Vilniaus universitetas
TARPTAUTINIŲ SANTYKIŲ IR POLITIKOS MOKSLŲ INSTITUTAS

TARPTAUTINIŲ SANTYKIŲ IR DIPLOMATIJOS MAGISTRO PROGRAMA

DOMINYKAS AUGUTIS
II kurso studentas

KIBERNETINĖS ERDVĖS SAUGUMIZAVIMAS LIETUVOJE 2018 – 2023 M. LAIKOTARPIU

MAGISTRO DARBAS

Darbo vadovas: dr. Nerijus Maliukevičius

Vilnius, 2023

Magistro darbo vadovo išvados dėl darbo gynimo:
.....
.....
.....

..... **.....**
.....
(data) (v., pavardė) (parašas)

Magistro darbas įteiktas gynimo komisijai:

..... **.....**
(data) (Gynimo komisijos sekretoriaus/ės parašas)

Magistro darbo recenzentas/ė:

.....
(v., pavardė)

Magistro darbų gynimo komisijos įvertinimas:

.....

Komisijos pirmininkas/ė:
Komisijos nariai:

PATVIRTINIMAS APIE ATLIKTO DARBO SAVARANKIŠKUMĄ

Patvirtinu, kad įteikiamas darbas „*Kibernetinės erdvės saugumizavimas Lietuvoje 2018 – 2023 m. laikotarpiu“* yra:

1. Atliktas mano paties ir nėra pateiktas kitam kursui šiame ar ankstesniuose semestruose;
2. Nebuvo naudotas kitame Institute/Universitete Lietuvoje ir užsienyje;
3. Nenaudoja šaltinių, kurie nėra nurodyti darbe, ir pateikia visą panaudotos literatūros sąrašą.

Dominykas Augutis

BIBLIOGRAFINIO APRAŠO LAPAS

Augutis, D., Kibernetinės erdvės saugumizavimas Lietuvoje 2018 – 2023 m. laikotarpiu: Tarptautinių santykių ir diplomatijos programos magistro darbas / VU Tarptautinių santykių ir politikos mokslų institutas; darbo vadovas dr. N. Maliukevičius. – V., 2023. – 79 p.

Reikšminiai žodžiai: saugumizavimas, saugumas, kibernetinis saugumas, kibernetinės grėsmės, kibernetinė erdvė, Kopenhagos mokykla

Šiame darbe nagrinėjamas Lietuvos kibernetinės erdvės saugumizavimo procesas 2018 – 2023 m. laikotarpiu, lyginant strateginiuose dokumentuose įtvirtintas kibernetinio saugumo nuostatas su saugumo politiką formuojančių ir įgyvendinančių institucijų atstovų diskursu. Darbe remiamasi saugumizavimo teorine prielaida, analizuojami saugotini (referentiniai) objektai, grėsmės šaltiniai ir priemonės, grėsmėms užkardyti. Dokumentų ir institucijų atstovų diskurso palyginimas per saugumizavimo teorijos perspektyvą leidžia atsakyti į klausimą, ar žvelgiant per šią teoriją galima rasti reikšmingų panašumų / skirtumų, darančių įtaką kibernetinės erdvės saugumizavimo procesui Lietuvoje.

Turinys

Įvadas

Kibernetinė erdvė jau kuris laikas yra neatsiejama gyvenimo dalis tiek eiliniams piliečiams, tiek valstybės institucijoms. 2020 m. duomenimis, Lietuvoje bent kartą per savaitę internetu naudojasi 83 procentai gyventojų, o 16-24 metų amžiaus grupėje šis skaičius siekia 99 proc. Čia gyventojai komunikuoja (78.5 proc.), skaito naujienas (74 proc.), ieško informacijos, susijusios su sveikatos priežiūra (57.1 proc.) ir kt.[1] Tuo tarpu valstybės institucijoms, užtikrinančioms įvairias paslaugas, tokias kaip komunikacijos, sveikatos apsauga ar vykdančioms kitas funkcijas, pavyzdžiui, krašto gynybą, skaitmenizacija leidžia tai daryti efektyviau, greičiau ir patogiau.

Vis dėlto, plataus masto „migracija“ į kibernetinę erdvę atveria ir naujus potencialius iššūkius, ir pavojus. Tiek pavieniai hakeriai ar jų susivienijimai („Anonymous“), tiek tokie tarptautiniai veikėjai, kaip valstybės ar teroristinės organizacijos, veikia kibernetinėje erdvėje. Karas jau seniai nebeapsiriboja tik konvenciniu lauku, ypač hibridinių konfliktų kontekste, apimančiame informacinę, ekonominę, **kibernetinę** ir kitas sritis. Žema „poveikio kartelė“ (teoriškai rezultatą galima pasiekti ir su eiliniam piliečiui prieinama kompiuterine įranga) ar nesusekamumas (ką jau ilgus metus demonstruoja „Anonymous“) daro skaitmeninę erdvę panašią į „Laukinius vakarus“, kur grėsmė gali slypėti bet kur.

Visgi, turint tik valstybėms prieinamas resursų apimtis ir politinį motyvą, galima pridaryti rimtos žalos priešininkui. NATO šalis Estija 2007-aisiais paskelbė iškelianti „Bronzinio kario“ skulptūrą iš Talino centro. Šis žingsnis supykdė Kremlių, kaip atsaką surengusį eilę atakų prieš Estijos bankus, internetinę žiniasklaidą ir valstybės komunikacinius kanalus, taip reikšmingai sutrikdant eilinių estų ir šalies politinės valdžios kasdienybę.[2] Tai iki šios viena didžiausių vienos valstybės prieš kitą surengtų kibernetinių atakų, kurios įvykdymą, beje, agresorė atkakliai neigė. Šis įvykis yra ir bene labiausiai nuskambėjusi ir daugiausiai įvairių sričių analitikų dėmesio susilaukusi dviejų valstybių konflikto kibernetinėje erdvėje apraiška, paskatinusi ir NATO kibernetinės gynybos kompetencijos centro (NKGKC) Taline įkūrimą 2008-aisiais, skirtą kovoti su grėsmėmis kibernetinėje erdvėje.[3]

Lietuvos kibernetinė erdvė taip pat nuolatos „testuojama“ įvairaus tipo priešiškų veikėjų. Kaip pastebi Nacionalinio kibernetinio saugumo centro (NKSC) atstovai, 2022-ųjų pirmąjį ketvirtį incidentų kibernetinėje erdvėje skaičius išlieka aukštas (per pirmuosius tris 2022 metų mėnesius fiksuota 1020 incidentų – per atitinkamą 2021 m. laikotarpį – 981), nepaisant blėstančios pandemijos,

[1] Oficialios statistikos portalas, Skaitmeninė ekonomika ir visuomenė Lietuvoje (2020 m. leidimas), žiūrėta 2023 m. sausio 12 d., https://osp.stat.gov.lt/skaitmenine-ekonomika-ir-visuomene-lietuvoje-2020/gyvenimas-internete

[2] Rain Ottis, „Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective“, *Cooperative Cyber Defence Centre of Excellence,* Talinas, 2008, žiūrėta 2023 m. sausio 12 d., https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

[3] The NATO Cooperative Cyber Defence Centre of Excellence, žiūrėta 2023 m. sausio 12 d., https://ccdcoe.org/about-us/

sukėlusios tokių atvejų šuolį.[4] Ekspertai pabrėžia ir tai, kad užfiksuotas išpuolių šuolis aštuntąją metų savaitę, prasidėjus Rusijos invazijai į Ukrainą, o 16 proc. Kibernetinių incidentų fiksuoti ypatingos svarbos informacinės infrastruktūros valdytojų ryšių ir informacinėse sistemose.[5] Pastarasis faktas rodo ir tai, kibernetinėmis atakomis gali būti bandoma sutrikdyti ir kritinės šalies infrastruktūros veikimą.

