinimo patikimumui

Buvo pasirinkta ekspertinė grupės imtis iš aštuonių ekspertų turinčių žinių ir patirties informacijos ir kibernetinio saugumo srityje.

Formuluojant struktūruoto interviu klausimus buvo siekiama išsiaiškinti tiek viešojo, tiek privataus sektorius atstovaujančių ekspertų nuomonę partnerystės įgyvendinimu kibernetinio saugumo srityje Lietuvoje, todėl tyrime pakviesti dalyvauti abiejų sektorių atstovai. Labai svarbus aspektas atrenkant respondentus buvo informacijos ir kibernetinio saugumo srities išmanymas bei dalyvavimas įvairiose valstybės koordinuojamose, valdomose ar kontroliuojamose kibernetinio saugumo srityse: teisinio reglamentavimo atitikties siekimas, svarbių ūkio sektorių veikla, kibernetinio saugumo užtikrinimo priemonių tiekimas, diegimas ar priežiūra ir pan. Renkant ekspertus buvo siekiama surasti vienodai aukštą kompetenciją turinčius asmenis, tačiau atranka atlikta pagal tyrėjo tiriamosios srities išmanymą.

Tyrimo dalyvių asmens duomenys nuasmeninti ir garantuotas konfidencialumas siekiant apsaugoti galinčia išryškėti organizacijų, kurioms respondentai atstovauja, neviešinamą informaciją, suteikiant respondentams kodus (arabiškais skaitmenimis nuo 1 iki x).

3.2.1. Tyrimo organizavimas

Prieš pateikiant klausimus raštu ar vykdant pokalbį telefonu su tyrimo dalyviais buvo bendraujama el. paštu supažindinant su keliamos problemos aktualumu, tyrimo tikslais, asmens duomenų naudojimu (žr. 1 priedą). Dėl dalyvių įtemptų darbotvarkių ir darbo vietos atstumo ekspertams klausimai buvo išsiųsti el. paštu (žr. 2, 3 ir 4 priedus). Kai kurie dalyviai pageidavo į klausimus atsakyti telefonu (žr. 5 priedą) . Interviu atlikti 2018 m. spalio mėnesį.

3.2.2. Tyrimo apribojimai

Rengiant darbą buvo tirtos viešojo ir privataus sektorių partnerystės apraiškos Lietuvoje remiantis CSP3 apibrėžimais nurodytais ENISA (2017), M. Carr (2016) ir K. Bechkoum ir kt. (2017) darbuose. Kadangi CSP3 nėra teisiškai reglamentuotas Lietuvoje ir analizuojamos apraiškos, daugeliu atveju, gali remtis sutartiniais, kaip partnerystės, ryšiais, kai vyksta komerciniai santykiai tarp viešojo ir privataus sektorių, labai tikėtina, jog ekspertų patirtis šioje srityje yra tyrimo apribojimas, kai pati partnerystė kibernetinio saugumo srityje gali būti traktuojama ir kaip informacijos dalybos per įvairias platformas arba savanoriškai tarp pačių partnerių ir t.t. Daugelis užsienio dokumentų ir pavyzdžių buvo analizuojami anglų kalba, todėl baigiamasis darbas yra apribojamas autoriaus anglų kalbos žinių lygiu arba atliktais vertinimais.

Aukščiau išvardinti tyrimo apribojimai negalėjo kardinaliai įtakoti atlikto tyrimo ar turėti esminės reikšmės magistro baigiamojo darbo rezultatams. Šie apribojimai atskleidė būtinus analizuoti tolimesnius aspektus: partnerystės metodiką ir formas tinkančias Lietuvai, įgyvendinimo gairių reglamentavimas ir kt. būtini atlikti pokyčiai (atsakingo informacijos dalinimosi teisinis reglamentavimas ir pan.) siekiant partnerystės įgyvendinimo užtikrinimo.

3.2.1. Tyrimo duomenų analizė

Tyrime sutiko dalyvauti 8 dalyviai. 5 dalyviai dirba privačiame sektoriuje, 2 dalyviai – viešajame sektoriuje arba turi patirties darbo šiame sektoriuje, taip pat dirba(o) dalinai valstybės valdomose įmonėse, 1 dalyvis tyrimo metu buvo laisvai samdomas, tačiau su ilgamete patirtimi viešajame sektoriuje.

Pirmas klausimas: Kokias viešojo ir privataus sektorių partnerystės apraiškas užtikrinant kibernetinį saugumą Lietuvoje šiuo metu pastebite?

Dauguma respondentų įvardino asociacijos „Infobalt“ ir KAM bendradarbiavimą, kuris, pasak dalyvio Nr. 1, vyksta „aptariant, planuojant kibernetinio saugumo valdymą“. Dalyvis Nr. 3 antrindamas mato tokį bendradarbiavimą „kuriant įstatyminę bazę“, nors tuo pačiu įvardina, kad viskas grindžiama „labiau asmeninių santykių lygyje“. Beveik visi dalyviai kaip CSP3 apraišką įvardina ir kibernetinio saugumo tarybą, tačiau daugeliu atveju visi sutinka, kad „jos įgaliojimai yra labai riboti“ ir „nėra sistemos pagal kurią vyktų bendradarbiavimas“ (Dalyvis Nr. 3). Dalyviai Nr. 3 ir Nr. 6 pamini ir nuolatinio struktūrizuoto bendradarbiavimo (PESCO) gynybos srityje Europos Sąjungoje projektą, kurio dalimi yra ir Lietuva su jai tenkančia atsakomybe plėtoti bendrų kibernetinio saugumo įrankių ir technologijų parinkimą Kibernetinėms greito reagavimo komandoms (angl. *Cyber Rapid Responce Teams*). Tai, kad ši apraiška priskiriama prie CSP3 pagrindžia Dalyvis Nr. 5 nurodydamas, kad „verslas realiai dalyvauja, jis kuria tuos produktus ir valstybė jų kažkiek nupirks“, tačiau pilnavertiškam CSP3, kai sakome, kad šie santykiai turėtų būti ilgalaikiai, kalbama ne apie pirkimą „nuo lentynos“, tačiau verslo dalyvavimą kaip individualių poreikių realizuotoją – „valstybė negali to pati pasidaryti ir sako: man reikia verslo“ ir „PPP yra apie tai, kad yra ilgalaikis santykis ir jis būtinai turi R&D dalį“ (Dalyvis Nr. 5). Dalyvis Nr. 7 kalbėdamas apie KAM bendradarbiavimą išreiškia abejones, kai viešasis sektorius įvardina „įrankius ir temas kuriomis remiantis turi būti plėtojama“ partnerystė, „tačiau niekas nepaklausė verslo ko jiems reikėtų jei būtų sukurta tam, kad pagerinti tą kibernetinį saugumą“.

Atsižvelgiant į surinktą ekspertinę nuomonę galime išskirti šias pagrindines CSP3 apraiškas Lietuvoje:

- Asociacijos „Infobalt“ ir KAM bendradarbiavimas,
- Žiniasklaidos ir KAM bendradarbiavimas,
- Kibernetinio saugumo taryba,
- Dalyvavimas nacionalinėse ir tarptautinėse kibernetinio saugumo pratybose (viešas, privatus ir akademinis sektoriai),
- PESCO projektas ir Lietuvos indėlis jame,

- Verslo kompetencijų perteikimas (mokymų, diskusijų pavidalu) viešajam sektoriui (pavieniai atvejai ne ilgalaikėje perspektyvoje).
- Lietuvos kariuomenės aktyvaus rezervo kariai savanoriai.

Antras klausimas: Ar šiuo metu įgyvendinami viešojo ir privataus sektorių partnerystės kibernetini saugumo srityje projektai yra efektyvūs?

Dalyviai Nr. 3 ir Nr. 8 neigiamai atsako į klausimą ir nurodo, kad pagrindinė neefektyvumo priežastis: „nes nėra sistemos“, bei „nelabai yra PPP“. Dalyvis Nr. 2 mato potencialą, „tačiau, mano nuomone, pakankamai nepasinaudota“. Dalyvis Nr. 5 taip pat abejoja efektyvumu grįsdamas abejones, kad „sunku kalbėti ar tai yra, kai nežinome kas tai yra“. Dalyvis Nr. 6 taip pat pastebi, kad apčiuopiamo rezultato kol kas nėra matęs ir pabrėžia, kad „kol kas verslas nėra suinteresuotas sudalyvauti CSP3“. Jo nuomone efektyvi partnerystė turi būti suprantama „kai kalbama apie problemas, pagalbą, kitus dalykus, o ne tik apie pinigus“.

Atsižvelgiant į ekspertų prieštaravimus apie CSP3 apraiškų efektyvumą galime daryti išvadą, kad be tinkamo apibrėžimo, t.y. sužinojimo apie ką kalbėti, bei metrikų įdiegimo, labai sunku atlikti matavimus.

Trečias klausimas: Kokia ekonominė ir socialinė viešojo ir privataus sektorių partnerystės įgyvendinimo Lietuvoje užtikrinant kibernetinį saugumą vertė?

Dalyvis Nr. 1 skeptiškai vertina dabartinę naudą kai „niekas ir nekelia aukštų tikslų“. Kiti tyrimo dalyviai įžvelgia didesnį potencialą įvardindami bendro kibernetinio saugumo žinių lygio didėjimą (Dalyvis Nr. 3), bei resursų sutelkimą ir veikimą iš vien (Dalyvis Nr. 8). Dalyvis Nr. 5 kalbėdamas apie partnerystę įžvelgia abipusę naudą „jei yra sukuriamas produktas iš verslo, tai jis bus nupirktas, t.y. verslas gaus pinigus, o valstybė efektyviau suvaldys grėsmę ir pasieks savo tikslų“, todėl šiai bendrai vertei sukurti „vienas iš nurodytų (Kibernetinio saugumo strategijos, aut. past.) uždavinių ir yra sukurti bendradarbiavimo modelį“. Dalyvis Nr. 6 įžvelgia, kad pati partnerystė kaip tokia verslui nėra reikalinga ir čia lieka tik viešojo sektoriaus interesas, kai „kalbame apie konsultacijas kibernetinio saugumo srityje viešajam sektoriui, tai visos konsultacijos yra iki tokio lygio, kad būtų parduotas produktas ir viskas“. Respondentas taip pat pabrėžia, kad socialinė vertė, kai bendradarbiaujant verslui ir akademijai ruošiami profesionalai, kibernetinio saugumo specialistų rengime vyrauja „dvi kompetencijos – vadybininkai ir CIRT (angl. *Computer Incident Response Team*, aut. past.) specialistai“ ir „dažniausiai tos kompetencijos ugdomos organizacijos viduje“. Šiuo atveju bendradarbiavimas padidintų kibernetinio saugumo kompetencijų lygį ir užpildytų rengimo spragas. Su šia mintimi netiesiogiai sutinka ir Dalyvis Nr. 3 teigdamas, kad „šiuo metu privataus sektoriaus kibernetiniai gebėjimai ir sukauptos žinios yra geresni, todėl jų panaudojimas viešajame sektoriuje leistų greičiau ir efektyviau kelti kibernetinė saugą [...] tuo pačiu kurtų naujas darbo vietas privačiame sektoriuje, didintų Lietuvos specialistų kompetenciją ir Lietuvos įmonių konkurencingumą

užsienio rinkose.“ Dalyvis Nr. 7 akcentuoja, kad pridėtinė vertė privačiam sektoriui „atsiranda per žmones arba per tam tikrų produktų atsiradimą iš kurio jie gali vėliau pardavinėdami užsidirbti“. Kalbant apie nacionalinio saugumo interesus respondentas kalba apie tai, kad „valstybė, suprasdama tam tikro verslo ar tam tikros įmonės kritiškumą įsipareigoja ją šiek tiek saugoti arba prisidėti prie jos saugumo užtikrinimo“. Tai kuria papildomą vertę ne tik valstybės įvaizdžiui, tačiau ir verslui per kibernetinio saugumo kompetencijų spragų švelninimą ar finansinę prizmę nukreipiant tik dalį investicijų į kibernetinį atsparumą, t.y. rizikų pasidalinimas tarp sektorių.

Išanalizavus ekspertų atsakymus galime daryti išvadą, kad CSP3 galėtų būti kaip katalizatorius išjudinant ir auginant kibernetinio saugumo rinką Lietuvoje, ne tik pasąmoningai galvojant apie kibernetinio saugumo žinių ar technologijų eksportą tuo prisidedant prie socialinės, ekonominės gerovės ir vertės kūrimo.

Ketvirtas klausimas: Kokie būtų pasiūlymai dėl viešojo ir privataus sektorių partnerystės plėtros ar papildomų įgyvendinimo formų siekiant kibernetinio Lietuvos atsparumo?

Dalyvis Nr. 2 siūlo sekti Izraelio valstybės pavyzdžiu, kai „kibernetinis saugumas kaip sritis yra šalies ekonomikos dalis“. Dalyvis Nr. 8 rekomenduoja pasirinkus teisingą modelį atsižvelgiant į efektyvų informacijos keitimąsi ir aiškiai apibrėžtas atsakomybes. Dalyvis Nr. 3 į CSP3 plėtrą žvelgia kaip į tiriamosios veiklos plėtojimą: „galbūt turėtų būti duodama daugiau užsakymų tyrimams ir produktų sukūrimui universitetams ir privataus sektoriaus įmonėms“. Dalyvis Nr. 5 išreikšdamas nusivylimą privačiu sektoriumi, kai „verslas daugiau koncentruotas į pardavimus tiktai“, griežtai kalba apie tai, kad „PPP be R&D (ang. *Research and Development*,aut. past.) nebūna“. Respondentas kalbėdamas apie „valstybė sau, verslas sau“ konkretizuoja, kad „mes per maži, kad galėtume sau tai leisti“, todėl kaip CSP3 pavyzdį pateikia Bretanėje (Prancūzija) kuriamą kelių universitetų sąjungą (klasterį) su vienu iš tikslų ruošti kibernetinio saugumo specialistus ne tik viešajam sektoriui, bet ir verslui. Dalyvis Nr. 3 taip pat atkreipia dėmesį į tai, kad „dabartinė aplinka yra per daug dinamiška, kad galėtume susitvarkyti kiekvienas atskirai“, todėl kibernetinio atsparumo didinimas turi vykti „ne atsiribojant vieniems nuo kitų, o kaip tik kuo labiau keičiantis informacija, žiniomis“. Dalyvis Nr. 6 pamini R&D veiklos populiarinimą, kaip vieną iš partnerystės būdų, „per kažkokią reputacijos ar smagaus laiko prizmę, o ne per pinigus“ – kibernetinio saugumo hakatonus „kai dirbama ant to paties pagrindo ieškant ir analizuojant problemas [...] įdomu kaip atradot, ką pamatėt ir t.t.“

Išanalizavus ekspertinę nuomonę galime teigti, kad pagrindiniai pasiūlymai dėl CSP3 plėtros ar įgyvendinimo formų sudėtinių dalių yra:

- turi apimti mokslinę tiriamąją veiklą (angl. *R&D*),

- kibernetinio saugumo specialistų ruošimas pasitelkiant akademiją (programų ruošimas ir tyrimai) ir privatų sektorių (finansavimas ir žinios),
- informacijos keitimosi įgalinimas ir aiškios dalyvių atsakomybės,
- ilgalaikis proceso užtikrinimas,
- finansavimo modelis, kad privatus sektorius nedalyvautų vien tik visuomeniniais pagrindais.

Penktas klausimas: Ar atskirų sektorių (viešojo ir privataus) įsitraukimas į viešojo ir privataus sektorių partnerystę yra pakankamas su aiškiai apibrėžtomis atsakomybėmis ir rizikomis? Jei nepakankamas, tai ko trūksta ir ką reikėtų tobulinti?

Dalyviai Nr. 1 ir Nr. 2 teigia, kad „pagal tai, kas vyksta ar kokie tikslai – pakankamas“, tačiau „trūksta tiktai valios, lyderio bei bendro noro pasiekti užsibrėžto tikslo“. Dalyvis Nr. 3 nesutinka su tokia nuomone ir įvardindamas to priežastis teigia, kad „yra padrikos iniciatyvos, bet nėra sistemos [...] nėra apibrėžtos rolės, [...] nėra atsakomybių, [...] oficialių susitarimų, [...] finansavimo modelių.“ Analogiškai mąsto ir Dalyvis Nr. 7 pastebėdamas, „kad daugumoje atvejų viešasis sektorius laiko pakankamą atstumą nuo privataus sektoriaus bendradarbiavimo srityje“. Čia pat įvardina ir tobulintiną sritį – „nėra aišku ar bus koks grįžtamasis ryšys“, bei priežastis – „bet gal tas atstumo ribos nubrėžimas sąlygotas įvairių viešųjų ir privačių interesų baimės sukurto pasipriešinimo“.