Ši statistika Lietuvoje neignoruojama ir į kibernetines grėsmes Lietuvoje žiūrima rimtai. Be veiklos NATO ir kituose formatuose, Krašto apsaugos ministerija leidžia metines Nacionalinio kibernetinio saugumo būklės ataskaitas, eskaluoja klausimą viešojoje erdvėje. Kibernetinis saugumas atskiro dėmesio susilaukia ir Valstybės saugumo departamento Grėsmių nacionaliniam saugumui vertinimuose. Bene didžiausias žingsnis čia buvo žengtas 2015-aisiais, įkuriant Nacionalinį kibernetinio saugumo centrą (NKSC). Centras atsakingas už kibernetinių incidentų valdymą, saugumo reikalavimų įgyvendinimo stebėseną ir kontrolę, ypatingos svarbos informacinės infrastruktūros kibernetinį saugumą ir informacinių išteklių akreditaciją.“[6]

NKSC buvo įkurtas pagal nuo 2015-ųjų sausio 1-ąją įsigaliojusį Kibernetinio saugumo įstatymą, nustatantį kibernetinio saugumo sistemos organizavimą, valdymą, kontrolę ir kitus aspektus.[7] Centro įkūrimas buvo pirmas, tačiau ne paskutinis didesnio masto žingsnis kibernetinio saugumo didinimo link. 2018-aisias, penkerių metų laikotarpiui buvo priimta Nacionalinė kibernetinio saugumo strategija, kuria siekiama įvairiapusiškai stiprinti valstybės kibernetinį saugumą, gynybos pajėgumų plėtrą ir kt.[8] Toks kibernetinės erdvės saugumo institucionalizavimas rodo ir politikų susidomėjimą šia sritimi, nors anuomet viešojoje erdvėje daug daugiau dėmesio susilaukė energetinis (suskystintų gamtinių dujų (SGD) terminalo statybos) ar konvencinis saugumas (šauktinių grąžinimas, bendrojo vidaus produkto (BVP) dalis skiriama krašto apsaugai).

Nors, kaip rodo statistika, internetu naudojasi didžioji dalis Lietuvos gyventojų, kibernetinės erdvės saugumas yra labai techninė sritis, gerai suprantama tik gana siauriam ratui informacinių technologijų ekspertų. Saugumizavimo teoretikai kibernetinę erdvę apibūdina kaip ypatingai palankią „technifikacijai“, atitolinančiai ją nuo politinio ir kasdienio piliečių gyvenimo, nes neturint specifinių žinių, operuoti reikalingomis sąvokomis yra per daug sudėtinga.[9] Vis dėlto, šalyje jau padaryti darbai,

[4] Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos, „Svarbiausia lietuvos kibernetinio saugumo būklės statistika ir tendencijos, 2021 m. – 2022 m. I ketv., 2022, žiūrėta 2023 m. sausio 13 d., https://kam.lt/wp-content/uploads/2022/05/Kibernetinio-saugumo-santrauka-1.pdf, p. 3-4

[5] *Ibid.*

[6] Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos, „Veikla“, žiūrėta 2023 m. sausio 12 d., https://www.nksc.lt/veikla.html

[7] Lietuvos Respublikos Seimas, *„Lietuvos Respublikos kibernetinio saugumo įstatymas“,* Vilnius, 2014, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee (žiūrėta 2023 m. sausio 13 d.)

[8] Krašto apsaugos ministerija, „Nacionalinė kibernetinio saugumo strategija”, 2018, žiūrėta 2023 m. sausio 13 d., https://kam.lt/wp-content/uploads/2022/03/nacionaline-kibernetinio-saugumo-strategija.pdf

[9] Myriam Dunn Cavelty, Florian J. Egloff, „Hyper-Securitization, Everyday Security Practice and Technification: Cyber-Security Logics in Switzerland“, *Swiss Political Science Review 27(1)*, p. 146

stiprinant kibernetinį saugumą bei tęsiamas diskursas (ataskaitos ir kt.) rodo, kad diskusijos šia tema vyksta tiek politikų, tiek ekspertų tarpe, o saugumizavimas, nepaisant jau nuveiktų darbų, vyksta ir toliau.

Atsižvelgiant į kibernetinės erdvės specifiškumą, polinkį technifikacijai, vertėtų atidžiau pažvelgti būtent į vyraujantį diskursą. Politikai nebūtinai yra kibernetinio saugumo ekspertai, be to, vedami kitų paskatų gali kalbėti ne tai, kas jau užfiksuota Kibernetinio saugumo įstatyme ar kituose dokumentuose. Tai, kaip bus parodyta vėlesniuose skirsniuose, gali trikdyti tebesitęsiantį saugumizavimo procesą.

Iš to ir kyla **pagrindinis darbo probleminis klausimas: ar kibernetinio saugumo suinteresuotųjų šalių (angl. *stakeholders*) diskursas sutampa su tuo, kas jau įtraukta į oficialius dokumentus?** Saugumizavimas yra kalbos aktas, todėl šiame procese siekiant sėkmės, diskursas turi būti naudojamas tikslingai, o komunikacinės klaidos gali sudaryti kliūtis gaunant auditorijos pritarimą – pagal teoriją būtiną sąlygą. Visgi, svarbu pabrėžti, kad čia dalyvauja ne viena šalis, todėl tyrimo metu bus apžvelgti pagrindinių šalies gynybos ir saugumą formuojančių pareigūnų pasisakymai iš Nacionalinio saugumo ir gynybos komiteto (NSGK), Krašto apsaugos ministerijos (KAM), Lietuvos kariuomenės, Kibernetinio saugumo tarybos (KST), Prezidentūros bei Vidaus reikalų ministerijos (VRM). Šios institucijos, remiantis Kibernetinio saugumo įstatyme numatytomis funkcijomis, laikytinos pagrindinėmis suinteresuotomis šalimis kibernetinio saugumizavimo procese. Atsižvelgiant į technifikacijos potencialiai keliamas problemas, į tyrimą taip pat įtraukta ir 10 pasisakymų iš kibernetinio saugumo ekspertų – šie duomenys leis patikrinti ar šalies institucijos šią erdvę mato taip pat, kaip ir geriausiai ją išmanantys ekspertai.

Darbo tikslas: ištirti kibernetinės erdvės saugumizavimo procesą, remiantis strateginiais dokumentais, politikų diskurso analize, nustatyti potencialius diskurso panašumus ar skirtumus, siekiant atsakyti į klausimą ar institucijos prisideda prie tolesnio šios srities saugumizavimo.

Darbo aktualumas: 2023-aisiais baigia galioti prieš penkerius metus priimta kibernetinio saugumo strategija, todėl tyrimas leis atskleisti visą strategijos veikimo metu vykusį saugumizavimo procesą ir įvertinti ar saugumo politiką formuluojančių ir įgyvendinančių pareigūnų komunikacija sutampa su tuo, kas deklaruojama dokumentuose. Tai gali būti reikšminga, siekiant atskleisti ar tai, kas deklaruojama, tėra šabloniškas formalumas, prasilenkiantis su realybe (politikų komunikacija ir veiksmais), ar, visgi, yra aiškus sutarimas ir kryptingas tikslų ir užduočių įgyvendinimas.

Metodologija: Darbe bus naudojama diskurso analizė. Pasitelkus šį metodą, bus tiriamas kibernetinės erdvės saugumizavimo procesas nuo 2018m. (priimama KAM Nacionalinė kibernetinio saugumo

strategija (NKSS)) iki 2023 m. balandžio (NKSS priimta penkerių metų laikotarpiui).[10] Suinteresuotųjų šalių pasisakymai, pranešimai žiniasklaidai ir kita vieša komunikacija bus tiriama pasitelkiant kokybinę turinio analizės prieigą.

Uždaviniai:

1. Ištirti pagrindines saugumizavimo teorijos prielaidas ir bruožus, išskiriant ir esminius kriterijus, reikalingus saugumizavimo vertinimui.
2. Pristatyti kibernetinės erdvės saugumo Lietuvoje raidą, vedusią iki sėkmingo saugumizavimo 2015-aisiais.
3. Išnagrinėti kibernetinės erdvės saugumizavimo bruožus strateginiuose dokumentuose ir saugumo ataskaitose tyrimo laikotarpiu.
4. Išnagrinėti politikų naudojamą kibernetinio saugumo diskursą ir palyginti su strateginiais dokumentais ir saugumo ataskaitomis, ieškant reikšmingų skirtumų ar tapatumų ar skirtumų.
5. Remiantis išvadomis ir politikų diskursu pateikti apibendrinimą apie galimą neatitikimą tarp diskursų ir pateikti rekomendacijas.

Ginamieji teiginiai:

1. Nepaisant sėkmingo saugumizavimo 2015-aisiais, kibernetinė erdvė oficialiuose dokumentuose saugumizuojama ir toliau.
2. Krašto saugumo politiką formuojančios ir įgyvendinančios institucijos ir jų atstovai viešojoje erdvėje prisideda prie tolesnio kibernetinės erdvės saugumizavimo.

Darbo struktūra. Darbą sudaro penkios dalys. Pirmojoje bus apžvelgiama saugumizavimo teorinė prieiga ir jos pritaikymas kibernetinės erdvės saugumo tyrimams. Antroji dalis skirta kibernetinės erdvės saugumo raidą šalyje. Trečioji – įstatymų, strategijų ir kitų dokumentų, skirtų reglamentuoti kibernetinės erdvės saugumą Lietuvoje analizei (2015 m.) Trečiojoje dalyje bus siekiama ištirti saugumo politiką formuojančių ir įgyvendinančių asmenų bei organizacijų pasitelkiamą kibernetinės erdvės saugumo diskursą. Paskutinėje darbo dalyje bus pateikiama lyginamoji diskurso ir oficialių dokumentų analizė bei pateikiamos apibendrinamosios darbo išvados.

[10] Krašto apsaugos ministerija, Nacionalinė kibernetinio saugumo strategija, p. 5
žiūrėta 2023 m. kovo 12 d.

1. Kibernetines erdves saugumizavimo tyrimai

Nors saugumizavimo studijos jau yra gerokai pažengusios, dėka Kopenhagos mokyklos ir tokių jos atstovų, kaip Barry Buzan pastangų, kibernetinės erdvės saugumas yra ganėtinai nauja niša politikos mokslų ir saugumo studijų kontekste. Kibernetiniu saugumu labiau domimasi tik porą pastarųjų dešimtmečių ir, nors šioje srityje jau pasiekta nemažai atradimų (tiek technologine, tiek teorine prasme), saugumizavimo ir kibernetinės erdvės saugumo sugretinimas tame pačiame tyrime yra ganėtinai nauja prieiga. Akademinėje literatūroje tokių atvejų vis dar nėra gausu, o juose dažniausiai kalbama apie JAV pastangas ar Estijos „Bronzinio kario“ istoriją.

1.1 B. Buzan ir saugumizavimo ištakos

Saugumizavimo teorijoje bene didžiausią vaidmenį vaidina konstruktyvistai iš jau minėtos Kopenhagos mokyklos, iš kurių bene žinomiausi – Barry Buzan, Ole Waever ir Jaap de Wilde, darbo „Security: a New Framework for Analysis“ autoriai.

Mokslininkai saugumizavimo aiškinimą pradeda nuo to, kaip valstybės reaguoja į grėsmes. Pirmuoju atveju jos yra visiškai ignoruojamos, laikomos nekeliančiomis realaus pavojaus, pavyzdžiui, valstybės išlikimui ar jos gyventojams, todėl net nėra įtraukiamos į politinį procesą – jos netampa sprendimų priėmėjų darbotvarkės dalimi. Antruoju, grėsmės suvokiamos kaip potencialiai galinčios padaryti žalos, tačiau nėra laikomos „egzistencinėmis“, todėl gali tapti pvz., viešojo diskurso dalimi (politizacija). Tai nulemia grėsmės įtraukimą į politinę darbotvarkę kaip vieną iš klausimų, kuris nėra išsiskiriantis savo svarba. Galiausiai, grėsmė gali būti matoma kaip egzistencinė, t.y., ji laikoma prioritetine, kurios sprendimui būtina skirti išskirtinį dėmesį bei imtis iš tradicinės politikos rėmų išeinančių veiksmų.[11]

Kalbant apie „iš tradicinės politikos rėmų“ išeinančius ar „politinio žaidimo taisykles laužančius“ veiksmus, autoriai kaip pavyzdžius pateikia mokestinius pakeitimus, žmogaus teisių apribojimus ar tiesiog visuomenės energijos ir kitų išteklių nukreipimą į konkrečią sritį ar darbą. Čia autoriai iškart pabrėžia, kad saugumizuojama grėsmė nebūtinai turi būti egzistencinė, svarbu, kad ji būtų pristatoma kaip tokia.[12] Būtent kalbinis aktas, sėkmingai legitimizuojantis „taisyklių laužymą“, o ne pats egzistencinės grėsmės faktas ar taisyklių pokytis yra svarbiausias autorių įvardintas saugumizavimo kriterijus. Visgi, be auditorijos pritarimo, saugumizavimas nėra laikomas sėkmingu ir Buzan bei kolegų yra įvardinamas kaip „saugumizuojantis ėjimas“ (angl. *securitizing move*), ir tik gavus auditorijos, kuriai komunikuojama pritarimą, ėjimas tampa sėkmingu saugumizavimu. Taigi, saugumizavimui nėra būtinas ir pats „taisykles laužantis“ veiksmas, veikiau sudaromos sąlygos, esant

[11] Barry Buzan, Ole Waever, Jaap de Wilde, „Security: a New Framework for Analysis, Lynne Rienner Publishers“, 1998, p. 21-22
[12] *Ibid.*, p. 24

reikalui, jį implementuoti.[13] Tai parodo ir esminę diskurso vietą procese ir kartu tai, kad tiriant saugumizavimą, reikėtų žiūrėti į kalbinius aktus.