Dalyvis Nr. 2 siūlo atsižvelgti į Izraelio valstybės PPP pavyzdį ir sukurti galimybę šalies kibernetinio saugumo pramonės plėtrai. Dalyvis Nr. 3 visų pirma rekomenduoja „išsigryninti koks PPP modelis Lietuvai būtų priimtinas, tada, greičiausiai, reikėtų atlikti įstatyminės bazės pakeitimus, turėtų atsirasti susitarimai su šalių rolėmis ir atsakomybėmis, bei finansavimo modeliais“.

Apibendrinant ekspertų išsakytas mintis galime teigti, kad:

- įgyvendinant PPP turi atsirasti kibernetinio saugumo pramonės plėtros galimybės,
- svarbu apsibrėžti CSP3 modelį ir atlikti su tuo susijusius įstatyminės bazės pakeitimus,
- nustatyti sektorių vaidmenis ir atsakomybes ir finansavimo modelius CSP3 apimtyje,
- nustatyti grįžtamojo ryšio ir komunikacijos kanalus tarp sektorių.

Šeštas klausimas: Kokios viešojo ir privataus sektorių partnerystės iniciatyvos nėra įgyvendintos Lietuvoje, nors buvo apie tai galvota, jos buvo inicijuotos arba jau pradėtos? Kokias neįgyvendinimo priežastis galite įvardinti?

Daugelio ekspertų nuomonė vienbalsiai – „neteko girdėti apie tokias“. Dalyvis Nr. 2 paminėjo „Saulėtekio slėnį“ ir projektą „Lietuva 2000“. Dalyvis Nr. 3 užsiminė apie tarpsektorinio informacijos su kibernetinio saugumo įvykiais dalinimosi platformą kitas mainų sistemos apraiškas.

Pagrindines tokių iniciatyvų įgyvendinimo nesėkmių priežastis ekspertai įvardina:

- PPP įgyvendinimo patirties nebuvimas,
- netinkamas kibernetinio saugumo koordinatoriaus parinkimas (Dalyvis Nr. 3 nesutinka tokios funkcijos pavedimui KAM dėl jos, kaip institucijos uždarumo ir „pakankamai sunkaus ėjimo į bendradarbiavimą“),
- bendros naudos, kaip tikslo, suvokimas,
- privataus sektoriaus suinteresuotumo dalyvauti CSP3 projektuose įgalinimas, „kad tai nebūtų laikoma kaip įtakojimas siekiant naudos sau (valstybei, aut. past.) (Dalyvis Nr. 3),
- Dalyvis Nr. 7 įvardina „kūrybiškumo ir iniciatyvos“ stoka bei tinkamai suformuotos idėjos (priemonių) su konkrečiais tikslais ir uždaviniais trūkumas,
- dėmesio veiklos tęstinumui trūkumas (Dalyvis Nr. 2).

Septintas klausimas: Kokią gerąją viešojo ir privataus sektorių partnerystės įgyvendinimo praktiką galima panaudoti žvelgiant į užsienio šalis? Kokie tokios gerosios praktikos įgyvendinimo pavyzdžiai ir kodėl jie pasiteisino (priežastys)?

Dalyvis Nr. 2 akcentuoja Izraelio patirtį nurodydamas, kad intelektinių resursų sutelkimas esant mažai valstybei didina kibernetinio atsparumo efektyvumą. Tačiau Lietuvos atveju, pasak eksperto, „trūksta lyderio, valios ir bendro noro pasiekti kilnių tikslų. Lietuva viską turi, bet – deja“. Be tikslaus pagrindimo Dalyvis Nr. 3 nurodo Olandijos ir D. Britanijos bendradarbiavimo modelius. „Pats privataus sektoriaus tikslas – pelno siekimas dažnai kertasi su saugumo tikslu“ teigia Dalyvis Nr. 4 nurodydamas būtinybę griežtesnio reglamentavimo/reguliavimo iš viešojo sektoriaus. Pasak eksperto „sritis reikalauja reguliatoriaus/reguliuojamojo santykio, o ne partnerystės“. Dalyvis Nr. 5 pateikia jau minėtą Bretanės kibernetinio saugumo slėnio pavyzdį, kur kelių universitetų sąjunga ruošdama kibernetinio saugumo specialistus bando eliminuoti šių profesionalų rinkos trūkumą. Dalyvis Nr. 7 kaip pavyzdį nurodo Estijos gynybos ministerijos iniciatyvą: savanoriškos veiklos valstybės labui kibernetines 300 „hakerių“ pajėgas.

Ekspertų nuomone sektini Lietuvai pavyzdžiai yra:

- Izraelio valstybė,
- Olandija,
- Didžioji Britanija,
- Estija,
- Jungtinės Amerikos Valstijos.

Izraelio valstybė galėtų būti pavyzdys kaip išnaudojant mokslo tiriamąją veiklą, kibernetinio saugumo priemonių kūrimo potencialą išlaikant vidinę rinką per partnerystę stiprinamas valstybės atsparumas ir užtikrinamas nacionalinis saugumas. JAV ir D. Britanijos patirtis puoselėjant ne tik kibernetinį atsparumą, tačiau ir visuomenės sąmoningumą per viešojo ir privataus sektorių bendradarbiavimą užtikrina kertinį kibernetinio saugumo, įtraukiant visus elementus (visuomenę, aut. past.) aspektą. Estijos partnerystės pavyzdžiai tarp viešojo, privataus, akademinio sektorių, taip pat dalyvaujant kariuomenei, įrodo tarpsektorinio bendradarbiavimo nacionalinio saugumo atžvilgiu potencialą. Olandijos atvejis grindžiamas partneryste organizuojamas informacijos dalinimosi platformas ir analizės centrus, paskiriant koordinuojančius įgaliotinius ir užtikrinant pasitikėjimo kūrimą visuose organizavimo lygmenyse.

Apibendrinant, viešojo ir privataus sektorių partnerystės plėtra Lietuvoje vyksta ir jos apraiškų vis daugėja, tačiau dar iki šiol susiduriama su tam tikrais iššūkiais, kurie, dažniausiai, kyla iš pačios partnerystės įgyvendinimo patirties stokos, teisinio reglamentavimo nubrėžiant aiškias atsakomybes trūkumo, bendro tikslo, kaip abipusės naudos, suvokimo nebuvimo ar grįžtamojo ryšio stokos.

Pasak tyrime dalyvavusių ekspertų, PPP plėtra reikalauja abipusio įsitraukimo su koordinacija iš viešojo sektoriaus ieškant priimtinų partnerystės būdų dalinantis rizikomis, nauda, įtraukiant tiriamąją veiklą ir sukuriant efektyvios komunikacijos kanalus (grįžtamojo ryšio nustatymą). Taip pat tarp svarbių trukdžių įvardinami viešųjų ir privačių interesų konfliktų atsiradimas, verslo suinteresuotumo stoka, viešojo sektoriaus atstumo nuo privataus sektoriaus laikymasis ar koordinuojančios institucijos uždarumas, bei pačio koordinatoriaus patirties CSP3 srityje spragos.

Įvertinus kokybinio tyrimo duomenis galima teigti, kad nepakankamas CSP3 prisideda prie neracionalių kibernetinį saugumą reglamentuojančių teisės aktų ir reikalavimų atsiradimo, kibernetinio saugumo specialistų rengimo potencialo neišnaudojimo, tarpusavio pasitikėjimo nebuvimo, o tai gali didinti kaštų, užtikrinant kibernetinį saugumą, privačiame sektoriuje didėjimą bei nepakankamą viešojo sektoriaus kibernetinio atsparumą.

IŠVADOS IR SIŪLYMAI

1. Viešojo ir privataus sektorių partnerystė, kaip bendrinis visų tokio reiškinio formų apibendrinančioji samprata gali būti apibūdinama kaip bendradarbiavimo instrumentų rinkinys (ekspertinės žinios, infrastruktūra, finansai ir pan.), kuris naudojamas viešojo intereso tikslams pasiekti, skirtas aktyviai į naudos viešajam sektoriui kūrimą įtraukti privataus sektoriaus dalyvius pasidalinant rizikomis ir gaunama nauda. Klasikinės partnerystės įgyvendinimo būdai remiasi viešojo, kaip vedančiojo, sektoriaus vaidmeniu bei poreikio pagrįstumu. Įgyvendinant partnerystę privatizacija ir elementarūs komerciniai santykiai (sukurti-įgyvendinti, perku-parduodu) gali būti laikomi už partnerystės sampratos ribų. Pagrindiniai įgyvendinimo būdai gali būti pasirenkami pagal rizikas ir atsakomybes (pvz. koncesija), turto ir nuosavybės valdymą (pvz. nuoma ir valdymas, privatizacija), finansinius susitarimus (pvz. finansuoja viešasis ar privatus sektorius) ar kompensavimo privačiam sektoriui pasirinkimą (pvz. privačioji finansinė iniciatyva). Išskiriamos šios partnerystės formos: sutartinė, institucinė ir strateginė.
2. Sėkmingas viešojo ir privataus sektorių partnerystės kibernetinio saugumo srityje vystymasis ir veikla priklauso nuo daugelio elementų: partnerystės formos, aplinkos (ekonominės, teisinės, politinės ir kultūrinės), interesų suderinamumo, rizikų pasidalijimo, kontraktų įgyvendinimo. Apibrėžiant aiškias CSP3 ribas būtina nurodyti informacijos, rizikų ir naudos pasidalinimo būtinumą, taip pat įtraukiant ilgalaikio bendradarbiavimo principą per pasitikėjimo sukūrimą, vaidmenų ir atsakomybių aiškumą bei komunikacijos kanalo sukūrimą. Taip pat svarbu į partnerystę įtraukti ir mokslinę tiriamąją veiklą. Tokios partnerystės sampratą galime apibrėžti kaip ilgalaikį susitarimą/bendradarbiavimą/paramą tarp dviejų ar daugiau viešojo ir privataus sektorių dalyvių paremta pasitikėjimu, informacijos, resursų ir žinių dalybomis bei atsakomybių ir rizikų pasiskirstymu siekiant kibernetinio atsparumo, kaip bendros naudos. Remiantis ENISA pateiktu pavyzdžiu CSP3 įgyvendinimo modelius galime suskirstyti į 4 pagrindines grupes: institucinis P3, į tikslą orientuotas P3, veiklos rangos P3 ir hibridinis P3.
3. Analizuotoje Europos Sąjungos narių valstybių imtyje (pasitvirtinusių ar atsinaujinusių kibernetinio saugumo strategiją laikotarpyje tarp 2016-2018 metų) galime įžvelgti unikalias gerąsias praktikas partnerystei organizuoti, stiprinti ar formuoti: partneriai įtraukiami į visus bendradarbiavimo lygmenis (strateginį, taktinį ir operacinį); į partnerystę, jei to reikalauja bendras tikslas, įtraukiamos ir žvalgybinės organizacijos; strateginiame lygmenyje, siekiant gerinti partnerystės veiklą, pasitelkiamas viešųjų pirkimų organizavimo efektyvinimas; kartu įtraukiant ir akademiją, kuri kuria ir įgyvendina tarpdisciplininės specialybes ugdant ekspertines kompetencijas; tinkamų finansavimo

modelių parinkimas bendrai naudai gauti; aiškaus koordinuojančio vaidmens su atsakomybėmis už ryšių palaikymą tarp partnerių nustatymas.

4. Didžioji dauguma apklausoje dalyvavusių ekspertų sutinka, kad šiuo metu Lietuvoje jau yra iniciatyvos galinčios patekti po viešojo ir privataus sektorių partnerystės užtikrinant kibernetinį saugumą apimtimi. Ekspertai sutaria, kad CSP3 įgyvendinimo vertė yra didelė: nuo eksportui paruoštų kibernetinio saugumo produktų, Lietuvos įmonių konkurencingumo užsienio rinkose didinimo, naujų darbo vietų atsiradimo privačiame sektoriuje, konkrečių uždavinių, kuriamų švietimo sektoriui, kėlimas didinant kompetencijų augimą ir specialistų poreikio patenkinimą iki kritinės infrastruktūros atsparumo užtikrinimo siekiant išlaikyti esmines paslaugas piliečiams. Tarp sektinų PPP įgyvendinimo pavyzdžių minima Izraelio valstybė, D. Britanija, JAV, Estija bei Olandija su Prancūzija: esminio vaidmens vyriausybei konsultuojant partnerystės įgyvendinimo klausimais priskyrimas, kibernetinio saugumo kritinių situacijų pajėgų privataus sektoriaus dalyvių pagrindu sukūrimas, informacijos dalinimosi platformų ir analizės centrų veikla per partnerystę ir ją koordinuojančio asmens iš viešojo sektoriaus paskyrimas, pasitikėjimo tarp partnerių kūrimas įtraukiant į visus bendradarbiavimo organizavimo lygmenis (strateginį, taktinį ir operatyvinį), partneryste paremto specialistų rengimo klasterio organizavimas. Tarp pirmų CSP3 oficialaus įgyvendinimo uždavinių ekspertai nurodo pačio CSP3 modelio sukūrimą, įstatyminės bazės pokyčius leisiančius plėtoti partnerystę, susitarimų dėl atsakomybių ir vaidmenų apibrėžimus, komunikacijos kanalų nustatymą (informacijos dalinimuisi bei grįžtamajam ryšiui užtikrinti) ir galimų finansavimo formų parinkimą.
5. Siekiant efektyvios ir abipusiai naudingos viešojo ir privataus sektorių partnerystės užtikrinant kibernetinį saugumą įgyvendinimo Lietuvoje būtina atlikti nuodugnesnius tyrimus siekiant suformuoti efektyvų CSP3 karkasą ar partnerystės gaires savireguliacijai, kuriose turi būti aiškiai apibrėžtos galimos partnerių atsakomybės ribos, atsakingo informacijos dalinimosi aspektai ir saugos užtikrinimo kontrolės, partnerystės koordinatoriaus nuo viešojo sektoriaus paskyrimas ir vaidmuo bei komunikacijos kanalas. Analizuojamuoju momentu CSP3 yra įtraukta į patvirtintą kibernetinio saugumo strategiją kaip vienas iš esminių uždavinių, taip pat, kibernetinio saugumo įstatymu, yra paskirtas viešojo sektoriaus atstovas atsakingas už kibernetinio saugumo politikos formavimą, įgyvendinimą, kontrolę ir koordinavimą šalyje – Krašto apsaugos ministerija, kibernetinio saugumo krizių koordinavimas pavestas Nacionaliniam kibernetinio saugumo centrui. Remiantis išnagrinėta užsienio šalių praktika, rekomenduojama sukurti ir įgyvendinti informacijos dalinimosi platformas ir analizės centrus, ne tik kritinės infrastruktūros apimtyje, vystyti ir plėtoti mokslinę tiriamąją veiklą

šalies mastu kibernetinio saugumo srityje kuriant partnerystės koncesijas stiprinančias vidinį valstybės kibernetinio atsparumo potencialą ir užtikrinant tiekimo grandinės saugumą, organizuoti aktyvesnį tarpdisciplininių specialybių ir kompetencijų rengimą pasitelkiant privataus sektoriaus kompetencijas (ir finansavimą), akademinio sektoriaus išteklius (paskiriant koordinatoriumi bei vykdytoju) ir viešojo sektoriaus finansavimą (ir rizikas), koordinuojančiai institucijai aktyviai ir skaidriai bendradarbiauti su privačiu sektoriumi kuriant pasitikėjimą ir išlaikant privataus sektoriaus susidomėjimą. Svarbus tolimesnės partnerystės kūrimo elementas – jau įgyvendinamų CSP3 iniciatyvų tęstinio proceso užtikrinimas.

LITERATŪRA

Akintoye, A., Beck, M., & Kumaraswamy, M. (2015). *public Private Partnerships: A Global Review.* Routledge.

Augustinaitis, A., Rudzkienė, V., Petrauskas, A. R., Dagytė, I., Martinaitytė, E., Leichteris, E., . . . Žilionienė, I. (2009). *Lietuvos e. valdžios gairės: atieties įžvalgų tyrimas.* Vilnius: Mykolo Romerio universitetas.

Baxter, J., Cunningham, B., Greenwald, E., Jacoby, J., Longley, J., Nolte, W., . . . Young, M. (2009). *Addressing Cyber Security Through Public-Private Partnership: An analysis of Existing Models.* Intelligence and National Security Alliance. Paimta 2018 m. spalio 5 d. iš https://www.insaonline.org/addressing-cyber-security-through-public-private-partnership-an-analysis-of-existing-models/

Bechkoum, K., Thomas, P., Campbell, L., & Brown, M. (2017). *Towards stronger cyber security public private partnerships in developing countries.* University of Gloucestershire. Retrieved 10 2018, from https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/FINAL%20REPORT%20CS%20PPP%20-%20FCO-BoE%20Final%20Copy.pdf

Bel, G., Brown, T., & Marques, R. (2016). *Public-Private Partnerships: Infrastructure, Transportation and Local Services.* Routledge.