Vis dėlto, diskursas yra subjektyvus, o saugumizavimo procesas nėra statiškas. Kaip pastebi mokslininkai, tai, kas priimtina kaip grėsmė vienai visuomenei, gali atrodyti paranoiška kitai ar priešingai – vienų valstybių konkrečios grėsmės atmetimas, kitoms gali atrodyti kaip aklas grėsmės ignoravimas. Tai gali priklausyti tiek nuo istorinių patirčių, tiek nuo dabartinės geopolitinės situacijos ar kitų veiksnių.[14] Autoriai apibrėžia ir procese dalyvaujančius veikėjus: „saugumizuojantys veikėjai" (angl. *securitizing actors*) – veikėjai, įprastai politikai ar visuomenės veikėjai, siekiantys parodyti problemas, keliančias egzistencinę grėsmę „referentiniam objektui" (angl. *referent objects*). Tai visuomenės ar valstybės gyvenimo aspektai, kuriuos būtina apsaugoti – dažniausiai mokslininkų pasitelkiamas pavyzdys yra suverenitetas ar esama valstybės santvarka, tuo tarpu, kaip parodys vėlesni darbai, kalbant apie kibernetinę erdvę, referentinis objektas gali būti ir kritinė infrastruktūra, tokia kaip ypatingos svarbos komunikacijos ar sveikatos apsauga. Tuo tarpu „funkciniai veikėjai" (angl. *functional actors*) – veikėjai, turintys įtaką specifinei sričiai, tačiau nesantys esminiai žaidėjai, sprendžiant konkretų klausimą.[15] Kalbant apie kibernetinį saugumą, tai galėtų būti informacinių technologijų (IT) įmonės, viešojoje erdvėje matomi IT ekspertai ir kt.

Kalbant apie tyrimus, kuriuose taikoma saugumizavimo teorinė prieiga, svarbu aiškiau apibrėžti ir jau minėtą skirtį tarp klausimo politizavimo bei saugumizavimo. O. Waeveris, vienas iš anksčiau aptarto teksto autorių, kitame savo veikale teigia, kad saugumas *„security"* ir nesaugumas *„insecurity"* nėra viena kitai priešiškos sąvokos. Veikiau saugumas atitinka dvi sąlygas – egzistuojančią grėsmę ir veiksmą, nukreiptą prieš ją, o nesaugumas – egzistuojančią grėsmę, kuriai nėra jokio atsako (veiksmo). Tuo tarpu, neegzistuojant saugumo problemai, mes nemąstome ir apie patį *saugumą* – absoliutus saugumas neegzistuoja, nes jam apibrėžti naudojamos sąvokos indikuoja nesaugumo atsiradimą.[16] Toks diskurso naudojimas anot autoriaus rodo, kad apie grėsmės saugumizavimą negalima mąstyti *saugumo* sąvokomis, tai reikėtų daryti tik nuo jų atsiribojus, priešingu atveju, grėsmė vis tiek bus saugumizuota.[17] Tai, anot mokslininko, rodo, kad „politizuojamus" klausimus reikėtų visiškai atsieti nuo saugumizavimo diskurso.

1.2 Kritika saugumizavimo teorijai

Norint geriau suprasti saugumizavimo procesą ir jo kriterijus, reikėtų apžvelgti ir Jungtinės Karalystės profesoriaus Alano Collinso įžvalgas. Savo tekste „Securitization, Frankenstein's Monster

[13] *Ibid.*, p. 25
[14] *Ibid.*, p. 30
[15] *Ibid.*, p. 36
[16] Ole Waever, Chapter 3, „Securitization and Desecuritization", „On Security", sud. Ronnie D Lipschutz, New York : Columbia University Press, 1995 m., p. 7
[17] *Ibid.*, p. 7-8

and Malaysian education“, Collinsas kvestionuoja dar Buzano, Weawerio ir de Wilde aprašytą saugumizavimo procesą ir kriterijus, reikalingus jam nustatyti.

Pirmąjį klausimą Collinsas kelia dėl saugumizavimo proceso inicijavimo (saugumizuojančio ėjimo (angl. *securitizing move*). Anot jo, autoritariniuose ir totalitariniuose režimuose tai – griežtai tik valdžios prerogatyva, nes čia valdantysis elitas dažniausiai turi visišką medijų, taigi, ir diskurso kontrolę. Tuo tarpu demokratijose, kaip pastebi profesorius, piliečių suteiktas mandatas valdžiai suteikia ir privilegiją saugumizuoti tam tikrus klausimus. Vis dėlto, visuomenė gali nepriimti saugumizuojančio ėjimo ar per kitus veikėjus, pvz., profesines sąjungas, kelti alternatyvas.[18]

Antroji Collinso formuluojama problema – nepaprastųjų priemonių (angl. *extraordinary measures*), išeinančių iš įprastinės politikos rėmų, svarba saugumizavimo procese. Viena vertus, tokios priemonės ir visuomenės pritarimas joms parodo, kad klausimas buvo sėkmingai saugumizuotas ir pakilo virš eilinės politikos. Be to, taip sukuriama „draugo“ (ar „mūsų“) ir „priešo“ perskyra, reikalinga saugumizuojant bei atsirandanti iš visuomenės mandato imtis nepaprastųjų priemonių ir aiškiai įvardinti priešą.[19] Tačiau čia Collinsas visgi atmeta nepaprastųjų priemonių būtinybę, kaip kriterijų, įrodantį saugumizavimo procesą. Anot jo, sėkmingai saugumizuoti problemą galima ir pasirinkus ją spręsti įprastu keliu, t.y. per politinę darbotvarkę (atmetama ir platformos nepaprastosioms priemonėms būtinybė). Iš įprastinės politikos rėmų išeinančių priemonių ėmimasis gali būti kontr-produktyvus specifinėse situacijose, taigi problemos (grėsmės) sprendimas politiniu keliu nereiškia, kad klausimas nebuvo sėkmingai saugumizuotas.[20]

1.3 Nepavykęs saugumizavimas

Svarbu paminėti ir tai, kaip literatūroje įvardinamas apibrėžiamas nepavykęs saugumizavimas. Anot Buzan, Waever ir Wilde sėkmingo saugumizavimo esminiai kriterijai yra egzistencinės grėsmės (ar pristatymo kaip tokios) egzistavimas bei auditorijos pritarimas saugumizuojančio veikėjo diskursui. Priešingas scenarijus – nesėkmė pristatant grėsmę kaip egzistencinę ar auditorijos nepritarimas kitiems proceso aspektams lems ir nepavykusį saugumizavimą. Mark B. Salter nesėkmes saugumizuojant skirsto į tris kategorijas: „Normalius atsitikimus“ (angl. *Normal accidents*), „Vidines nesėkmes“ (angl. *Internal failures*) ir „Išorines nesėkmes“ (angl. External failures).[21] Pirmoji kategorija nurodo, kad nepaisant sėkmingo saugumizavimo ėjimo, dėl kompleksiškų visuomenės ir biurokratinių procesų, nesėkmės kartais yra neišvengiamos (tuomečiui JAV prezidentui George W. Bush pavyko įtikinti Kongresą, kad Irako

[18] Alan Collins, „Securitization, Frankenstein's Monster and Malaysian education“, *The Pacific Review*, 18:4, 2005 m., p. 570-571
[19] *Ibid.*, p. 571
[20] *Ibid.*, p. 573
[21] Mark B. Salter, „When securitization fails: The hard case of counter-terrorism programs“, *Securitization Theory,* Routledge, 2010 m., p. 116-131

grėsmė yra egzistencinė, tačiau klausimui persikėlus į visuomenę, atsirado vietos ir debatams). Vidinės nesėkmės apibūdina saugumizuojančio veikėjo santykį su auditorija ir įvyksta nepavykus įtikinti, kad grėsmė priklauso politiniam laukui ir yra egzistencinė (klausimas gali persipinti su pvz., ekonomine plotme). Galiausiai, išorinės nesėkmės apibūdinamos kaip tokios, kurių metu auditorija nepriima pasiūlyto sprendimo būdo ar nenori suteikti iš įprastos politikos rėmų išeinančių įgaliojimų (George W. Bush iš pradžių nepavyko įtikinti teismų ir visuomenės, kad invazija į Iraką yra tinkamas Al-Qaeda keliamų problemų sprendimų būdas, nepaisant to, kad grėsmė pripažinta kaip egzistencinė JAV).[22]

1.4 Kibernetinės erdvės saugumizavimas

Pereinant prie kibernetinės erdvės saugumizavimo, bene labiausiai žinomas ir akademinėse diskusijose dažniausiai pasirodantis straipsnis yra Lene Hansen ir Helen Nissenbaum Estijos atvejo analizė. Autorės savo tekste „Digital Disaster, Cyber Security and the Copenhangen School“ pasitelkia B. Buzano suformuluotą teorinę prieigą, tirdamos, kaip Estija saugumizavo savo kibernetinę erdvę po 2007-ųjų Rusijos įvykdytos kibernetinės atakos prieš kritinę šalies kibernetinę infrastruktūrą – oficialius valstybės internetinius puslapius, bankus ir žiniasklaidą.[23]

Pačioje teksto pradžioje, pasitelkdamos tokius pavyzdžius, kaip Kritinės infrastruktūros apsaugos komisijos (angl. *Commission on Critical Infrastructure Protection)* įkūrimas, Džordžo Bušo jaunesniojo formuluota Nacionalinė kibernetinės apsaugos strategija (angl. *The National Strategy to Secure Cyberspace*) ar NATO kibernetinio saugumo centro įsteigimas Estijoje, teigia, kad kibernetinė erdvė jau yra sėkmingai saugumizuojama.Vis dėlto, pagrindinis autorių darbo tikslas – rasti kibernetinės erdvės saugumo vietą platesniame saugumo studijų spektre. Anot Hansen ir Nissenbaum, tam reikia įvardinti galimus referentinius objektus ir grėsmes, kaip konkretūs saugumizavimo atvejai gali būti analizuojami ir ką iš viso to galima pasiimti.[24]

Autorių tyrimas parodo, kad „tinklas“ (angl. *the Network*) ir „individas“ (angl. *the Individual*) yra kertiniai kibernetinės erdvės referentiniai objektai, kuriems dažniausiai ir kyla grėsmės.[25] „Tinklą“ autorės apibūdina kaip kompiuterių sistemas, kurios kontroliuoja pvz., fizinius objektus – traukinius, vamzdynus, elektrą ir kt. Tuo tarpu po terminu „individas“ slepiasi grėsmės gyventojams. Visgi, autorės pabrėžia, kad nei tinklas, nei individas nėra atsieti nuo platesnio konteksto – neigiamas poveikis tinklui paveiks ir gyventojus (individus), tuo tarpu pačių individų saugumas yra matomas kaip neatsiejama dalis visame kibernetinės erdvės saugumizavimo procese. [26]

---

[22] *Ibid*.
[23] Lene Hansen, Helen Nissenbaum, „Digital Disaster, Cyber Security, and the Copenhagen School“, *International Studies Quarterly*, Vol. 53, Nr. 4, 2009 m.
[24] *Ibid.*, p. 1157
[25] *Ibid.*, p. 1171
[26] *Ibid.*, p. 1161, 1163

Kitas svarbus autorių atradimas – kibernetinės erdvės saugume, skirtingai nei kituose sektoriuose dažnai susiduriama su sąvokomis *„hipersaugumizavimas“, „technifikacija“ ir „kasdienės saugumo praktikos“.*[27] Technifikacijos atsiradimą lemia tiek šios erdvės saugumizavimo hipotetiškumas (kibernetinių išpuolių, sukėlusių rimtą žalą valstybei istorijoje nėra daug), tiek srities problematiškumas, nes greitai besivystančios sudėtingos technologijos suprantamos tik siauram ratui IT specialistų, tampančių „privilegijuotais“ kalbėti apie kibernetinį saugumą. Tuo tarpu hipersaugumizavimas – terminas, nurodantis tiek grėsmės, tiek priemonių, kaip atsako jai, hiperbolizavimą buvo įvardintas dar B. Buzan, kaip terminas, vedantis virš „normalaus“ saugumizavimo. Paskutinė sąvoka – kasdienės saugumo praktikos – skirtos parodyti žmonėms, kad katastrofiniai kibernetinės erdvės scenarijai jų neaplenks ir palies jų kasdienybę. Taip gali būti siekiama didesnio pritarimo saugumizuojančiam ėjimui bei sukurti jungtį tarp katastrofinių scenarijų ir auditorijos.[28]

Būtent hipersaugumizavimas dažnai atsispindi ir kitų autorių darbuose, kuriuose nagrinėjamas kibernetinės erdvės saugumizavimas. Tiesa, čia dažniau sutinkamas „Kibernetinės pražūties“ (angl. *Cyberdoom*) terminas. Mokslininkai Miguel Alberto Gomez ir Christopher Whyte, „pražūties“ scenarijus apibrėžiantys kaip tokius, kuriuose nesaugumas lemtų rimtus socialinius, ekonominius ar politinius trikdžius, pastebi, kad tokie naratyvai nėra reti. Pavyzdžiui, konvencinėje plotmėje neretai sutinkami Rugsėjo 11-osios ar Šaltojo karo naratyvai, jau sėkmingai gyvuojantys net ir nenaudojant jų saugumizuojančių veikėjų diskurse.[29] Visgi, Gomez ir Whyte teigimu, „kibernetinė pražūtis“ yra veikiau žalinga, nei naudinga saugumizuojant kibernetinę erdvę. Atlikę kiekybinį tyrimą, ir apklausę per tūkstantį interneto vartotojų Jungtinėje Karalystėje ir JAV, jie padarė išvadas, kad vietoje grasinimų „pražūtimi“, respondentai daug labiau linkę reaguoti į teigiamą diskursą, t.y., galimus saugios kibernetinės erdvės naudas verslui ir patiems gyventojams bei potencialų jų praradimą, neužtikrinant kibernetinio saugumo.[30]