Brock, W. A., & Hommes, C. H. (1997). A rational route to randomness. *Econometrica, 65*(5), 1059-1095.

Burke, R., & Demirag, I. S. (2016). Risk transfer and stakeholder relationships in Public Private Partnerships. *Accounting Forum (Account Forum)*. doi:10.1016/j.accfor.2016.06.004

Buso, M., Marty, F., & Tra, T.-P. (2016). Public-Private Partnerships from Budget Constrains: Looking for Debt Hiding? *International Journal of Industrial Organization*. Paimta 2018 m. 10 23 d. iš https://halshs.archives-ouvertes.fr/halshs-01275217/document

Carr, M. (2016 m. Sausio 1 d.). Public–private partnerships in national cyber-security strategies. *International Affairs, 92*(1), 43–62. doi:doi.org/10.1111/1468-2346.12504

Dūda, M. (2010). Teoriniai viešojo ir privataus sektorių partnerystės įgyvendinimo aspektai. *Viešoji politika ir administravimas*(33), 139-151. doi:2029-2872

ENISA. (2017). *Public Private Partnerships (PPP) Cooperative models.* Heraklion, Greece: European Union Agency for Network and Information Security. doi:10.2824/076734

European Commision. (2016 m. liepos 5 d.). Contractual Public Private Partnership on Cybersecurity and Accompanying Measures. *Commission Decision on the signing of a contractual arrangement on a public-private partnership for cybersecurity industrial research and innovation between the European Union*. Brussels. Paimta 2018 m. spalio 16 d. iš https://ec.europa.eu/transparency/regdoc/rep/10102/2016/EN/10102-2016-216-EN-F1-1-ANNEX-1.PDF

European Network and Information Security Agency. (2011). *Cooperative Models for Effective Public Private Partnerships.* Heraklion, Greece. doi:10.2824/21793

Europos komisija. (2015). *EUR-Lex.* Paimta 2018 m. gegužės 1 d. iš A Digital Single Market Strategy for Europe: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447773803386&uri=CELEX:52015DC0192

Europos parlamentas. (2016 m. sausio 19 d.). *European Parliament.* Paimta 2018 m. gegužės 1 d. iš Towards a Digital Single Market Act: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2016-0009+0+DOC+PDF+V0//EN

Federal Ministry of the Interior. (2009). National Strategy for Critical Infrastructure Protection (CIP Strategy). Berlin, Germany. Paimta 2018 m. rugsėjo 18 d. iš https://www.kritis.bund.de/SharedDocs/Downloads/BBK/EN/CIP-Strategy.pdf?__blob=publicationFile

Gall, M. D., Gall, J. P., & Borg, W. R. (2007). *Educational research: An Introduction* (8 leid.). Pearson/Allyn & Bacon, 2007.

Germano, J. H. (2014). *Cybersecurity partnerships: A new era of Public-Private collaboration.* New York University School of Law. New York: The Center on Law and Security. Nuskaityta iš http://www.lawandsecurity.org

Givens, A. D., & Busch, N. E. (2013). Realizing the promise of public-private partnerships in U.S. critical infrastructure protection. *International Journal of Critical Infrastructure protection, 6*, 39-50.

Gudelis, D., & Rozenbergaitė, V. (2004). Viešojo ir privataus sektorių partnerystės galimybės. *Viešoji politika ir administravimas*(8), 58-73. doi:1648-2603

HM Government. (2016). National Cyber Security Strategy 2016-2021. London. Paimta 2018 m. rugsėjo 23 d. iš https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Hodge, G., & Greve, C. (2007). Public-Private Partnerships: An International Performance Review. *Public Administration Review, 67*(3), 545-558.

Jakutyte, J. (2012). Analysing Public-Private Partnership. *Magistro baigiamasis darbas*. Aarhus University. Paimta 2018 m. spalio 24 d. iš http://pure.au.dk/portal/files/48150942/MSc_thesis_Jurgita_Jakutyte.pdf

Kavaliauskaitė, V., & Jucevičius, R. (2009). Viešojo ir privataus sektorių partnerstės svarba realizuojant regiono konkurencinę strategiją. *Ekonomika ir vadyba, 14*, 809-818.

Klijn, E.-H., & Teisman, G. R. (2003). Institutional and Strategic Barriers to Public Private Partnership: An Analysis of Dutch Cases. *Public Money & Management, 23*(3), 137-146.

Lietuvos Respublikos krašto apsaugos ministras. (2018 m. gegužės 8 d.). Dėl Krašto apsaugos ministro 2015 m. gegužės 26 d. įsakymo Nr. V-535 "Dėl kibernetinio saugumo tarybos personalinės sudėties patrvitinimo" pakeitimo. *Įsakymas Nr. 422*. Vilnius. Paimta 2018 m. rugsėjo 29 d. iš https://www.e-tar.lt/portal/lt/legalAct/e91cbf90534e11e884cbc4327e55f3ca

Lietuvos Respublikos Ūkio ministerija. (2010 m. liepos 16 d.). Dėl Viešojo ir privataus sektorių partnerystės tikslingumo kirterijų nustatymo ir Metodinių rekomendacijų dėl Viešojo ir privataus sektorių aprtnerystės taikymo tikslingumo kriterijų patvirtinimo. *Įsakymas*. Vilnius. Paimta 2018 m. spalio 29 d. iš https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.378578

Lietuvos Respublikos Vyriausybė. (2015 m. balandžio 23 d.). Dėl kibernetinio saugumo tarybos sudarymo ir jos reglamento patvirtinimo. *Nutarimas Nr. 422*. Vilnius. Paimta 2018 m. rugsėjo 25 d. iš https://www.e-tar.lt/portal/lt/legalAct/4e3539f0ee4611e4927fda1d051299fb

Liu, T., Wang, Y., & Wilkinson, S. (2016). Identifying critical factors affecting the effectiveness and efficiency of tendering processes in Public-Private Partnerships (PPPs): A comparative analysis of Australia and China. *International Journal of Project Management*(34), 701-716. doi:10.1016/j.ijproman.2016.01.004

Luiijf, E., Besseling, K., & de Graaf, P. (2013). Nineteen national cybersecurity strategies. *Critical Infrastructures, 9*(1/2), 3-31. doi:10.1504/IJCIS.2013.051608

Mantzoufas, N. (2017 m. lapkričio 7 d.). The 24 Schools PPP in Greece: a lesson i perseverance and innovative funding. *Infrastrukcture & Public private partnerships Blog*. Paimta 2018 m. rugsėjo 24 d. iš http://blogs.worldbank.org/ppps/24-schools-ppp-greece-lesson-perseverance-and-innovative-funding

McGraw Hill Construction. (2009). Public-private partnership: Accelerating transportation.

Namavičiūtė, I. (2018). *Pasiūlymai dėl kibernetinio saugumo specialistų ugdymo Lietuvoje.* Vilnius: Programa "Kurk Lietuvai". Paimta 2018 m. spalio 28 d. iš http://kurklt.lt/wp-content/uploads/2018/04/KS-pasi%C5%ABlymai-talent%C5%B3-vytymui-Lietuvoje-galutin%C4%97.pdf

National Cooperative Highway Research Program. (2009). *Public sector decision making for Public-Private Partnerships.* Washington, D.C.: Transportation research board. doi:10.17226/13901

NCSC. (2018 m. rugpjūčio). *Cyber Security Assessment Netherlands CSAN 2018.* Paimta 2018 m. rugsėjo 12 d. iš National Coordinator for Security and Counterterrorism: https://www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/cyber-security-assessment-netherlands/cyber-security-assessment-netherlands-2018/1/cyber_security_assessment_netherlands_2018.pdf

Oehme, R. (2015). Cyber security in Sweden. *With focus on National Collaboration forum and Private Public Partnership*, (p. 40). Paimta 2018 m. rugsėjo 18 d. iš https://www.viestintavirasto.fi/attachments/esitykset/Richard_Oehme_Presentation_Fi_2015-11-04.pdf

Paliulis, N. K., Meidutė, I., & Garškienė, A. (2008). Lietuvos transporto sistemos modernizavimo ir plėtros galimybės taikant viešojo ir privataus sektorių partnerystės (PPP) finansavimo modelį. Vilniaus Gedimino technikos universiteto transporto institutas. Paimta 2018 m. rugsėjo 25 d. iš https://sumin.lrv.lt/uploads/sumin/documents/files/Teisine_informacija/Tyrimai_ir_analizes/PPP_ataskaita_Galutine.pdf

Rasimavičiūtė, D., Sadaunykaitė, G., & Bernotas, I. (2014). *Kibernetinis saugumas: bendradarbiavimas tarp viešojo ir privataus sektorių.* Vilnius: Jaunųjų profesionalų komanda "Kurk Lietuvai".

Ropė, Ž. (2015). Organizacijos X kibernetinės erdvės gynyba. 99. Vilnius: Mykolo Romerio universiteto verslo ir medijų mokykla.

Savas, E. S. (2000). *Privatization and punlic-private partnerships.* New York: Sevent Bridges Press, LLC.

Shafqat, N., & Masood, A. (2016 m. sausis). Comparative Analysis of Variuos National Cyber Security Strategies. *International Journal of Computer Science and Information Security, 14*(1), 129-136. Nuskaityta iš https://sites.google.com/site/ijcsis/

Skelcher, C. (2010). Governing partnerships. Esantis G. Hodge, C. Greve, & A. E. Boardman, *International Handbook on Public-Private Partnerships* (p. 292-304). Cheltenham: Edward Elgar.

Skietrys, E., & Raipa, A. (2009). Viešosios ir privačios partnerystės socialinio poveikio vertinimo teoriniai aspektai. *Socialinis darbas, 1*(8), 11-16. doi:2029-2775

Solana, J., Saz-Carranza, A., & Estebanez Gomez, J. F. (2016). *On the way towards a European Defence Union - White Book as a first step.* European Union, European Parliament's Committee on Foreign Affairs. EU. doi:10.2861/058460

Štitilis, D. (2013). Kibernetinio saugumo teisinis reguliavimas: kibernetinio saugumo strategijos. *Socialinės technologijos, 3*(1), 189-207.

Štitilis, D., Pakutinskas, P., Laurinaitis, M., & Malinauskaitė-van de Castel, I. (2017). *Lietuvos kibernetinio saugumo strategijos modelis.* Vilnius: Mykolo Romerio universitetas. Paimta 2018 m. lapkričio 2 d. iš https://repository.mruni.eu/handle/007/14642

Šutavičienė, Ž. (2011). Viešojo ir privataus sektorių partnerystės poreikis ir galimybės Lietuvoje. *Socialinių mokslų studijos, 3*(3), 789-815. doi:2029-2244

Tidikis, R. (2003). *Socialinių mokslų tyrimų metodologija.* Vilnius: Lietuvos teisės universitetas.

Transportation Research Board. (2009). *Public Sector Decision Making for Public-Private Partnerships: The Synthesis of Highway Practice.* Washington, D.C.: National Cooperative Highway Research Program. Paimta 2018 m. rugsėjo 12 d. iš https://www.nap.edu/read/13901/chapter/1

Transportation Research Board. (2018). *The relationship between transit asset condition and service quality.* Trancit Cooperative Research Program.

United States Government Accountability Office. (2008). *Federal-aid Highways: Increased Reliance on Contractors can pose overshight challenges for Federal and State Officials.* Washington, DC: GAO. Paimta 2018 m. rugsėjo 12 d. iš https://www.gao.gov/assets/280/270892.pdf

Užkuraitytė, G. (2015). Kibernetinio saugumo valdymo užtikrinimas: pasaulinė patirtis ir Lietuvos perspektyva. 83. Vilnius: Mykolo Romerio universiteto verslo ir medijų mokykla. Paimta 2016 m. gruodžio 27 d. iš http://gs.elaba.lt/object/elaba:14911194/14911194.pdf

Zetter, K. (2014 m. 12 14 d.). *Wired*. Paimta 2018 m. rugpjūčio 12 d. iš The evidence that North Korea hacked Sony is flimsy: https://www.wired.com/2014/12/evidence-of-north-korea-hack-is-thin/

Zhao, Z. J., Saunoi-Sandgren, E., & Barnea, A. (2011). *Advancing Public Interest in Public-Private Partnership of State Highway Development.* Minnesota: Minnesota Department of Transportation Research Services Section. Paimta 2018 m. rugsėjo 12 d. iš http://www.lrrb.org/pdf/201109.pdf

Žilinskas, R., & Trakimavičius, L. (2016). The Perils of Cyber-attacks against the Energy Industry. *Energy Security: Operational Highlights, 10*, 10-17. Nuskaityta iš https://www.icds.ee

Breivė J. (2018). *Viešojo ir privataus sektorių partnerystė užtikrinant kibernetinį saugumą Lietuvoje* (magistro baigiamasis darbas).

ANOTACIJA

Magistro baigiamojo darbo tikslas – išanalizuoti viešojo ir privataus sektorių bendradarbiavimo užtikrinant kibernetinį saugumą situacija ir plėtros galimybes Lietuvoje. Darbe išanalizuotos ir įvertintos klasikinio viešojo ir privataus sektorių formos bei metodai, valdymo būdai, tokios partnerystės skirtumai kibernetinio saugumo srityje, galimos jau egzistuojančios apraiškos Lietuvoje bei pateikti pasiūlymai dėl bendradarbiavimo apibrėžimo. Pirmoje dalyje teoriniu aspektu analizuojama viešojo ir privataus sektorių partnerystės samprata, bendradarbiavimo formos ir įgyvendinimo būdai, taip pat nagrinėjami esminiai skirtumai tokios partnerystės atsiradimo kibernetinio saugumo užtikrinimo apimtyje. Antroje dalyje analizuojamos užsienio šalių praktikos įgyvendinant viešojo ir privataus sektorių bendradarbiavimą kibernetinio saugumo srityje per kibernetinio saugumo strategijos prizmę. Pateikiami partnerystės apraiškų pavyzdžiai Lietuvoje ir Europoje, apibendrinti duomenys bei pateikiamos pagrindinės prielaidos tokios partnerystės vystymuisi. Trečioje dalyje atliekama kibernetinio saugumo srityje dirbančių ekspertų apklausa siekiant išsiaiškinti dabar egzistuojančias partnerystės apraiškas Lietuvoje, galimas bendradarbiavimo kryptis, daromas klaidas ir suformuojant išvadas dėl viešojo ir privataus sektoriaus partnerystės užtikrinant kibernetinį saugumą Lietuvoje tobulinimo.

Pagrindiniai žodžiai: viešojo ir privataus sektorių partnerystė, kibernetinis saugumas, bendradarbiavimas.

Breivė J. (2018). *Public-Private Partnership for Cyber Security in Lithuania* (master thesis). Vilnius: Mykolas Romeris University.

ANOTATION

The aim of the master's thesis is to analyze the situation of public-private cooperation in ensuring cybersecurity and development opportunities in Lithuania. The paper analyzes and evaluates the forms and methods of classical public and private sectors, methods of management, differences in such partnerships in the area of cyber security, possible existing forms in Lithuania, and presents proposals for the definition of co-operation. The first part analyzes and a theoretical point of view, the concept of public-private partnership, forms of cooperation and implementation methods, as well as examines the essential differences in the scope of ensuring such a partnership in the field of cyber security. The second part analyzes the practice of foreign countries in implementing public-private cooperation in the field of cyber-security through the prism of the cyber security strategy. The examples of partnership manifestations in Lithuania and Europe are presented, data are summarized and the main preconditions for the development of such a partnership are presented. In the third part, a survey of experts working in the field of cyber-security is being conducted in order to find out the current manifestations of partnership in Lithuania, possible directions of cooperation, mistakes and formulating conclusions on the improvement of partnership between the public and private sectors in ensuring cyber security in Lithuania.

Key words: public-private partnership, cybersecurity, cooperation, cybersecurity public-private partnership.

Breivė J. (2018). *Viešojo ir privataus sektorių partnerystė užtikrinant kibernetinį saugumą Lietuvoje* (magistro baigiamasis darbas).

SANTRAUKA

Nepaisant nuolankios kovos su sunkiai apibrėžiamomis kibernetinėmis grėsmėmis daugeliu atveju kuriama kibernetinio saugumo strategija grindžiama bendradarbiavimu. Vienas iš esminių kibernetinio saugumo, grėsmių neapibrėžtumui valdyti, strategijos elementų yra bendradarbiavimo tobulinimas ir informacijos dalybų įgalinimas tarp įvairių suinteresuotųjų šalių sukuriantis prielaidas viešojo ir privataus sektorių partnerystei: lygiaverčių partnerių atsakomybių susikūrimas, tarpusavio pasitikėjimas, rizikų prisiėmimas ir bendros naudos siekis.