1.5 Kibernetinės erdvės saugumizavimo kritika

Svarbu pabrėžti ir tai, kad egzistuoja ir kibernetinės erdvės saugumizavimo oponentų stovykla, kuri taip pat remiasi hipersaugumizavimo, kibernetinės pražūties naratyvais ar empirinių atvejų trūkumais. Luisa Cruz Lobato ir Kai Michael Kenkel tekste „Discourses of cyberspace securitization in Brazil and in the United States“ pastebi, kad beveik visas kibernetinės erdvės saugumizavimo diskursas remiasi spekuliacijomis, nes skirtingai nei su karinėmis ar ekonominėmis

[27] *Ibid.*, p. 1171
[28] *Ibid.*, p. 1164-1167
[29] Miguel Alberto Gomez, Christopher Whyte „Breaking the Myth of Cyber Doom: Securitization and Normalization of Novel Threats“, *International Studies Quarterly* 65, 2021 m., p. 1138
[30] *Ibid.*

grėsmėmis, turime labai mažai didelio masto kibernetinių incidentų pavyzdžių. Todėl kibernetinės erdvės saugumizuoti gali būti neverta ar net žalinga, nes nėra jokių įrodymų, kad tai gali virsti egzistencine grėsme referentiniam objektui. [31] Anot autorių, neretai sukuriama situacija, kurios metu grėsmė militarizuojama, o resursai skiriami užkardyti grėsmei, kurios tikimybė yra labai maža. Be to, hipotetiniai „kibernetiniai Perl Harborai" gali paskatinti ir savotiškas valstybių ginklavimosi varžybas, šnipinėjimą ar kitokio pobūdžio išpuolius skaitmeninėje erdvėje.[32]

1.6 Kibernetinės erdvės saugumizavimo apibendrinimas ir kriterijai

Hans, Nissenbaum, Gomez ir kiti saugumizavimo teoretikai savo darbuose argumentuoja kibernetinės erdvės saugumizavimo svarbą. Mokslininkai savo veikaluose deda svarbų žingsnį, spręsdami saugumizavimo teorijos pritaikymo spragas, kurios nėra tokios ryškios kitose, pvz., konvencinėje karo ar energetikos srityse. Spręsdami hipersaugumizavimo, kibernetinės pražūties ir kitas dilemas, mokslininkai pateikia (ar adaptuoja) vertingus įrankius tolimesniems kibernetinės erdvės saugumizavimo tyrimams, leidžiančius įvardinti galimas proceso klaidas, jo efektyvumą ir kt. Panašiai į šią sritį žvelgia ir Thierry Balzacq, Sarah Léonard ir Jan Ruzicka. Anot jų, kibernetinė erdvė ir jos saugumas yra ganėtinai jauna sritis, todėl kai Buzanas su kolegomis dešimtajame dešimtmetyje vystė saugumizavimo teorijos postulatus, šis sektorius dar nepatraukė jų dėmesio.[33] Vis dėlto, auganti tinklų svarba ir įtaka žmonėms lėmė išaugusį dėmesį šios srities saugumui, nors erdvės naujiems darbams yra pakankamai. Ypač remiantis saugumizavimo praktikomis iš kitų sričių, tokių kaip sveikatos ar aplinkos apsauga.[34]

Remiantis aptartais saugumizavimo teoretikų darbais, išskiriami šie kriterijai, leisiantys įvertinti kibernetinės erdvės saugumizavimo procesą tiek dokumentuose, tiek diskurse:

Kriterijus	**Paaiškinimas**
Ar saugumizuojamas objektas yra referentinis?	Remiantis klasikine saugumizavimo teorija, saugumizuojamas objektas turėtų būti būtina sąlyga normaliam valstybės ar visuomenės funkcionavimui palaikyti.
Ar siūlomos nepaprastosios priemonės objektui apsaugoti?	Nors nepaprastųjų priemonių taikymas kai kurių teoretikų nuomone nėra būtina sąlyga, siekis jas implementuoti gali rodyti

[31] Luisa Cruz Lobato, Kai Michael Kenkel, „Discourses of cyberspace securitization in Brazil and in the United States", internete: <https://www.scielo.br/j/rbpi/a/zDC3D9BWxQvBxk56CmLdckJ/?lang=en>
[32] *Ibid.*, p. 37-38
[33] Thierry Balzacq, Sarah Léonard ir Jan Ruzicka, „'Securitization' revisited: theory and cases", *International Relations*, Vol. 30(4), 2016 m. p. 515
[34] *Ibid.*, p. 517

	saugumizuojančio veikėjo intencijas auditorijai parodyti klausimo svarbą.
Ar minimas aiškus grėsmės šaltinis?	Grėsmės referentiniam objektui šaltinis yra būtina sąlyga, glaudžiai susijusi su referentinio objekto sąvoka.
Ar saugumizuojant naudojamas radikalesnis diskursas (kibernetinės pražūties naratyvas), ar laikomasi nuosaikesnių scenarijų?	Kaip rodo Gomez ir Whyte tyrimas, hipersaugumizavimas gali trikdyti saugumizavimo procesą. Nors tai dar savaime nelemia sėkmės/nesėkmės, patikrinus diskursą, remiantis šiuo kriteriju, galima daryti preliminarias išvadas apie kalbos vartojimo tikslingumą.

Šaltinis: sudaryta autoriaus, remiantis aprašyta teorine medžiaga.

Šių kriterijų pagalba bus analizuojami oficialūs dokumentai ir politikų naudojamas diskursas, siekiant ištirti ar tai, kas yra deklaruojama yra saugumizavimo procesas. Aiškiai įvardintos grėsmės, referentiniai objektai ir siūlomos priemonės leis susikurti bendrus vardiklius lyginamajai analizei. Jais remiantis visų pirma bus ištirti oficialūs dokumentai, kategorizuojant turinį pagal tai, kas būtų laikytina referentiniais objektais, grėsmės šaltiniais ir siūlomomis priemonėmis. Toks pat procesas bus atkartotas ir su tiriamų institucijų atstovais. Susisteminta medžiaga leis atsakyti į darbo pradžioje iškeltą tikslą, kuriuo siekiama nustatyti saugumizavimo proceso panašumus ir skirtumus tarp dokumentų ir institucijų atstovų.

Prieš pereinant prie saugumizavimo literatūros apibendrinimo, svarbu paminėti, kad kibernetinės erdvės saugumizavimo klausimo Lietuvoje nagrinėjimui jau yra skirtas akademinis darbas. Vilniaus Universiteto Tarptautinių santykių ir politikos mokslų instituto (VU TSPMI) bakalauro studentė Ieva Juknevičiūtė 2016 metais parengto bakalauro darbo metu nagrinėjo 2013 – 2015 metų laikotarpį ir tuo metu vykusį kibernetinės erdvės saugumizavimo procesą.[35] Autorė parodė, kad duotuoju laikotarpiu kibernetinė erdvė buvo sėkmingai saugumizuota įstatymuose, dokumentuose ir kitur bei kaip prie to prisidėjo tuo metu valstybės gynybą formavę politikai. Visgi, tiek kibernetinė erdvė, tiek geopolitinė situacija nuo minėto laikotarpio gana reikšmingai pasikeitė, su dar labiau išaugusia Rusijos grėsme ar išryškėjusia Kinija, kaip saugumo politikos problema. Siekiant nedubliuoti I. Juknevičiūtės atlikto darbo, į 2013 – 2015 metų laikotarpį bus referuojama

[35] Ieva Juknevičiūtė, „Kibernetinės erdvės saugumizavimas Lietuvoje“ (Bakalauro darbas, Vilniaus universitetas, Tarptautinių santykių ir politikos mokslų institutas, 2016)

kaip atspirties tašką, nuo kurio prasidėjo reikšmingi žingsniai saugumizuojant Lietuvos kibernetinę erdvę, fokusuojantis į 2018 – 2023 metų laikotarpį kaip tyrimo rėžius.