Magistro baigiamojo darbo tikslas – išanalizuoti viešojo ir privataus sektorių bendradarbiavimo užtikrinant kibernetinį saugumą situacija ir plėtros galimybes Lietuvoje.

Teorinėje dalyje išanalizuota mokslinė literatūra ir įvertinta viešojo ir privataus sektorių partnerystės samprata, galimos įgyvendinimo formos bei būdai.

Praktinėje dalyje, remiantis užsienio šalių patirtimi apibrėžiant partnerystę strateginiame lygmenyje, analizuojant jau esamas tokio bendradarbiavimo apraiškas Lietuvoje bei dirbant su ekspertų patirtimi siekiama nustatyti kibernetinio saugumo užtikrinimo pasitelkiant viešojo ir privataus sektorių partnerystę galimybe ir grėsmes.

Tyrimo metu prieita prie išvados, kad nepaisant viešojo ir privataus sektorių partnerystės įgyvendinimo patirties bei teisinio reglamentavimo Lietuvoje jau galime nubrėžti konkrečias gaires tolimesniam apraiškų apibrėžimui ir tęstinumui. Nors įgyvendinami projektai vis dar kelia klausimų apie jų priskyrimą partnerystei, tačiau šių apraiškų įgyvendinimas gali turėti stiprią socialinę ir ekonominę naudą su abiem pusėms vienodai suprantamais tikslais bei teisingai pasidalinta rizika. Hipotezė: nepakankamas viešojo ir privataus sektorių bendradarbiavimas didina neracionalių kibernetinį saugumą reglamentuojančių teisės aktų ir reikalavimų atsiradimą, neišnaudojamos kibernetinio saugumo specialistų rengimo potencialas, neatsiranda tarpusavio pasitikėjimas, o tai įtakoja investuojamų kaštų į kibernetinio saugumo užtikrinimą privačioje infrastruktūroje didėjimą neišnaudojant visų įmanomų kibernetinio atsparumo priemonių valstybės mastu, pasitvirtino.

Pagrindiniai žodžiai: viešojo ir privataus sektorių partnerystė, kibernetinis saugumas, bendradarbiavimas.

Breivė J. (2018). *Public-Private Partnership for Cyber Security in Lithuania* (master thesis). Vilnius: Mykolas Romeris University.

SUMMARY

In spite of the humble struggle against hard-to-define cyber threats, cybersecurity strategies are often based on collaborative work. One of the key elements of the strategy for managing cybersecurity and managing uncertainties is to improve cooperation and enable information sharing between the various stakeholders to create a prerequisite for a public-private partnership: creating equal partner responsibilities, building trust, assuming risks and achieving common goals.

The aim of the master's thesis is to analyze the situation of public-private cooperation in ensuring cybersecurity and development opportunities in Lithuania.

The theoretical part analyzes scientific literature and evaluates the concept of public-private partnership, possible forms and methods of implementation.

In the practical part, based on the experience of foreign countries in defining partnership at the strategic level, analyzing the already existing manifestations of such cooperation in Lithuania and working with expert experience, aims to establish the possibility and threats of securing cyber security through public-private partnerships.

The study concludes that, in spite of experience in the implementation of public-private partnerships and legal regulation in Lithuania, we can already draw specific guidelines for further definition and continuity of expressions. Although ongoing projects still raise questions about their attribution to a partnership, implementation of these manifestations can have strong social and economic benefits with objectives that are equally comprehensible to both parties and share risks equitably. Hypothesis: Insufficient public-private partnerships increase the emergence of irrational laws and regulations on cyber security, the potential for training cyber security specialists, and the lack of mutual trust, which affects the increase in the cost of investing in cyber security in private infrastructure without exploiting all possible cyber-resistance measures at national level proved to be true.

Key words: public-private partnership, cybersecurity, cooperation, cybersecurity public-private partnership.

PRIEDAI

1 PRIEDAS. Informuotas asmens sutikimas dalyvauti tyrime

Gerb., [įrašomas dalyvio vardas],

2018 m. rugpjūčio 13 d. Lietuvos Respublikos Vyriausybė patvirtino Nacionalinę kibernetinio saugumo strategiją nustatydama penkerių metų laikotarpiui svarbiausias nacionalinės kibernetinio saugumo politikos viešajame ir privačiame sektoriuose kryptis. Vienas iš strateginių krypčių yra „glaudaus viešojo ir privataus sektorių bei mokslo institucijų bendradarbiavimo stiprinimas“.

Esu M. Romerio universiteto, Ekonomikos ir verslo fakulteto, Kibernetinio saugumo valdymo magistro studijų programos studentas Juozas Breivė. Šiuo metu atlieku baigiamojo darbo tyrimą tema „Viešojo ir privataus sektorių partnerystė užtikrinant kibernetinį saugumą Lietuvoje“. Atlieku tyrimą, kurio tikslas – ištirti viešojo ir privataus sektorių partnerystės užtikrinant kibernetinį saugumą Lietuvoje apraiškas. Darbo vadovas: Prof. dr. Darius Štitilis.

Prašau Jūsų prisidėti savo žiniomis bei patirtimi ir atsakyti į pateikiamus klausimus el. paštu. Tyrimo rezultatai padės įvertinti viešojo ir privataus sektorių partnerystės užtikrinant kibernetinį saugumą Lietuvoje situaciją ir įtaką bendram valstybės kibernetiniam atsparumui, taip pat Jūsų įžvalgos ir patirtis bus indėlis į tokios partnerystės formavimąsi Lietuvoje.

Visi tyrimo metu surinkti asmens duomenys išliks konfidencialūs ir bus naudojami tik šio tyrimo tikslais kaip apibendrinti rezultatai, padedantys parengti ir apginti baigiamąjį magistro studijų darbą ir išnagrinėti viešojo ir privataus sektorių partnerystės įgyvendinimą užtikrinant kibernetinį saugumą Lietuvoje. Asmens duomenys bus prieinami tik tyrimą atliekančiam studentui ir tik iki baigiamojo darbo sėkmingo apgynimo.

Jūsų vardas, pavardė ir el. pašto adresas, taip pat kiti duomenys pagal kuriuos galima identifikuoti apklausos dalyvį, nebus naudojami tyrimo išvadose ir bus nuasmeninti suteikiant arabiškais skaitmenimis pažymėtą unikalų kodą.

Atsakydamas į šiame el. laiške pateikiamus klausimus Jūs išreiškiate sutikimą dalyvauti atliekamame tyrime.

Į klausimus prašome atsakyti el. paštu arba kita Jums priimtina forma iki š.m. [mėnuo] [diena] d.

Jei turite klausimų ar pageidaujate detalesnės informacijos apie tyrimą prašome kreiptis į:

- tyrimo vykdytoją: Juozą Breivę telefonu +370 685 03489 arba el. paštu juozas.breive@gmail.com
- baigiamojo darbo vadovą: prof. dr. Darių Štitilį el. paštu stitilis@mruni.eu

Tyrimo klausimai:

1.Kokias viešojo ir privataus sektorių partnerystės (toliau PPP) apraiškas užtikrinant kibernetinį saugumą Lietuvoje šiuo metu pastebite?

2.Ar šiuo metu įgyvendinami PPP kibernetinio saugumo srityje projektai yra efektyvūs?

3.Kokia ekonominė ir socialinė PPP įgyvendinimo Lietuvoje užtikrinant kibernetinį saugumą vertė?

4.Kokie būtų pasiūlymai dėl PPP plėtros ar papildomų įgyvendinimo formų siekiant kibernetinio Lietuvos atsparumo?

5.Ar atskirų sektorių (viešojo ir privataus) įsitraukimas į PPP yra pakankamas su aiškiai apibrėžtomis atsakomybėmis ir rizikomis? Jei nepakankamas, tada ko trūksta ir ką reikėtų tobulinti?

6.Kokios PPP iniciatyvos nėra įgyvendintos Lietuvoje, nors buvo apie tai galvota, jos buvo inicijuotos arba jau pradėtos? Kokias neįgyvendinimo priežastis galite įvardinti?

7.Kokią gerąją PPP įgyvendinimo praktiką galima panaudoti žvelgiant į užsienio šalis? Kokie tokios gerosios praktikos įgyvendinimo pavyzdžiai ir kodėl jie pasiteisino (priežastys)?

Papildomai prašau atsakyti į žemiau pateiktus klausimus siekiant apibrėžti apklausoje dalyvaujančių asmenų grupę:

1.Koks organizacijos, kurioje dirbate, tipas (tarptautinė organizacija, vietinis verslas, valstybinė įstaiga (įmonė ir pan.)?

2.Koks organizacijos, kurioje dirbate, dydis (0-50, 51-100, 101-400, 401-1000 darbuotojų)?

3.Kokias atsakomybes ir pareigas (vaidmenis) užimate įvardintoje organizacijoje?

4.Kiek ilgai jau dirbate šioje organizacijos pozicijoje?

5.Kokia Jūsų patirtis informacijos ir kibernetinio saugumo srityje?

6.Ar Jūsų organizacija dalyvauja kokiuose nors kibernetinio saugumo PPP projektuose?

7.Jei atsakėte teigiamai į 6 klausimą, prašome įvardinkite kokią Jūsų darbo laiko dalį užima darbas pagal įvairius kibernetinio saugumo PPP projektus?

2 PRIEDAS. Ekspertų atsakymai el. paštu

Dalyviai Nr. 1-4, 7-8

Klausimai	Dalyvis Nr. 1	Dalyvis Nr. 2	Dalyvis Nr. 3	Dalyvis Nr. 4	Dalyvis Nr. 7	Dalyvis Nr. 8
1. Kokias viešojo ir privataus sektorių partnerystės (toliau PPP) apraiškas užtikrinant kibernetinį saugumą Lietuvoje šiuo metu pastebite?	Asociacija "Infobalt" – KAM bendradarbiavimas (aptariant, planuojant kibernetinio saugumo valdymą). Įmonė X – teisėsaugos analitikai: analitikų apvalaus stalo ketvirtinė diskusija. Kibernetinio saugumo taryba. Įmonės X ekspertų dėstymai įvairiose srityse (pvz. karo akademijoje).	Vienintelę informaciją, kurią aš žinau, galite rasti pagal žemiau nurodytą nuorodą: https://www.securityweek.com/lithuanian-media-sign-pact-govt-counter-hackers	Jei atvirai, tai didelių apraiškų nepastebiu. Yra bendradarbiavimas pvz. tarp Infobalt ir KAM kuriant įstatyminę bazę, bet jis nėra oficialus, sakyčiau kad viskas yra labiau asmeninių santykių lygyje. Yra pavieniai užsakymai universitetams padaryti tyrimus, bet tai nėra sistema. Gal galima būtų prie partnerystės priskirti kibernetinių pratybų (Gintarinė migla/Kibernetinis skydas), kurios vyksta naudojant KTU ir VU informacinių sistemų resursus, vykdymą. Pernai Infobalt kartu su KAM organizavo konferenciją CyberInn. Kibernetinio saugumo tarybą galima būtų priskirti prie PPP, nes į ją	Manau, kad pastarųjų mėnesių bendra kelių šalių (įskaitant Lietuvos) numatyti automatines ES sankcijas už kibernetinius nusikaltimus yra labai gera politikų iniciatyva kuri padės ir privačiam sektoriui. Nesu tikras ar tai tikrai patenka į PPP apibrėžimą, bet laikau tikrai naudinga iniciatyva kibernetiniam saugumui.	Kibernetinio saugumo taryba, Nacionalinės kibernetinio saugumo pratybos. Jei bus realizuotas kibernetinio saugumo informacinio tinklo prieinamumas ir privačiam sektoriui, tai ir ši veikla. Bendrų renginių rengimas kibernetinio saugumo tema	Iki šiol nesu pastebėjęs, bet natūralu nes mano žiniomis, tik nesenai Infobalt aptarinėjo siūlyti modelį/ius (nes strategijoje PPP yra numatytas).

Klausimai	Dalyvis Nr. 1	Dalyvis Nr. 2	Dalyvis Nr. 3	Dalyvis Nr. 4	Dalyvis Nr. 7	Dalyvis Nr. 8
			įeina įvairių sektorių atstovai. Bet jos įgaliojimai yra labai riboti, tai yra patariamasis darinys, o realiai, bent iki šiol, yra periodinis informacijos apie tai ką daro KAM, NKSC platinimas tarp tarybos narių. Bet, sakyčiau, kad tai yra padriki atvejai, ir nėra sistemos pagal kurią vyktų bendradarbiavimas. Dar prisiminiau Lietuvos koordinuojamą Europos Sąjungos PESCO Greitojo kibernetinio reagavimo komandų (CRRT) projektą. Projektas apima tam tikrų priemonių sukūrimą, kas gali būti įdomu Lietuvos įmonėms.			
2. Ar šiuo metu įgyvendinami viešojo ir privataus sektorių partnerystės kibernetinio saugumo srityje projektai yra efektyvūs?	Daugmaž, pagal savo ambicijų lygį.	Sunku pasakyti. Pagal Kibernetinio saugumo įstatymą https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc990	Sakyčiau, kad ne, nes nėra sistemos. Yra padrikos iniciatyvos, kurios nėra sistemos leidžiančios:	Deja, negaliu įvertinti, nes nesu susipažinęs ar girdėjęs apie šiuos projektus.	Kadangi kibernetinio saugumo projektai yra ne infrastruktūriniai, o daugiau susiję su kompetencijos kėlimu, tai sunku	ne, nes nelabai yra PPP

Klausimai	Dalyvis Nr. 1	Dalyvis Nr. 2	Dalyvis Nr. 3	Dalyvis Nr. 4	Dalyvis Nr. 7	Dalyvis Nr. 8
		1227533ee numatyta Kibernetinio saugumo tarybos (9 straipsnis) sukūrimas. Ten turėtų atsispindėti Lietuvos PPP, tačiau nežinau kiek kartų per metus taryba susirenka, kas dalyvauja, kokie klausimai yra keliami ir kokie pasiūlymai yra svarstyti ir pateikti. PPP potencialas yra, tačiau, mano nuomone, pakankamai nepasinaudota.	gerinti bendrą žinių apie kibernetinio saugumą lygį, didinti bendrą Lietuvos atsparumą kibernetinėms grėsmėms bei gebėjimą gintis, kurti kibernetinio saugumo paslaugų, produktų rinką, skatinti tyrimus kibernetinio saugumo srityje, įtraukti privatų sektorių į kibernetinių paslaugų teikimą viešajam sektoriui, sistemingai keistis informaciją apie kibernetinį saugumą, apjungti privataus ir viešojo sektorių gebėjimus, ruošti kibernetinio saugumo profesionalus dalimi.		pamatuoti jų efektyvumą, bet kad yra naudingi abiem pusėms tai tikrai. Jei laikyti, kad NKSC sensorių diegimas yra PPP veikla, tai šis projektas pakankamai efektyvus	
3. Kokia ekonominė ir socialinė viešojo ir privataus sektorių partnerystės įgyvendinimo Lietuvoje užtikrinant kibernetinį saugumą vertė?	Nedidelė. Bet niekas ir nekelia aukštų tikslų.	Potencialiai galėtų būti didelė, kadangi kibernetinė sauga sąlygoja šalies ekonominę ir socialinę būklę. Sėkminga kibernetinė ataka, nutaikyta prieš šalies ypatingos svarbos infrastruktūras, turėtų rimtų pasekmių.	Vystant PPP kiltų bendras kibernetinio saugumo žinių lygis, būtų daugiau skiriama dėmesio kibernetiniam saugumui, kas savo ruožtu mažintų riziką nukentėti nuo kibernetinių piktavališkų veikų, o tai reikia ir mažintų	Manau, kad labai daug kibernetinio saugumo sprendimų yra teisiniame reglamentavime, todėl viešojo sektoriaus vaidmuo yra itin svarbus.	Vertė yra pakankamai didelė, kadangi privataus sektoriaus patirtį ir žinias viešasis sektorius gauna neatlygintinai, o privatus sektorius ne tik turi galimybę pasirodyti, užsirekomenduoti, bet ir gali pagilinti savo žinias ir	vienareikšmiškai teigiama, resursų sutelkimas ir veikimas iš vien leis efektyviai įgyvendinti kibernetinį saugumo Lietuvoje

Klausimai	Dalyvis Nr. 1	Dalyvis Nr. 2	Dalyvis Nr. 3	Dalyvis Nr. 4	Dalyvis Nr. 7	Dalyvis Nr. 8
			galimus finansinius nuotolius. Privataus ir viešojo sektorių pajėgumų apjungimas leistų efektyviau išnaudoti turimus resursus. PPP šalys galėtų pasinaudoti geriausiais kitų šalių gebėjimais. Nepaslaptis, kad bent jau šiuo metu, privataus sektoriaus kiber gebėjimai ir sukauptos žinios yra geresni, todėl jų panaudojimas viešajame sektoriuje, leistų greičiau ir efektyviau kelti kibernetinę saugą viešajame sektoriuje. Tai tuo pačiu kurtų naujas darbo vietas privačiame sektoriuje, didintų Lietuvos specialistų kompetenciją ir bei Lietuvos įmonių konkurencingumą užsienio rinkose. Bendradarbiavimas su švietimo sektoriumi, leistų išvystyti kibernetinių		supratimą kitose situacijose nei dirba įprastai	