Apibendrinant, nors kibernetinės erdvės saugumizavimas, palyginus su kitais sektoriais, yra palyginti gana nauja niša, Hansen, Nissenbaum ir kitos (-i) mokslininkės (-ai) parodė, kad čia taip pat galima pritaikyti šią teorinę prieigą. Visgi, kibernetinės erdvės specifika (spartus vystymasis, empirinių atvejų trūkumas ir kt.) kelia papildomus iššūkius, siekiant ištirti kaip ši sritis saugumizuojama, o neretai pasitelkiamas hipersaugumizavimas ar pražūties scenarijai gali kišti koją saugumizuojantiems veikėjams. Nepaisant to, remiantis dar Buzan ir kolegų suformuluotais, bei Gomez, Whyte ir kitų papildytais kriterijais, galima ištirti ar politikų naudojamas diskursas yra naudingas ar veikiau žalingas, siekiant tikslingai saugumizuoti kibernetinę erdvę.

2. Kibernetinės erdvės saugumo raida Lietuvoje

Lietuvos kibernetinio saugumo būklę galima skirti į tris periodus – nuo nepriklausomybės atkūrimo iki 2001; 2001 – 2014 m. ir nuo 2014-ųjų iki dabar. Tokią skirtį galima daryti dėl požiūrio, vyravusio į šią sritį. Lietuvai siekiant euroatlantinės integracijos ir narystės ES bei NATO, atitinkamai buvo vystomi ir gynybiniai pajėgumai. Pirmasis laiko intervalas žymi periodą, kurio metu į kibernetinį saugumą buvo žiūrima ribotai, nepaisant beprasidedančios kompiuterizacijos. Tik nuo XXI a. pradžios, kibernetiniam saugumui užėmus reikšmingą vietą ir NATO darbotvarkėje, Lietuvoje taip pat pradėta aktyviai kalbėti apie šios srities gynybą, keliant diskusijas ir pradedant plėsti pajėgumus. Antrojo periodo pabaiga galima laikyti maždaug 2014-uosius, po agresyvių Rusijos veiksmų prieš Ukrainą, pradėjus rimčiau galvoti ne tik apie konvencinį, bet energetinį, kibernetinį ir kitas saugumo rūšis. Nors šio darbo tikslas nėra apžvelgti Lietuvos kibernetinių pajėgų vystymosi raidą, šis procesas atskleidžia ir kaip apie šią sritį buvo mąstoma bėgant metams bei kaip prieita iki reikšmingų sprendimų XXI a. antrojo dešimtmečio viduryje ir kaip tai daro įtaką diskursui 2018 – 2023 metų laikotarpiu.

2.1 Pirmasis nepriklausomybės dešimtmetis

Pirmasis periodas žymi laikotarpį, kurio metu bene svarbiausi Lietuvos geopolitikos tikslai buvo tapimas NATO ir ES nare. Lietuvos Respublikos nacionalinio saugumo pagrindų įstatyme, priimtame 1996-ųjų pabaigoje ir numatančiame nacionalinio saugumo pagrindus daug dėmesio skiriama konvencinei gynybai ar NATO standartų atitikimui.[36] Visgi, nors jau anuomet buvo įžvelgiama energetinės nepriklausomybės ar Europinės geležinkelio vėžės svarba nacionaliniam saugumui, kibernetinei erdvei dėmesio beveik neskiriama.[37] Tokia situacija atitiko to laikmečio realijas – nors kompiuterizacija jau buvo prasidėjusi, apie kibernetinės erdvės apsaugą plačiai dar nebuvo svarstoma. NATO kibernetiniu saugumu rimčiau susidomėjo tik po 2002-ųjų, įtraukus šį aspektą į aljanso politinę darbotvarkę.[38] Iki tol strateginiuose Aljanso dokumentuose buvo tik trumpai užsimenama apie informacijos apsaugos standartus ir technologinį bei informacinį standartizavimą.[39]

Visgi, jau minėtame Nacionalinio saugumo pagrindų įstatyme trumpai užsimenama apie informacijos, ryšių sistemų ir techninių priemonių standartizavimą pagal NATO reikalavimus bei informacijos apsaugos sistemos kūrimą, kuri būtų integrali su NATO sistema.[40] Algirdas Orenius,

[36] Lietuvos Respublikos Seimas, Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas, Vilnius, 1996, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.34169?jfwid=wqwn5jq6k (žiūrėta 2023 m. balandžio 17 d.)
[37] *Ibid*.
[38] NATO, „Prague Summit Declaration“, Praha, 2002, pranešimas spaudai, https://www.nato.int/cps/en/natohq/official_texts_19552.htm (žiūrėta 2023 m. balandžio 17 d.)
[39] NATO, „Study on NATO Enlargement“, 1995, 62, 77, https://www.nato.int/cps/en/natohq/official_texts_24733.htm, (žiūrėta 2023 m. balandžio 17 d.)
[40] Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas, Ketvirtasis skirsnis, „Integravimosi į NATO priemonės“, (žiūrėta 2023 m. balandžio 17 d.)

tekste „1990–2002 m. Lietuvos krašto apsaugos politikos raidos analizė“ pastebi, kad tai buvo būtina sąlyga pagal Lietuvos ir NATO Individualios partnerystės programą (angl. *Individual Partnership Programme*), pagal kurią, greta oro gynybos pajėgumų plėtros, logistikos gerinimo ir kitų aspektų, Lietuva turėjo pasitempti ir „Vadovavimo, kontrolės, ryšių ir informacinės sistemos įdiegime.“[41] Nors dokumentuose tiesiogiai neužsimenama apie gynybinių pajėgumų kibernetinėje (informacinėje) erdvėje plėtrą, NATO standartų atitikimas bei „informacijos apsaugos sistemos kūrimas“ nurodo ir egzistuojantį saugumo aspektą. Visgi, nuoseklesnė prieiga matoma tik nuo 2001 m.