Klausimai	Dalyvis Nr. 1	Dalyvis Nr. 2	Dalyvis Nr. 3	Dalyvis Nr. 4	Dalyvis Nr. 7	Dalyvis Nr. 8
			tyrimų sritį bei tyrimų rezultatų panaudojimą viešajame ir privačiuose sektoriuose. Tai vėl keltų konkurencingumą, vestų prie EU kibernetinio saugumo paslaugų ir produktų kūrimo. Konkrečių uždavinių kėlimas švietimo sektoriui didintų studentų susidomėjimą šia sritimi, būtų ruošiamo nauji specialistai, kurie įgytų ne tik teorines, bet ir praktines žinias. Kas savo ruoštu vėl keltu Lietuvos konkurencingumą. EU yra pripažinusi, kad stipriai atsilieka kibernetinio saugumo srityje nuo JAV ir ieško būdų kaip suaktyvinti šią sritį. Vienas iš žingsnių to link buvo Cyber cPPP pasirašymas 2016m. (http://europa.eu/rapid/press-release_IP-16-2321_en.htm)			

Klausimai	Dalyvis Nr. 1	Dalyvis Nr. 2	Dalyvis Nr. 3	Dalyvis Nr. 4	Dalyvis Nr. 7	Dalyvis Nr. 8
			Iš esmės PPP, manau, gali būti katalizatoriumi išjudinant ir auginant kibernetinio saugumo rinką Lietuvoje, bei plečiant eksportą.			
4. Kokie būtų pasiūlymai dėl viešojo ir privataus sektorių partnerystės plėtros ar papildomų įgyvendinimo formų siekiant kibernetinio Lietuvos atsparumo?	Nėra.	Puikus sektinas PPP pavyzdys yra Izraelis. Kibernetinis saugumas kaip sritis yra šalies ekonomikos dalis. Žiūrėkite į https://cyberstartupobservatory.com/cybersecurity-landscape-slide-israel/ Deja, Lietuvoje nieko nėra panašaus, tačiau galėtų būti.	Sunkus klausimas. Galbūt turėtų būti duodama daugiau užsakymų tyrimams ir produktų sukūrimui universitetams ir privataus sektoriaus įmonėms. Turėtų būti bent dalinai finansuojami tyrimai, paslaugų, produktų kūrimas. Turėtų būti sukurta sistema kaip yra apsikeičiama informacija ir žiniomis tarp privataus, viešojo sektorių. Viešasis sektorius neturėtų bijoti bent dalies paslaugų tiekimą atiduoti į privačias ranka. Tam reikia taisyklių reikalavimų, sertifikavimo ir pan. Šiais laikais atsparumą galima didinti ne atsiribojant vieniems nuo kitu, o	Papildomas teisinis reglamentavimas šalies ir ES mastu galėtų padėti. Pavyzdžiai - Bendrasis duomenų apsaugos reglamentas, JAV vienos iš valstijų gero reglamentavimo pavyzdys - https://www.forbes.com/sites/leemathews/2018/09/21/california-lawmakers-want-to-ban-bad-default-passwords/#a8de7c540daa	Atsižvelgiant į viešojo sektoriaus kompetencijas ir finansinius resursus, PPP galėtų pasireikšti ir per tam tikrų sprendimų kūrimą ir pritaikymą viešajam sektoriui ar tam tikros SOC paslaugos teikimą, nes NKSC nesugebės pilnai padengti viso sektoriaus. Už tai privačiam sektoriui gali būti mokama arba kitaip padengiamos išlaidos	pasirinkti teisingą modelį, efektyvus informacijos keitimasis, aiškūs “stakeholderiai”

Klausimai	Dalyvis Nr. 1	Dalyvis Nr. 2	Dalyvis Nr. 3	Dalyvis Nr. 4	Dalyvis Nr. 7	Dalyvis Nr. 8
			kaip tik kuo labiau keičiantis informacija, žiniomis. Dabartinė aplinka yra per daug dinamiška, kad galėtume susitvarkyti kiekvienas atskirai. Privatus sektorius ir švietimo įstaigos turėtų būti labiau įtrauktos į įstatyminės bazės kūrimą ir tobulinimą. Gal turėtų atsirasti ir bendrų grupių finansavimo modelis, kad privačiam sektoriui nereikėtų dirbti vien visuomeniniais pagrindais.			
5. Ar atskirų sektorių (viešojo ir privataus) įsitraukimas į viešojo ir privataus sektorių partnerystę yra pakankamas su aiškiai apibrėžtomis atsakomybėmis ir rizikomis? Jei nepakankamas, tada ko trūksta ir ką reikėtų tobulinti?	Pagal tai, kas vyksta ar kokie tikslai – pakankamas.	Trūksta tiktai valios, lyderio bei bendro noro pasiekti užsibrėžto tikslo, pvz., sukurti "cybersecurity landscape". Remiantis nurodytu Izraelio PPP pavyzdžiu, būtų galimybė šalies kibernetinio saugumo pramonės plėtrai.	Nepakankamas. Kaip ir rašiau anksčiau, yra padrikos iniciatyvos, bet nėra sistemos. Bėda tame ir yra, kad nėra apibrėžtos rolės, nėra atsakomybių , nėra oficialių susitarimų, nėra finansavimo modelių. Visų pirma reikėtų išsigryninti koks PPP modelis Lietuvai būtų priimtinas, tada, greičiausiai, reikėtų atlikti įstatyminės	Negaliu komentuoti- nesu pakankamai susipažinęs su šia tema.	Manau, kad pakankamai aiškiai apibrėžta. Bet trūksta iniciatyvos, supratimo, kad PPP naudingas ne tik valstybei, bet ir verslui. Manyčiau, kad trūksta daugiau bendravimo ir bendradarbiavimo, kad PPP vystytųsi	negaliu pakomentuoti, bet manau tarp atskirų sektorių PPP turbūt egzistuoja

Klausimai	Dalyvis Nr. 1	Dalyvis Nr. 2	Dalyvis Nr. 3	Dalyvis Nr. 4	Dalyvis Nr. 7	Dalyvis Nr. 8
			bazės pakeitimus, turėtų atsirasti susitarimai su šalių rolėmis ir atsakomybėmis , bei finansavimo modeliais. Konkrečių pasiūlymu negalėčiau dabar pasakyti. Tam tikrų minčių galima rasti pvz. šiame dokumente https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/FINAL%20REPORT%20CS%20PPP%20-%20FCO-BoE%20Final%20Copy.pdf			
6. Kokios viešojo ir privataus sektorių partnerystės iniciatyvos nėra įgyvendintos Lietuvoje, nors buvo apie tai galvota, jos buvo inicijuotos arba jau pradėtos? Kokias neįgyvendinimo priežastis galite įvardinti?	Neteko girdėti apie tokias.	Nežinau, ar buvo iš vis tokių iniciatyvų, nebent „Saulėtekio slėnis“. 1993 metais LR Vyriausybė rėmė projektą “Lietuva 2000”. Koordinuoti šalies ryšių ir kibernetinę politiką buvo sukurta LR Ryšių ir informatikos ministerija. Dėl daugiau informacijos žiūr: https://ccdcoe.org/site	Kažkokių konkrečių iniciatyvų negalėčiau įvardinti. Atskiros idėjos buvo, bet nesakyčiau, kad už jas kažkas labai stipriai būtų „kovojęs“. Taip pat sakyčiau, kad idėjos, kurios buvo iškeltos nėra atmestos ir po truputį skinasi savo kelią, gal tik ne taip greitai kaip norėtųsi. Ne karta buvo	Negaliu komentuoti- nesu pakankamai susipažinęs su šia tema.	Lietuvoje PPP iniciatyvų kibernetinio saugumo srityje kaip ir nebuvo daug numatytų. Buvo ieškoma, galvojama ką būtų galima padaryti per PPP, tačiau iki konkrečių veiklų nebuvo prieita, todėl galima sakyti, kad didesnės PPP iniciatyvos strigo dėl kūrybiškumo ar iniciatyvumo stokos,	mano manymu jos dabar yra procese.

Klausimai	Dalyvis Nr. 1	Dalyvis Nr. 2	Dalyvis Nr. 3	Dalyvis Nr. 4	Dalyvis Nr. 7	Dalyvis Nr. 8
		s/default/files/multimedia/pdf/CS_organisation_LITHUANIA_092015.pdf). Deja, realiai projektas nebuvo vykdomas, finansavimas neskirtas, 1998 m. ministerija buvo panaikinta ir jos funkcijos išbarstytos tarp likusių ministerijų. Manau, kad tos nesėkmės susiję su perimamumo nebuvimu keičiantis vyriausybėms. Tęstiniai projektai negauna pakankamai dėmesio, tenka daug iniciatyvų pradėti „iš naujo“.	kalbėta, kad reikėtų kažkokio darinio, kuris dalyvautų įstatyminės bazės kūrime ir tobulinime nuo pirmų akimirkų. Tačiau , bent jau kol kas, niekas nesugalvoja kaip oficialiai įtraukti privatų sektorių į tokią veiklą, kad tai nebūtų laikoma kaip įtakojimas siekiant sau naudos. Todėl dažnokai, bet ne visada, apie naujus dokumentus privatus sektorius sužino tik suderinimo etape ir ką nors keisti jau būna pakankamai sunku. Buvo kalba apie informacijos, apie kibernetinio saugumo įvykius, mainų sistemos sukūrimą, kuria galėtu naudotis tiek viešasis tiek privatus sektoriai. Idėja palaipsniui yra vystoma. Idėja, kad galėtų būti sukurta kibernetinio saugumo paslaugas teikiančių įmonių sertifikavimo		t.y. nebuvo tinkamai suformuoja idėja (priemonė) su konkrečiais tikslais ir uždaviniais	

Klausimai	Dalyvis Nr. 1	Dalyvis Nr. 2	Dalyvis Nr. 3	Dalyvis Nr. 4	Dalyvis Nr. 7	Dalyvis Nr. 8
			sistema. Tas leistų nustatyti kurios įmonės gali teikti kibernetinio saugumo paslaugas viešajam sektoriui ir kokia apimtimi. Idėja nėra numarinta, bet sunkiai skinasi kelią. Tokių iniciatyvų yra ir daugiau, bet aktyvumo jas vystant, sakyčiau, kad trūksta iš abiejų pusių. Sakyčiau, kad pirmas dalykas dėl ko taip sunkiai skinasi kelią PPP, tai PPP įgyvendinimo patirties nebuvimas. Iki galo nesuprantame kas tai yra, kokia to nauda ir tuo labiau kaip tai įgyvendinti. Dar vienas faktorius yra tai, kad kibernetiniu saugumu Lietuvoje užsiima KAM, o tai, istoriškai yra pakankamai uždara organizacija ir pakankamai sunkiai einanti į bendradarbiavimą. Nors reikia pripažinti, kad tai tikrai keičiasi			

Klausimai	Dalyvis Nr. 1	Dalyvis Nr. 2	Dalyvis Nr. 3	Dalyvis Nr. 4	Dalyvis Nr. 7	Dalyvis Nr. 8
			ir į gerąją pusę. Kalbant apie PPP atskiras iniciatyvas, dažnai kyla klausimas, o kaip tai legaliai apiforminti. Dar dažnai yra sunkiai suprantama, kad viešas ir privatus sektoriai gali bendradarbiauti ir siekti bendros naudos. Siekiant pagerinti situaciją, vienas iš galimų variantų galėtų būti detalios studijos apie cybersecurty PPP modelius, jų pritaikomumą Lietuvoje užsakymas pas akademinį sektorių. Tai, manau, būtų naudinga tiek viešajam tiek privačiam sektoriams, nes tikiuosi įvestų daugiau aiškumo kaip vistyti PPP.			
7. Kokią gerąją viešojo ir privataus sektorių partnerystės įgyvendinimo praktiką galima panaudoti žvelgiant į užsienio šalis? Kokie	Vienas ar kitas sektorius pasiūlo/susiderina techninius reikalavimus reguliavimui ir tada jie priimami	Žiūr. į atsakymus į ketvirtą ir penktą klausimus. Izraelio politika šiuo klausimu tikrai pasiteisino, kadangi jie supranta kad jų	Aš analizės nedariau, todėl negalėčiau atsakyti. Kaip minėjau, būtų gerai, kad būtų atlikta rimta studija šia tema.	Manau kibernetinio saugumo sritis reikalauja daugiau reguliatoriaus/reguliu ojamojo santykio, o ne partnerystes. Privatus sektorius	Užsienyje pakankamai daug geros ir skirtingos praktikos. Kiekviena šalis turi skirtingą požiūrį, kurį nebūtinai galima	Didžioji Britanija, Olandija

Klausimai	Dalyvis Nr. 1	Dalyvis Nr. 2	Dalyvis Nr. 3	Dalyvis Nr. 4	Dalyvis Nr. 7	Dalyvis Nr. 8
tokios gerosios praktikos įgyvendinimo pavyzdžiai ir kodėl jie pasiteisino (priežastys)?	/patvirtinami valstybės (pvz. suderintas atsakingo informacijos atskleidimo susitarimas).	valstybė yra maža, be resursų, tačiau turi didelius intelektualinius resursus. Jie pasinaudoja tuo, ką jie turi labai efektyviai. Lietuvoje yra panaši situacija, tačiau nėra tokio supratimo kaip pvz., Izraelyje. Trūksta lyderio, valios ir bendro noro pasiekti kilnių tikslų. Lietuva viską turi, bet - deja.	Galėčiau gal paminėti, kad neblogai atrodo Nyderlandų ir Didžiosios Britanijos bendradarbiavimo modeliai, bet apie priežastys kodėl jie pasiteisino negalėčiau pasakyti.	savarankiškai nesugebėjo išspręsti kibernetinio saugumo problemos. Pats privataus sektoriaus tikslas - pelno siekimas dažnai kertasi su saugumo tikslu, todėl aš esu šalininkas griežtesnio reglamentavimo/reguliavimo iš viešojo sektoriaus. Pavyzdžiai - jau minėti BDAR, Kalifornijos valstijos iniciatyvos.	pritaikyti Lietuvoje. Lietuvos PPP veiklų alternatyvos pastebimos ir kitose valstybėse. Kitos valstybės daugiau valstybės funkcijų yra atidavusios privačiam sektoriui, todėl pas jas galima aptikti daugiau PPP apraiškų, o Lietuvoje, viską stengiamasi išlaikyti valstybės "rankose". Iš užsienio šalių galima pasimokyti kūrybiškumo, nebijojimo rizikuoti ir atsakomybes atiduoti privačiam sektoriui	

3 PRIEDAS. Bendriniai klausimai ekspertams

Klausimai	Dalyvis Nr. 1	Dalyvis Nr. 2	Dalyvis Nr. 3	Dalyvis Nr. 4	Dalyvis Nr. 5	Dalyvis Nr. 6	Dalyvis Nr. 7	Dalyvis Nr. 8
Koks organizacijos, kurioje dirbate, tipas (tarptautinė organizacija, vietinis verslas, valstybinė įstaiga (įmonė ir pan.)?	Tarptautinė įmonė	Viešoji įstaiga	Tarptautinė įmonė	Tarptautinė įmonė	Valstybinė įstaiga	Valstybės valdoma įmonė	Tarptautinė įmonė	Tarptautinė įmonė
Koks organizacijos, kurioje dirbate, dydis (0-50, 51-100, 101-400, 401-1000 darbuotojų)?	0-50	0-50	51-100	Daugiau kaip 1000	Daugiau kaip 1000	Daugiau kaip 1000	Daugiau kaip 1000	0-50
Kokias atsakomybes ir pareigas (vaidmenis) užimate įvardintoje organizacijoje?	Įmonės vadovas	Ekspertas kibernetinio saugumo srityje	Skyriaus vadovas, kibernetinio saugumo konsultantas.	Informacijos saugumo analitikas	Vadovas kibernetinio saugumo srityje	Vadovas kibernetinio saugumo srityje	Informacijos saugumo valdymo grupės vadovas	Įmonės vadovas
Kiek ilgai jau dirbate šioje organizacijos pozicijoje?	5 metai	2 metai	8 metai	3 mėn.	2 m.	8 m.	7 mėn.	10 m.
Kokia Jūsų patirtis informacijos ir kibernetinio saugumo srityje?	Vidutinė	Nuo 1990 m.	15 m.	15 m.	Nuo 2009 m.	Nuo 1998 m.	Daugiau kaip 9 m.	-

Klausimai	Dalyvis Nr. 1	Dalyvis Nr. 2	Dalyvis Nr. 3	Dalyvis Nr. 4	Dalyvis Nr. 5	Dalyvis Nr. 6	Dalyvis Nr. 7	Dalyvis Nr. 8
Ar Jūsų organizacija dalyvauja kokiuose nors kibernetinio saugumo viešojo ir privataus sektorių partnerystės projektuose?	Taip	Taip	Dalyvauja kaip Infobalt narė.	Ne	Taip	Taip	Ne	Kol kas ne
Jei atsakėte teigiama į aukščiau esantį klausimą, prašome įvardinkite kokią Jūsų darbo laiko dalį užima darbas pagal įvairius kibernetinio saugumo viešojo ir privataus sektorių partnerystės projektus?	4 val. per mėnesį	Anksčiau tekdavo daug dėmesio skirti panašiems klausimams. Šiuo metu ne.	Apie 5% darbo laiko	-	-	Apie 1-2 val. per mėnesį	-	-

4 PRIEDAS. Papildomi nestruktūruoti klausimai ekspertams

Klausimai	Dalyvis Nr. 1	Dalyvis Nr. 2	Dalyvis Nr. 3	Dalyvis Nr. 7
Ar nepakankamas CSP3 gali prisidėti prie neracionalių kibernetinį saugumą reglamentuojančių teisės aktų ir reikalavimų atsiradimo, kibernetinio saugumo specialistų rengimo potencialo neišnaudojimo, nėra tarpusavio pasitikėjimo stiprinimo įgalintojo, kas galėtų būti kaštų, užtikrinant kibernetinį saugumą, kaip viešojo sektoriaus siekiamybė, privačiame (o gal ir viešame) sektoriuje didėjimas?	Prisidėti gali. Niekas netrukdo ir šiaip bendradarbiauti, be CSP3 apibrėžimo. Dažniausiai kyla klausimas ar yra noro iš abiejų pusių, taip pat susišnekėjimo – supratimo, kad abi pusės sėdi vienoje valtyje ir yra suinteresuotos viena kitos sėkme. Kai tai įsisavinama, tada viskas pradeda eiti sklandžiau, bendros iniciatyvos atsiranda ir tai galima pavadinti PPP. Pirmiausiai PPP nuoširdžiai savaime niekam nėra įdomu. Istoriškai šis terminas bent jau IT galėjo atsirasti, kai valstybės turėjo priversti interneto paslaugų teikėjus kažką daryti dėl kibernetinio saugumo. „Kietai“ priversti sunku, todėl susitarimai pradėti vadinti PPP.	Taip, “private sector” dirba su realybe, praktiniai dalykai, o Vyriausybė neturi daug praktikos ir patirties. Labai padėtų jeigu Vyriausybės iniciatyvos pereitu per ”private sector” filtrą, kuris iš karto suprastu ir pasakytu ar tai nesąmonė ar ne. Irgi reikia atsiminti, kad daugiausia specialistai randasi ne vyriausybes institucijose, o privačiam sektoriui. Būtinas PPP bendradarbiavimas t.y. „Win-Win“ partneryste, tiek viešojo tiek privataus.	CSP3 nebuvimas ar nepakankamas buvimas ne tik kad gali, bet tikrai prisidės prie to ką išvardinai. Jei nebus gero bendradarbiavimo teisės aktai bus rašomi į vienus vartus neatsižvelgiant į privataus sektoriaus specifiką ir poreikius. Nes rašytojai bus iš valstybinio sektoriaus ir jiems bus geriau žinoma valstybinio sektoriaus specifika, o ne privataus. Jei nėra PPP tai ir informacija apie sektorių poreikius nėra apsikeičiama, o tai reiškia, kad ir mokymo programos paruošiamos neatsižvelgiant į realius poreikius, ruošiamų specialistų kiekiai neatitinka poreikių, akademiniam sektoriui nepakankamai įtraukiamas į mokslinė veiklą surišta su Cybersecurity, kuri gali būti naudinga tiek viešajam, tiek privačiam sektoriams ir pan. Na kai nėra bendradarbiavimo, tai vieni į kitus visada žiūri su nepasitikėjimu, taip pat prasideda veiklų dubliavimas, kurio galima būtų išvengti turint bendrus suderintus tikslus. Nebūtina tomis pačiomis	Iš esmės – taip.

Klausimai	Dalyvis Nr. 1	Dalyvis Nr. 2	Dalyvis Nr. 3	Dalyvis Nr. 7
			veiklomis užsiimti tiek privačiame tiek viešajame sektoriuose. Kaip pavyzdys galėtų būti tam tikrų kibernetinio saugumo paslaugų, kurios atitinka keliamus reikalavimus, pirkimas iš privataus sektoriaus, kuris galbūt jau tokias paslaugas teikia. O jei net neteikia gal gali pradėti teikti, o vėliau jas teikti ne tik LT, bet ir kitose šalyse. Žiūrėk ir eksportas padidėja ir rinkos dalyvių kompetencija auga, mokesčių mokėtojų pinigų mažiau sunaudojama, nes nedubliuojama tai ką jau kažkas teikia. Beje valstybei reikia neužmiršti, kad jo tikslas yra ne konkuruoti su privačiu sektoriumi, o teikti tik tas paslaugas, kurios komerciškai yra nepatrauklios, bet jų reikia visuomenei.	

5 PRIEDAS. Ekspertų interviu telefonu nuorašas

Dalyviai Nr. 5-7

Interviu su respondentu Nr. 5 pokalbio išrašas

Juozas Breivė (JB): Tikslas paanalizuoti kiek tų apraiškų valstybėje kibernetinio saugumo srityje pastebime. Turime šiuo metu strategiją, bet gilesnio teisinio reglamentavimo nėra. Europos šalyse CSP3 per paskutinius 2 metus nėra labai populiarus reglamentuojant ir tiksliai apsibrėžiant kas tai yra. Mano žiniomis ir pati sąvoka Lietuvoje kol kas yra derinimo stadijoje tarp įvairių institucijų ir sektorių.

Respondentas Nr. 5 (R5): PPP? Ta prasme, taip. Po tuo pačiu daug kas turi skirtingą supratimą. Reikia turėti omenyje, kad PPP yra projektai kai aiškiai apibrėžiama jog valstybė iškelia uždavinį, verslas įgyvendiną, o valstybė įsipareigoja tas paslaugas nupirkti. Kai kalbame apie CSP3, tai kas akcentuojama netgi Europos komisijoje, tai yra „value chain“. Jei imti ir akademiją – kai valstybės ir verslo finansuojamas prototipo sukūrimas iškarto turima omenyje, kad tai bus kažkada masinėje produkcijoje – sensorius, ugniasienė ir pan. Tai yra normali praktika. Visų pirma reikia kalbėti apie tai CSP3 apimtyje.

JB: bendraujant su keliais kitais šaltiniais ir bandant apibrėžti CSP3, jūsų nuomone ar paprasti komerciniai santykiai, perku-parduodu, patenka į šitą apibrėžimą?

R5: ne. mano manymu, ne.

JB: kalbant apskritai apie PPP, ne CS srityje, būtent ir yra apibrėžiama, kad PPP yra kažkur tarp privatizacijos ir paprastų komercinių santykių. Vieni laikosi nuomonės, kad būtent tie paprasti komerciniai santykiai turėtų patekti į apibrėžimą. Kiti teigia, kad, pvz., ugniasienės nupirkimas iš verslo nėra PPP apimtis.

R5: ne, jei tiesiog perkame iš verslo, tai čia nieko nėra bendro su PPP. Mano manymu, PPP yra tada, kai pirmoje eilėje kalbame apie inovacijų kūrimą, turint omenyje kibernetinio saugumo sritį. Dabar inovacijų kūrimas yra susijęs su rizika. Todėl, kad iš 10 projektų 9 bus nesėkmingi. Tai kalbame apie PPP, tai vat aš matau, kur akademija, verslas ir valstybė pasidalina ta rizika, t.y. valstybė dalį finansuoja, verslas dalį finansuoja, suprasdamas, kad gali nieko iš to neišeiti. Bet pasidalinę riziką jie kartu, taip sakant, ir pasidžiaugs rezultatais. Tai čia, sakyčiau, toks modelis, nes pradžia viso PPP koncepto buvo pastatuose: valstybė neturi pinigų naujam bendrabučiui ir sutaria su verslu, kad jis pastatytų per metus, o valstybė išsimokės per 25 metus. Bet čia vyriausybė dalinai perduoda riziką, nes pastatą valdys tas privatus vienetas ir sprendžia uždavinį, kai nėra finansavimo, o ir taip efektyviai, kaip verslas, valstybė nepastatys to bendrabučio. Kibernetinėje erdvėje, mano manymu, PPP atsiremia pirmoje eilėje į rizikos pasidalinimą. Tai aš čia tokią matau pagrindinę dimensiją ir dėl to reikia žiūrėti ne į trumpalaikę naudą – perku/parduodu – bet į kažkokį ilgalaikį procesą kurį mes norime nueiti.

JB: tai šis požiūris dalinai sutampa su darbe minimu CSP3 apibrėžimu, kai CSP3 yra ilgalaikis susitarimas, bendradarbiavimas ar parama tarp dviejų ar daugiau viešojo ir privataus sektorių dalyvių paremtas pasitikėjimu, informacijos, resursų ir žinių dalybomis, bei atsakomybių ir rizikų pasiskirstymu siekiant kibernetinio atsparumo kaip bendros naudos. Tenka išgirsti iš verslo sektoriaus teiginių, kad PPP reikalingas tik valstybei ir jokie argumentai apie tai, kad visada reikia turėti omenyje bendruomenės gerovę taipogi, irgi yra labai svarbu.

R5: Principe taip. Aš tai irgi taip manyčiau, kad vertės jos įvairialypės gali būti. Atpažinimas, sensoriai, indicators of compromise, kitos geros sistemos paremtos dirbtiniu intelektu jos kainuoja daug, reikalinga daug ir įvairių tyrimų, o po to visi jas naudoja bendrai, tai pats kibernetinis atsparumas yra didesnis negu pavieniai ar skirtingas jas naudoti. Minėtas apibrėžimas yra tinkamas, nes būtent akcentuojama, kad „dalinamasi naudomis“, „dalinamasi rizikomis“ ir „ilgalaikis“.

JB: Tai taip. Šis apibrėžimas nelabai kuom skiriasi nuo nesenai atlikto Europos Sąjungos mastu tyrimo kur irgi tie akcentai yra „privatus“, „viešas sektorius“ (įtraukiant pramonę ir akademinę bendruomenę), švelninti kibernetines grėsmes, tai mes turime „rizika“, „informacijos pasidalinimas“ ir „pasitikėjimas“, na ir „komunikacijos kanalas“. Tik šiame apibrėžime nėra būtent to „ilgalaikiai“, kai čia patenka ir verslo taip norimi paprasti komerciniai santykiai.

R5: Geras dar pavyzdys, tarkime, medicinoje – pasaulyje išplitęs virusas. Verslas, kaip toks, neturi tikslo suvaldyti epidemiją: gerai būtų, bet tik tiek, kad patys nesirgtų. Iš valstybės perspektyvos – ji nori suvaldyti, bet neturi resursų kaip. Ir čia atsiranda PPP, kai sakai, va, žiūrėkit, verslas sukurkite, o mes iš jūsų nupirksime siekdami bendro gėrio – suvaldyti grėsmę. Čia irgi momentas, kai verslas neturi tikslo apsaugoti Lietuvą.

JB: tai ar mes pasąmoningai neprieiname prie išvados, kad PPP yra nauda valstybei? Viešajam sektoriui labiau?

R5: Ne. Yra abi naudos. Ta prasme, jei yra sukuriamas produktas iš verslo, tai jis bus nupirktas, t.y. verslas gaus pinigus, o valstybė efektyviau suvaldys grėsmę ir pasieks savo tikslų. Čia labai svarbu iš kokio „kampo“ žiūrėsi: jeigu iš verslo, tai taip, galutinis tikslas valstybei pasiekti savo naudą – valstybė laimi. Bet jei žiuri ar mano įmonei kažkas yra iš to, tai taip – uždirbai pinigų, kai tikslas didinti pinigų uždirbimą.

JB: bet aš įsivaizduoju, kad tas PPP ar CSP3 turės būti teisiškai apibrėžtas? Jei jau sakome, kad mes strategijoje įsivardiname kaip vieną iš uždavinių, bet neturime dar reglamentavimo.

R5: Tai vienas iš nurodytų uždavinių ir yra sukurti bendradarbiavimo modelį.

JB: Įsivaizduokime, kad diskusijos šiuo klausimu greičiausiai bus nemažos tarp sektorių. Bet pažiūrėkime iš šono: turime strategiją su uždaviniais, neturime CSP3 teisinio reglamentavimo, bet ar tos apraiškos dabar yra šiuo metu yra pastebimos jau Lietuvoje?

R5: Nu, aš taip grynąja prasme tai negalėčiau taip atsakyti. Pirmas kurį galėčiau paminėti yra nuolatinio struktūrizuoto bendradarbiavimo (PESCO) gynybos srityje Europos Sąjungoje projektas kur kelios šalys susitaria kažką daryti daugiau negu visos kitos. Ir ten yra vienas projektas Lietuvos patvirtintas, t.y. Cyber Rapid Responce Teams, kuriame sakoma, kad iš keliu šalių žmonės po vieną, po du, po tris kartu susirenka ir sprendžia kaip jie galės veikti. Jiems reikia kažkokio bendro „set of tools“, kad jie iš kelių šalių, bet dirbtų su tais pačiais įrankiais. Tai šis projektas jau prasidėjęs ir porą strateginių planavimo sesijų su verslu jau įvyko sprendžiant įrankių parinkimo klausimus – kas tai galėtų būti? Ir radus ES finansavimą, tai pradžioje bus padarytas prototipas, po to seks vystymas ir išvysčius ir valstybė bus įsipareigojusi nupirkti kažkiek tai. Verslas realiai dalyvauja, jis kuria tuos produktus ir valstybė jų kažkiek nupirks. Čia va toks, kaip tas ir veikia. Bet valstybė nesako, kad pirkimas bus „off the shelf“, nes mes turime poreikių, kuriuos jūs (verslas) turėtumėte realizuoti. Dabar projektus siūlys ir privačios, ir akademija, ne tik verslas.

JB: iš kitų apraiškų, ką asmeniškai aš pastebiu, mes dar esame nuėję tokiu Vokietijos UP KRITIS keliu savotiškai – informacijos dalinimasis su kritine infrastruktūra, kuriant tą pasitikėjimą. Ar tai nėra viena irgi iš apraiškų?

R5: nu galbūt, bet čia sunku kalbėti „ar tai yra“, kai nežinome „kas tai yra“.

JB: na, be abejo, tai mes kalbame bandydami numanyti kas tai galėtų būti.

R5: bet tokie modeliai, aš manau, vis tiek, atsiremiame į tą modelį, kad, pavyzdžiui, šiuo atveju, PESCO – realiai yra du atvejai. Vienas nėra PPP, kai valstybės nusipirks tuos pačius įrankius (t.y. komercinius produktus), tai čia ne PPP, mano manymu. Kitas būdas: valstybės apsispręs kokio set‘o (angl. konfigūracija - aut. past.) jos nori ir tada verslas pagamins tokį set‘ą, padarys mokymus, sukonstruos ir tos valstybės nusipirks. Tai čia, mano manymu, jau PPP, t.y. valstybė negali to pati pasidaryti ir sako – man reikia verslo. Bet verslas nedaro šiaip sau ką nori, bet daro tai valstybei. Tai va, čia toks, žinai, pamąstymas tiesiog.

JB: o va, tarkim, iš užsienio šalių, gal teko susidurti kokios tos gerosios PPP praktikos dar galėtų būti įgyvendintos Lietuvoje? „Galėtų būti: mes vėl kalbame apie tai neturėdami konkretaus patvirtinto apibrėžimo.

R5: na, Prancūzijoje yra kuriamas klasteris, kur labai matosi. Na, bet jie dideli, turi daug pinigų. Jie įsteigė kelių universitetų sąjungą pavadindami jį klasteriu ir nusprendė ruošti kibernetinio saugumo specialistus kompanijoms, viešajam sektoriui. Valstybė tuo pasakė, kad jūs dabar (verslas – aut. past.) investuokite į tą regioną, kad čia bus mokslininkai ir mūsų kibernetinio saugumo pajėgos irgi bus čia.

JB: bet ar čia nėra gera idėja ne tik gaivinti regionus su visa švietimo infrastruktūra, bet ir papildyti trūkstamų kibernetinio saugumo specialistų būrį? Dabar esu suskaičiavęs, kad per visą Lietuvą yra tik 4 studijų programos siejamos su informacijos ir kibernetiniu saugumu. Bet užpildyti susidariusį vakuumą reikia įvairios specializacijos kibernetinio saugumo specialistų: technikų, auditorių, vadybininkų ir t.t.?

R5: Bretanėje tas klasteris yra – France cybersecurity cluster. Strategija, tai kur link valstybė nori eiti. Čia kilo daug diskusijų viešoje erdvėje – valstybė sau, verslas sau. Mes per maži, kad galėtume sau tai leisti. Iš kitos pusės, verslas daugiau koncentruotas į pardavimus tiktai. R&D (angl. research and development – aut. past.) išvis neužsiima (verslas – aut. past.). Ir čia dabar yra problema, nes PPP be R&D nebūna. Čia irgi labai svarbus momentas. Pas mus verslas kibernetiniame saugume įsivaizduoja, kad gali būti toks, kur jie neinvestuoja į R&D.

JB: tai čia ką aš girdžiu diskusijose viešoje erdvėje, kad mums (verslui – aut. past.) reikia, kad PPP nebūtų žodžio „ilgalaikiai“, nes mums po PPP reikia „pakišti“ perku-parduodu.

R5: Ne, tai čia, vienareikšmiškai, kur mes sutinkame, kad labai svarbu valstybei perku-parduodu santykis, nes mes turime galėti nusipirkti tai ko mums reikia, bet PPP nėra apie tai. PPP yra apie tai, kad yra ilgalaikis santykis ir jis būtinai turi R&D dalį.

JB: taip pat ką aš pastebiu, kad po viešuoju sektoriumi dažniausiai taip pat yra „pakišama“ akademija atskirai neišskiriant. Nors, pavyzdžiui, nepakankamas CSP3 iš dalies didina neracionalių kibernetinį saugumą reglamentuojančių teisės aktų atsiradimą, nes nėra to ekspertinio bendradarbiavimo, arba, tarkime, nėra išnaudojamas kibernetinio saugumo specialistų rengimo potencialas – turime tik 4 aiškiai išreikštas studijų programas, o gal mūsų šaliai to pakanka?

R5: nu tai va, čia labai svarbus rišasi kitas dalykas dėl rengimo pačio, nors gal ne taip visai su PPP, bet vienas iš strategijos tikslų, kur mes bandysime atsakyti – padaryti kompetencijų aprašą. Nes kas yra kibernetikos specialistas, tai žinai, jei tai yra kibernetinės saugos auditorius dar galima jį išskirti, bet šiaip tai yra IT specialistas su pakraipa į kibernetinį saugumą: laužimą, hakinimą ir pan. Tai kiek jų reikia? Kaip sako, reikia kibernetinių specialistų 10 tūkstančių. Netgi tada aš sakau, kokių 10 tūkstančių? Adminų (IT administratorių – aut. past.), programuotojų? Tūkstančio adminų ir devynių tūkstančių programuotojų? Ko konkrečiai reikia? Ir tada diskusijose išaiškėja, kad reikia kibernetinio saugumo auditorių, reikia „white hat“ (angl. baltųjų kepurių hakeriai – aut. past.), reikia kažkiek pentesterių (įsilaužimo specialistų – aut. past.). Ką aš dažnai girdžiu iš verslo, kad ateina iš universiteto ir mes juos permokinti turime – nieko jie nemoka. Sutinku su tokiu požiūriu, bet greičiausiai dar darbe reikia mokytis ir tada aš klausiu, o kokios kompetencijos specialistų jums reikia? Nes kai man pavyzdžiu pastato kibernetinio saugumo specialistą baigusį vadybą ir klausia ar jis gali kažką nulaužti, bet aš klausiu nulaužti ką? Įsilaužti į sistemą? Tuomet aš sakau nedirbu tokio darbo, kad jūs greičiausiai mane su kažkuo painiojate. Aš esu vadovas. Mano kompetencijų didžioji dalis yra vadovavimas žmonėms, bet ar dabar mums reikia laužtis į kažką? Na, ne. Suprasti kaip tai daroma – taip. Tada kas mes tokie? Kas yra saugos specialistas? Kas yra CIO, kas yra CISO? Čia manau svarbu nusipiešti kompetencijų žemėlapį. Tada geriau galėsime pasakyti ko mums reikia ir čia atsiranda PPP, kai valstybė sako „mums neaišku, ką mes turėtume finansuoti?“, tada akademija rengia tą kompetencijų žemėlapį „ko reikia“, kur verslas sako taip ar ne. Ir galutinis produktas gaunasi geras. Valstybė žino ką finansuoja, akademija žino ką rengia, verslas žino ką gauna. Va čia yra ilgalaikė PPP strategija. Pasirengti pakankamą kiekį specialistų.

JB: aš sakyčiau, kad tai papildomai apima ir kitų IT specialistų rengime integruoti kibernetinio saugumo pagrindus, tarkime, kaip saugiai programuoti, kaip saugiai valdyti sistemas ir pan. Ačiū labai už mintis iš išvadas.

Interviu su respondentu Nr. 6 pokalbio išrašas

Juozas Breivė (JB): Aš rašau MBD tema PPP užtikrinant kibernetinį saugumą Lietuvoje. Tokio CSP3 reglamentavimo Lietuvoje nėra. Turime tik strategiją, kur vienas iš uždavinių yra plėtoti bendradarbiavimą, bet niekas neįsivaizduoja kaip tai daryti. Dabar svarbi yra patirtis ekspertinė siekiant išsiaiškinti galimas apraiškas Lietuvoje jau dabar. Pabandyti sužinoti ar nepakankamas PPP įtakoja neracionalų teisinį reglamentavimą kibernetinio saugumo srityje, ar įtakoja ruošiamų kibernetinio saugumo specialistų trūkumą ir pan. Kalbant apie CSP3 kaip apibrėžimą norėtųsi kalbėti kaip apie ilgalaikį susitarimą tarp dviejų ar daugiau sektorių dalyvių, nes dažniausiai iš verslo viešoje erdvėje yra girdima, kad į CSP3 turi papulti ir elementarūs komerciniai santykiai, kur

ta abipusė nauda nėra pilnavertė iš PPP perspektyvos, nėra rizikų pasidalinimo. Labai svarbi asmeninė nuomonė siekiant išsiaiškinti, kad ir neturint reglamentuoto CSP3, kokios apraiškos pastebimos jau dabar Lietuvoje, kai sakome, jog CSP3 yra rizikų pasidalinimas, resursų pasidalinimas, pasitikėjimas, bendra nauda, žinių „know-how“ dalybos, na ir be abejo, ilgalaikėje perspektyvoje.

Respondentas Nr. 6 (R6): iš savo patirties galiu tik nuliūdinti, nes noras atrasti tą gražią partnerystę kol kas nerealus, nes jos tiesiog šiuo metu pas mus nėra. Deja, bet pirminis dažniausiai siekis yra perku-parduodu.

J: bet gal pastebite kryptingos veiklos, kaip pvz. Vokietijos kritinės infrastruktūros CSP3 projektas UP KRITIS ir pan.? Jungtinė Karalystė ima CSP3 plačiau pritraukdama ir visuomenę.

R6: man kyla dar klausimų pačiam dėl savo organizacijos traktavimo šioje plotmėje, kai esame komercinė organizacija, tačiau valstybės valdoma, bet įnašą vieną ar kita strategijos kūrime padarėme. Taip pat pasisiūlėme pasidalinti rizikų vertinimo metodikos „know-how“. Ir šitoje vietoje yra toks dalykas, kad tokia veikla mes nedarome sau pelno, t.y. akivaizdžios naudos negauname. Bet čia gal supratimas toks ateina, kad augame visi ir visiems nuo to geriau. Ta iniciatyva palaikoma iš mūsų pusės kol kas. Sutikime, kad neprivalėjome ten nieko daryti.

J: bet tai gal ir yra CSP3 apraiška apimanti žinių dalybas? Valstybė žinių neturi, jūs turit, kompetencijų taipogi. Galit kažką pasidalinti ir parodyti.

R6: nu aš manau.

J: Bet čia gal nėra apibrėžtas toks koordinatorius, kas yra labai svarbu? Jei kalbant apie PPP, yra požiūrio, kad pati partnerystė kaip tokia verslui nėra reikalinga ir čia tik viešojo sektoriaus interesas.

R6: žinok, tame gali būti labai daug tiesos. Nes jei kalbame apie konsultacijas kibernetinio saugumo srityje viešajam sektoriui, tai visos konsultacijos yra iki tokio lygio, kad būtų parduotas produktas ir viskas. Aš suprantu ir verslą, nes visko jie atskleisti negali, nes tai reiškia jiems pajamų praradimą. Nes tokios partnerystės kai yra nemokama, neįvardinčiau, kad esame gavę.

J: ar verslas būtų pajėgus atsilaikyti ATP atakoms, kurios valstybinio masto, žaidžia dideli pinigai ir žvalgybinė informacija – tiksli, laiku ir vietoje. Ar šioje situacijoje būtų atsilaikyta?

R6: bet šioje vietoje dabar yra partnerystė – padeda NKSC, kaip viešasis sektorius. Reiškia mes kažką jau gauname.

J: tai jau galime sakyti, kad turime vieną apraišką?

R6: ta prasme iš viešo sektoriaus į privatų – na, taip. Bendradarbiavimas vyksta pakankamai aktyviai. Nebijome pasidalinti incidentų esminiais indikatoriais ir pan.

J: šiuo atveju galime įžvelgti bendrą tikslą – švelninti rizikas tobulinant gynybinius pajėgumus.

R6: na, ir mes pradedame dalintis tai indikatoriais, tik mechanizmas iki galo neveikia, bet jau informacijos dalinimasis yra. Phishing‘o (kenkėjiški laiškai – aut. past.) atakos metu, tarkime, neprivalome pranešti, nes pagal incidentu metodiką incidentas nėra kritinis, tačiau pranešėme, nes pasidalinti yra noras. Kaip suprantu dar nelabai veikia IOC (angl. indicators of compromise – aut. past.) dalinimosi platforma pilnavertiškai. Bet noras yra, kad išeitų plačiau ta informacija. Taip pat matau bendradarbiavimo tarp to paties sektorių dalyvių kibernetinio saugumo srityje, kai susitikus bendrai aptariamos problemos ir bandoma ieškoti būtų kuom gali vienas kitam padėti – ką žinom, ką mokam, kuom norėtume pasidalinti principu. Bet čia gal mūsų pozicija leidžia tai daryti, nes būnant kibernetinio saugumo kompanija vargiai ar galėtume tokiomis žiniomis dalintis.

J: bet ar čia nesigauna toks savo sąžinės užklausimas, kai verslas, kuris sukurtas gauti pelną, bet būdamas Lietuvos, kaip valstybės, dalis, kalbant apie valstybinio atsparumo kibernetinėms grėsmės kūrimą, apsisprendžia į rinką tiekti nesaugius kibernetinio saugumo produktus?

R6: nu, ne.

J: tai kažkokia socialinė ir ekonominė CSP3 vertė vis vien turi kažkokia būti, tuo labiau abipusė.

R6: bet gal šitoj vietoj neturėčiau atsakymo, nes CSP3 atveju toks produktas atsidūręs organizacijoje tiesiog būtų keičiamas tos organizacijos sąskaita., nes tokios iniciatyvos, kad mes kaip organizacija, tarkime, suprantame nacionalinius interesus ir pakeisime, tikrai nebūtų. Taigi, kol kas iš kibernetinės saugos produktus siūlančių kompanijų visas CSP3 yra tik piniginiai santykiai: produkto pardavimo galimybė, diskusija, reklama ir viskas. Tuo ir pasibaigia žinių pasidalinimas ir partnerystė. Tokia asmeninė patirtis.

J: čia prieiname prie paprasto dalyko, kad kol nėra teisinio apibrėžimo dėl atsakomybių ir rizikų paskirstymo, praktiškai...

R6: na, kitas dalykas, pavyzdžiui, interneto svetainių turėjimas, kai dalis laikoma savoje infrastruktūroje, o dalis ne ir, tarkime, paprašius gamintojų „užlopyti“ pažeidžiamumus galima sulaukti atsakymo, kad pagal kontraktą tai nepriklauso ir tai bus jų tiesa. O jau kitą kartą užsakant programavimo paslaugas bus į tai atsižvelgta ir sutartys papildytos reikalavimais dėl reakcijos laiko ir atsakomybių. Tai taip ir su CSP3 branda manyčiau. Visada bus sektoriaus dalyvių, kurie supras ir dalinsis bendra nauda, o bus tokių, kurie skaitys „įstatymo raidę“ ir viskas.

J: ar, na, pavyzdžiui, kas būtų jei viešasis sektorius bendradarbiavimo aspektu teiktų nemokamus kibernetinio saugumo kompanijų teikiamų paslaugų analogus?

R6: jie galėtų, bet dabar galvoju, kad čia būtų diskusija dėl abipusio nesutarimo tarp sektorių, kai iškyla interesų konfliktas tiesiogine to žodžio prasme iš verslo „atimant“ pinigus, nors nauda valstybei stiprinant atsparumą be abejo būtų. Taip pat kyla iškart klausimas, kokios kokybės tos paslaugos būtų teikiamos? Dažniausiai perku-parduodu santykiai remiasi noru turėti rinką, joje veikti, iš to uždirbti, o tai, kad padaryti tvarkingai su palaikymu visu ir reguliariu pažeidžiamumų tvarkymu čia nelabai daug kas lieka.

J: grįžtant prie tyrimo klausimų: kaip suprantu apraiškų Lietuvoje nelabai pastebima, ar teisingai suprantu?

R6: na, yra, žinok, NKSC veikla ganėtinai aktyvi. Sakyčiau, kad yra tų apraiškų. Taip pat ir taryba (kibernetinio saugumo taryba – aut. past.) koordinacijai. Nors Lietuvos kariuomenėje yra padalinys, kaip rezervas, kuris gali pretenduoti į vieną stipriausių CSP3 apraiškų Lietuvoje, kur vyrai iš įvairių sektorių surenkami bendram tikslui. Jie pirmiausiai yra sukonstruoti dėl pagalbos kariuomenei siekiant atremti ir būti gynybos linijoje metus darbą įmonėje X šoktų gelbėti kažkokias svarbias Lietuvai sistemas. Ten va yra ta tikroji vieta kur žmonės bičiuliaujasi ir keičiasi „know-how“ be tikslo „kalti pinigus“.

J: o kaip dėl viešojo sektoriaus akademinė bendruomenė? Lietuvoje turime tik 3 studijų programas. Vieną bakalauro ir dvi magistro. Ar tos akademinės kibernetinio saugumo specialistų ruošimo apraiškos yra efektyvios?

R6: neįvardinčiau. Nes dabar tokios aiškios krypties nelabai yra.

J: o kaip su kibernetinio saugumo specialistų rengimo kryptimis?

R6: taip, tas svarbu, kadangi vyrauja, bent iš mano patirties, dvi kompetencijų grupės – vadybininkai ir CIRT specialistai. Dažniausiai tos kompetencijos ugdomos organizacijos viduje. Nors ir pasiimama iš išorės kažką patyrusio, bet viskas kitkas – adaptacija ir auginimasis vyksta viduje. „Iš parduotuvės“, kad taip pasižiūrėjau ir nupirkau dar nebuvo.

J: kokia ekonominė ir socialinė CSP3 įgyvendinimo nauda galėtų būti tenkinant specialistų poreikį?

R6: hm, aš manau, kad mums kaip darbdaviams būtų labai gera. Padidėtų pasirinkimas, jei kalbame apie specialistų poreikį, bei sumažėtų kaina, nes dabar visi „nosytes“ užrietę vaikšto.

J: ar mano keliama hipotezė, kad nepakankamas CSP3 sąlygoja kibernetinio saugumo specialistų rengimo potencialo neišnaudojimą po šios diskusijos yra teisinga?

R6: sutinku.

J: bet ar nesigauna taip, kad tų keturių studijų programų mums nepakanka, nes jos bendrinės ir neturi aiškios specializacijos kibernetinio saugumo terminais?

R6: nu, taip, bet čia gal mums paprastai atrodo, kad paleidau programą ir čia atsirado po 4 metų „injekcija“ į rinką. Bet ar yra norinčių sudalyvauti? Tuo labiau dalyvauti CIRT veikloje reikia labai praktinės patirties, teorijos vien neužtenka. Tas dalykas neateina per kelis metus „kalant“ vieną ar kitą kursą.

J: ar atskirų sektorių įsitraukimas yra pakankamas šiuo metu, nors ir neturint aiškaus kol kas reglamentavimo?

R6: tai matai, gal pas mus gimsta kol kas tas viskas dalykas. NKSC šiuo atveju siekia, kviečia visus įsitraukti. Verslą irgi įtraukinėja kažkiek. Mes kažkiek patys dalinamės priemonių planais ir t.t. Asociacija Infobalt irgi kiek ji ten įsitraukusi yra dėdama pastangas ir pan. Koks ten matymas yra kibernetinio saugumo paslaugas siūlančių organizacijų. Tai bendrai iniciatyva yra. Ji gimsta. Gimsta reglamentavimo „raidė“. Apčiuopiamo rezultato aš kol kas nesu matęs. Bet, kad įpareigoti kažką bendradarbiauti tai kol kas ne. Nes kol kas verslas nėra suinteresuotas sudalyvauti CSP3. Aš partnerystę šiek tiek kitaip suprantu, nei suinteresuotumas dalyvauti komerciniuose santykiuose, kai kalbama apie problemas, pagalbą, kitus dalykus, o ne tik apie pinigus.

J: o R&D veikla? Kurioje vietoje CSP3 ji yra čia?

R6: vienas iš pavyzdžių galėtų būti populiarūs „hakatonai“, kai dirbama ant to paties pagrindo ieškant ir analizuojant problemas. Jei kažkas norės šioje vietoje reklamos – prašome. Jei kažkam pavyks – įdomu kaip atradot, ką pamatėt ir t.t. Čia motyvacija per kažkokią reputacijos ar smagaus laiko prizmę, o ne per pinigus. Iš vienos pusės verslui turėtų būti naudinga dalyvauti ir dalintis „know-how“. Tai darant auga kompetencijos, galbūt prarandama rinkos dalis, tačiau svarbu suprasti, kad visa rinka niekada nepasidarys tokia ir niekas tiek daug neinvestuos. O užsiauginus savo raumenis automatiškai atsiranda R&D veikla. Pasidarius pagrindus.

J: kiek laiko jau kibernetinio saugumo srityje dirbate?

R6: 8 metai oficialiai esamoje pozicijoje, o apskritai nuo 1998 m.

J: kiek tenka dalyvauti CSP3 projektuose?

R6: einame „naglai“ gerąja to žodžio prasme – iniciatyviai.

J: kiek laiko užima dalyvavimas CSP3 veikloje?

R6: nedaug. Valanda, dvi bendrai.

Interviu su respondentu Nr. 7 pokalbio išrašas

Juozas Breivė (JB): Šiuo metu ruošiu magistro baigiamąjį darbą tema „Viešojo ir privataus sektorių bendradarbiavimas užtikrinant kibernetinį saugumą Lietuvoje. Uždavinys yra išsiaiškinti kiek CSP3 šiuo metu, neturint teisinio PPP apibrėžimo, atsakomybių toje srityje reglamentavimo ir pan., pastebimas Lietuvoje. Kiek tų apraiškų pastebi viešasis sektorius ar verslas?

Respondentas Nr. 7 (R7): Jeigu, ten tarkime, pasiėmus nuo aukščiau ten tą, tai kibernetinio saugumo įstatyme bent jau buvo kalbama apie viešo ir privataus sektorių partnerystę, bet ten daugiau neišplėtota. Bet jeigu, kitas yra tas viešos ir privačios partnerystės, toks kaip ir įstatymas, šiek tiek, bet tenai jisai tik tiek kaip Lietuva supranta tą PPP. Pakankamai sudėtingos procedūros, tenai pagal viešuosius pirkimus ir t.t., kai, pavyzdžiui privatus kapitalas pastato tiltą ir valstybė už tą tiltą 20 metų moka. Tuo metu PPP kibernetinio saugumo srityje remiantis mano patirtimi buvo suprantamas išviso kaip bendradarbiavimas, ta prasme, nesiekiant deleguoti tam tikrą valstybės

funkciją, kaipo tokią, pagal PPP lietuvišką apibrėžimą, bet, tarkim, bendradarbiauti vykdant vieną ar kitą veiklą. Tai jei kalbėti apie tai, tai iš to bendradarbiavimo kaip ir buvo įsteigta ta kibernetinio saugumo taryba, kurioje yra įtraukta ir privataus sektorių atstovų, kad juos išgirsti ir įtraukti į tą visą partnerystės procesą. Tai ten buvo keliamos tokios idėjos iš esmės dėl, tarkim, dalyvavimo kibernetinio saugumo pratybose ne tik nacionaliniu, bet ir tarptautiniu mastu kartu priimant ir privatų sektorių. Kitas klausimas, kaip pavyzdys, buvo dėl kompetencijų iš privataus sektorių pasitelkimo pagal poreikį eliminuojant trūkumą valstybiniame sektoriuje ir t.t. ar tai per žinių prizmę. Tačiau kažkokio didesnio apčiuopiamo projekto kol kas lyg ir nebuvo Lietuvoje.

JB: o jeigu pažvelgti iš tos perspektyvos kai CSP3 suvedant į tokį apibrėžimą, kai tai yra ilgalaikiai santykiai, bendradarbiavimas ar tai parama kažkokia kur dalinamasi rizikomis, informacija ir atsiranda pasitikėjimas bei bendra nauda.

R7: Jo, tai jeigu tada pagal šį apibrėžimą iš esmės Lietuvoje tada dar nieko nėra.

JB: na, o tarkime, NKSC veikla?

R7: NKSC veikla yra visiškai valstybinė, ta prasme, ir nieko bendro ten nėra bendradarbiaujant su privačiu.

JB: juk, teoriškai, kritinė infrastruktūra yra dažniausiai privataus sektoriaus rankose.

R7: matai, iš kurios pusės pažiūrėsi...

JB: pažiūrėkime iš dalinimosi IOC (angl. indicators of compromize), žinių ar informacijos dalybų ir pan.

R7: bet matai, šitoje vietoje ta kritinės infrastruktūros apsauga, ką daro, tarkime, NKSC, yra vien tam, kad užtikrinti valstybės saugumą iš nacionalinio saugumo pusės. Čia yra ta pusė.

JB: tai ką Jūs sakote yra nauda viešajam sektoriui labiau negu kritinei infrastruktūrai?

R7: ne. Aš labiau sakau tai, kad čia šitoje vietoje valstybė, suprasdama tam tikro verslo ar tam tikros įmonės kritiškumą įsipareigoja jį šiek tiek saugoti arba prisidėti prie jo saugumo užtikrinimo, bet tuo pačiu, iš kitos pusės, jam yra nustatyti aukštesni reikalavimai, tai čia nežinau ar iš esmės galima pavadinti PPP. Dėl bendradarbiavimo, galbūt, ten siekiant bendro tikslo kaip nacionalinio saugumo gal, kažkaip, ten ir pritempti gali.

JB: bet žiūrėkime – NKSC metinės pratybos: dalyvauja akademinė bendruomenė suteikdama infrastruktūrą ir žinias, kritinė infrastruktūrą kaip privataus sektoriaus atstovai (dalis) su savo kompetencijomis, na ir NKSC lieka kaip toks koordinuojantis.

R7: va šitas iš esmės yra vienas man ir yra toks kaip PPP pavyzdys. Tai NKSC šiuo atveju pritraukdama visus šiuos dalyvius mato galimybę kompetencijų spragoms šalinti. Bet jis yra, ta prasme, reguliarus, kasmetinis, kur galima įvardinti „ilgalaikis“. Bet iš esmės jisai neturi termino pabaigos. O gal kitais metais privataus sektoriaus nebebus? Bet gali būti, kad ir bus.

JB: kalbant apie patį termino „ilgalaikis“ naudojimą CSP3 apibrėžime Jūsų akimis ar laiku ir vietoje? Nes nubraukus šį terminą į CSP3 santykius iš klasikinio PPP atkeliauja ir perku/parduodu elementarūs komerciniai santykiai.

R7: taip, taip, bet aš žiūrėčiau iš tos pusės, kad CSP3 neturi to materialiojo viešojo sektoriaus pirkimo iš privataus sektoriaus, kad pasiekti tam kažkokį tikslą, o, tiesiog, privatus sektorius investuoja, na ta prasme, savomis investicijomis stiprina tą partnerystę.

JB: na, o atvirkščiai gali būti? Tarkime, viešasis sektorius investuoja per akademinę bendruomenę ruošdamas kibernetinio saugumo specialistus verslui.

R7: tas irgi yra taip. Dėl šito taip. Tik, va, sakau šitoje vietoje dar yra kitas PPP reikalas kai bendradarbiavimas vyksta ir tarp valstybiniu mastu, kaip pavyzdžiui renginiai dalinantis patirtimi kritinės infrastruktūros (o vėliau ir

privataus sektoriaus) apsaugos srityje. JAV ir Baltijos šalys. Konkretus žinių pasisėmimas iš partnerių, kaip valstybių. Jis irgi gali būti ilgalaikis kai valstybė savo iniciatyva pritraukia privatų sektorių tam, kad pakelti jų kompetenciją ir sąmoningumą.

JB: tos sąvokos „ilgalaikis“ įtraukimas juk eliminuoja ir tokį dalyką kaip, pavyzdžiui, verslas sukuria kažkokį kibernetinio saugumo modelį ir jį parduoda viešajam sektoriui, kurį jis naudos ne vienerius metus. Nors tai ir yra perku/parduodu santykiai, bet lyg ir pasąmonėje kažkur kirba mintis, kad tai ilgalaikėje perspektyvoje naudojamas rezultatas bus. Taip pat ilgalaikiai santykiai perku/parduodu galėtų atsirasti turint įsipareigojimų kontraktą kažkurį laiką taisyti programines klaidas ar pan.

R7: bet čia produkto aprašymo esmė. Kiek gyvuoja produktas, tiek duodama garantija. Realiai į tą vietą reikėtų dar žvelgti ir kitų sąvokų paminėtų apimtyje – rizikų pasidalinimas, naudų kažkokių pasidalinimas. Tą perku/parduodu, iš esmės, gali pasakyti apie trukmę, nes pagal viešųjų pirkimų įstatymą, man atrodo, ilgiau kaip 36 mėn. kontraktas tęstis negali, paskui turi būti vėl pirkimas. Tai čia tas galėtų būti apibūdinimas kas tai yra „ilgalaikiai“ – ilgiau nei 36 mėn. Nes vadovaujantis viešųjų pirkimų įstatymu labai sunku kalbėti apie PPP Lietuvoje įgyvendinimą įtraukiant ir komercinius santykius, taip pat turi skelbti konkursą, tam, kad susirastum partnerį, turi atsirinkti paskui tą partnerį, tada, berods, skelbti pirkimą, tada ta įmonė kažką padaro ir tuo metu valstybė, galbūt, moka jai proporcijomis. Tokie reglamentavimai apsunkina CSP3 atsiradimą Lietuvoje, kaipo tokį. Kibernetinė erdvė yra labai greitai kintantis fenomenas ir užtikrinti savalaikį prisitaikymą prie pokyčių vadovaujantis esamu teisiniu reglamentavimu yra sudėtinga. Čia galima netgi atskirą mokslinį darbą inicijuoti apie pačios CSP3 sąvokos supratimą pasauliniu mastu ir tai kur link dabar viskas eina Lietuvoje su dabartiniu teisiniu reglamentavimu.

JB: mano atliekamame darbe keliama kaip tik analogiška hipotezė, kad nepakankamas CSP3 įgyvendinimas sąlygoja neracionalių įstatymų ar teisinių reikalavimų atsiradimą, nepakankamą aukštojo mokslo išnaudojimą siekiant užpildyti kibernetinio saugumo profesionalų trūkumą, nėra tarpusavio pasitikėjimo stiprinimo ir tai visumoje įtakoja investuojamų kaštų į kibernetinį saugumą privačiame sektoriuje didėjimą ir neišnaudojamos visos įmanomos priemonės kibernetinio atsparumo didinimui netgi valstybės mastu.

R7: iš esmės – taip. Kuom dar galime papildyti, tai PESCO projektas dėl greitojo reagavimo CIRT pajėgų, kai valstybė kviečia kurti įrankius, paskui finansuoja dalinai privatų sektorių, kuris kažką kuria ir paskui valstybė tai nuperka. Tai vėl tas perku/parduodu santykis atsiranda, tačiau čia aš pastebiu trūkumą to įsiklausimo ko iš tiesų reikia privačiam sektoriui, ne tik viešajam sektoriui paskelbiant kryptį ar temas ir pritraukiant mokslinį sektorių.

JB: ar čia mes jau kalbame apie tai, kad CSP3 turi būtinai apimti ir R&D veiklą?

R7: iš esmės – taip. Tam, kad verslas irgi turėtų naudą turi iš tos pusės atsirasti ir jam kažkokia pridėtinė vertė. Verslui pridėtinė vertė atsiranda arba per žmones, arba per tam tikrų produktų atsiradimą iš kurio jie gali vėliau pardavinėdami užsidirbti.

JB: tarkime nesenai atlikto ES mastu tyrimo atskaitoje CSP3 apibrėžime nekalbama apie ilgalaikį santykį, tačiau pabrėžiamas bendras tikslas – kibernetinio saugumo pajėgumų didinimas ir rizikų švelninimas. Tai šiuo atveju tas PESCO projektas patenka po CSP3, nes tai yra gynybinių pajėgumų stiprinimas.

R7: tada po šita sąvoka iš esmės patenka. Tačiau po dabartine situacija Lietuvoje ir kalbant apie PPP apraišką, tai bus eilinis konkursas sukurti kažkokius įrankius, kuriuos po to valstybė nupirks naudojimui.

JB: bet pradinėje projekto stadijoje juk yra verslas ir akademinė bendruomenė kviečiami bendradarbiauti kuriant įrankius, bet verslo segmente šiuo mastu yra ne tik įrankių kūrėjai, bet ir kompetencijų turėtojai, tarkime infrastruktūrų valdytojai.

R7: bet šitoje vietoje, KAM (aut. past. Krašto apsaugos ministerija) įvardino įrankius ir temas kuriomis remiantis turi būti plėtojama. Tačiau niekas nepaklausė verslo ko jiems reikėtų jei būtų sukurta tam, kad pagerinti tą kibernetinį saugumą. Aš sakyčiau šitoje vietoje nėra to tikro bendradarbiavimo. Bent jau aš taip suvokiu. Visa tai liko dalinai nuošaly.

JB: tai Jūs sakote, kad Lietuvoje sektorių įsitraukimas į PPP veiklą nėra pakankamas?

R7: taip. Ką aš pastebiu kol kas, kad daugumoje atvejų viešasis sektorius laiko pakankamą atstumą nuo privataus sektoriaus bendradarbiavimo srityje. Kai viešajam sektoriui kažko reikia – jis paklausia verslo, kai kažko reikia verslui – nėra aišku ar bus koks grįžtamasis ryšys. Be abejo kalbant apie kritinę infrastruktūrą, tai tas bendradarbiavimas matosi, kad yra geras ir toliau sėkmingai plėtojamas. Bet gal tas atstumo ribos nubrėžimas sąlygotas įvairių viešųjų ir privačių interesų baimės sukurto pasipriešinimo.

JB: bet jei kalbame apie gamintoją, tai jo įtraukimas turi kitą neigiamą pusę iš verslo – nesant perku/parduodu, o tik partneryste grįstuose santykiuose gamintojas praranda kompetenciją ar rinką. Juk perėmus tam tikras verslo siūlomas paslaugas viešajam sektoriui ir teikti jas savo segmento dalims bus iškraipoma rinka. Truputi peršokant toliau: kas Jūsų manymu turėtų koordinuoti CSP3 veiklą?

R7: kibernetinio saugumo taryba šiam atvejui netinka, nes pačios tarybos tikslas bendras yra truputėlį kitoks. Iš esmės valstybės mastu tai turėtų būti pilno etato žmonės dirbantys kaip atskiras segmentas KAM‘e, kaip politiką formuojančioje institucijoje arba NKSC, kaip politiką įgyvendinančioje institucijoje. Vienas iš jų vienareikšmiškai.

JB: o gal esate susidūrę su kokia nors verta dėmesio užsienio praktika, kurią galima panaudoti įgyvendinant CSP3 Lietuvoje?

R7: aš dabar galvoju ar pas Estus irgi yra su jų savanoriška veikla valstybės labui. Va ten vienas iš pavyzdžių galėtų būti. Pas mus analogas yra per KASP (aut. past. Krašto apsaugos savanorių pajėgos) užsisukęs, o ten nepamenu ar per karinę ar civilinę prizmę. Nors Lietuvos atveju, gali būti, kad tai irgi nėra PPP, nes privataus sektoriaus atstovai užsivilkę uniformą patampa viešojo sektoriaus, vadinkime taip, dalimi įgaudami Krašto apsaugos savanorio statusą.

JB: bet šiuo atveju pažiūrėkime: valstybė neturi kompetencijų, jai reikia šią spragą užlopyti ir ji naudojasi privataus sektoriaus darbuotojais toms kompetencijoms gauti.

R7: bet jeigu jie negautų uniformos, aš sakyčiau, kad 100% PPP. O gavę uniformą jie patampa viešojo sektoriaus dalimi. Kaip CSP3 apraiška tai taip, bet ar ateityje tai atitiks patvirtinus sąvokas – neaišku.