2.2 2001 – 2014 m.: kibernetinio saugumo atsiradimas politinėje darbotvarkėje

2001-ieji žymi iki tol bene didžiausią žingsnį nacionalinėje saugumo politikoje ir kibernetinės erdvės apsaugojime. Tų metų gruodžio 21-ąją Vyriausybė patvirtino nutarimą: „Dėl Informacijos technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo.“ Šiuo dokumentu buvo siekiama ne tik priartėti ES ar NATO standartų ar nustatyti saugos reikalavimus internetiniam verslui ir kompiuterių tinklams, bet ir stiprinti „svarbiausiųjų valstybės informacinių sistemų saugą.“[42] Strategijoje taip pat minima ir būtinybė atsižvelgti į tai, kad technologijos sparčiai vystysis, todėl nuo šio proceso neturėtų atsilikti ir saugos priemonės,[43] taip bent formaliai įtvirtinant ilgalaikį siekį apsaugoti kibernetinę erdvę. Kitais metais buvo žengtas dar vienas žingsnis – Seimas nutarė patvirtinti Vyriausybės pateiktą Nacionalinė saugumo strategiją.[44] Nors strategijoje vis dar dominuoja stojimo į NATO ir ES naratyvas, palyginti su 1996-ųjų dokumentu, (informacinis) kibernetinis dėmuo čia daug ryškesnis. Skyriuje „Pagrindiniai nacionalinio saugumo strategijos įgyvendinimo būdai ir priemonės“ atsiranda atskira skiltis informaciniam saugumui: „6.2.2. *Informacijos apsauga*.“ Atsižvelgiant į tarptautinius standartus, tobulinamas informacijos technologijų saugos teisinis reglamentavimas, stiprinama svarbiausių valstybės informacinių sistemų sauga, užtikrinama tinkama informacijos technologijų ir duomenų saugos priemonių įgyvendinimo kontrolė.“[45] Be to, taip pat akcentuojama ir nusikaltimų internetinėje erdvėje užkardymo ar duomenų nutekinimo prevencijos svarba.[46] Reikia paminėti ir tai, kad 2005-ųjų Nacionalinio saugumo strategijos redakcijoje

[41] Algirdas Orenius, „1990–2002 m. Lietuvos krašto apsaugos politikos raidos analizė“, *Viešoji politika ir administravimas*, Nr. 6 (2003), Lietuvos teisės universitetas, p. 84
[42] Lietuvos Respublikos Vyriausybė, Dėl Informacijos technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo, Vilnius, 2001, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.157225?jfwid=rivwzvpvg (žiūrėta 2023 m. balandžio 17 d.)
[43] *Ibid.*
[44] Lietuvos Respublikos Seimas, Dėl nacionalinio saugumo strategijos patvirtinimo, Vilnius, 2002, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.167925?jfwid=wqwn5jplo (žiūrėta 2023 m. balandžio 17 d.)
[45] *Ibid*., 6.2.2. skirsnis, (žiūrėta 2023 m. balandžio 17 d.)
[46] *Ibid*., 4.1.9; 6.1.4 skirsniai (žiūrėta 2023 m. balandžio 17 d.)

reikšmingų pokyčių dėl informacinio (kibernetinio) saugumo nėra – tiek grėsmės, tiek strategijos įgyvendinimo būdai ir priemonės išvardinti identiškai ankstesniam leidimui.[47]

Nors 2006-aisiais pasirodė nauja strategija, skirta užtikrinti saugą valstybės informacinėse sistemose, kaip pastebi Darius Štitilis ir Valdas Klišauskas, abi 2001-ųjų ir 2006 -ųjų strategijos buvo gana pasyvios teisinio reguliavimo prasme, nepaisant to, kad kibernetinis saugumas jau tuomet buvo matomas kaip vienas iš prioritetų.[48] Paskutinioji, 2011-ųjų strategija, skirta apibrėžti kibernetiniam saugumui iki pat 2019-ųjų turi ir aiškiai suformuluotus rodiklius, skirtus įvertinti atsakingų institucijų užduočių atlikimą bei apibrėžtą „Kritinės infrastruktūros“ sąvoką: „**Ypatingos svarbos informacinė infrastruktūra** – elektroninių ryšių tinklas, informacinė sistema ar informacinių sistemų grupė, kurioje įvykęs incidentas padaro ar gali padaryti didelę žalą nacionaliniam saugumui, šalies ūkiui ar visuomenės gerovei.“[49] Žvelgiant iš saugumizavimo teorijos perspektyvos, tokį apibrėžimą jau galima laikyti referentiniu objektu, būtinu normaliam valstybės funkcionavimui. Visgi, Štitilio ir Klišausko teigimu, nors 2001-2011 metais ir buvo daroma pažanga, visi dokumentai iki pat Kibernetinio saugumo įstatymo buvo nenuoseklūs ir nepilni.[50] Atsižvelgiant į tai, kad nors referentinis objektas dokumentuose egzistavo jau anuoment, sėkmingam saugumizavimui vis dar trūko priemonių (ar platformos joms) siūlymų bei aiškiai akcentuojamų grėsmių, todėl negalima teigti, kad šiuo laikotarpiu kibernetinė erdvė Lietuvoje buvo sėkmingai saugumizuota.

Kibernetinės erdvės saugumo Lietuvoje raida 1994-2014

Dokumentas	Kibernetinio (informacinio) saugumo akcentas
Lietuvos ir NATO individualios partnerystės programa, 1994	Vadovavimo, kontrolės ir ryšių sistemų diegimas.
Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas, 1996	Informacijos, ryšių ir technologijos apsaugos standartizavimas pagal NATO reikalavimus.
Informacijos technologijų saugos valstybinė strategija, 2001	Siekis gerinti „svarbiausiųjų valstybės sistemų“ apsaugą, neatsilikti nuo technologinio progreso.

[47] Lietuvos Respublikos Seimas, Dėl Seimo nutarimo "Dėl Nacionalinio saugumo strategijos patvirtinimo" priedo pakeitimo, Vilnius, 2005, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.249438 (žiūrėta 2023 m. balandžio 19 d.)
[48] Darius Štitilis, Valdas Klišauskas, „Aspets of cybersecurity: the case of legal regulation in Lithuania“, *Journal of security and sustainability issues*, Volume 5, No 1 (2015), p. 49
[49] Lietuvos Respublikos Vyriausybė, Dėl Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo", Vilnius, 2011, https://www.e-tar.lt/portal/lt/legalAct/TAR.1ABB945646B7 (žiūrėta 2023 m. balandžio 20 d.)
[50] Štitilis, Klišauskas, p. 49

Nacionalinė saugumo strategija, 2002	Gerinti „svarbiausiųjų valstybės sistemų“ apsaugą, tobulinti technologijų saugos teisinį reglamentavimą.
Nacionalinė saugumo strategija, 2005	Reikšmingų pokyčių, lyginant su 2002 metų dokumentu, nėra.
Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymas, 2006[51]	Pirmą kartą apibrėžiama „Kritinės infrastruktūros“ sąvoka, nurodanti svarbą nacionaliniam saugumui, šalies ūkiui ar visuomenės gerovei.
Elektroninės informacijos saugos (kibernetinio saugumo) plėtros programa, 2011	Reikšmingų pokyčių, lyginant su 2006 metų dokumentu, nėra.
Nacionalinė saugumo strategija, 2012[52]	Kibernetinis saugumas įvardinamas kaip vienas iš nacionalinių saugumo interesų, akcentuojama šios srities teisinio reglamentavimo svarba.

Šaltinis: sudaryta autoriaus, remiantis strateginių dokumentų ir „Aspets of cybersecurity: the case of legal regulation in Lithuania“ straipsnio duomenimis.

2.3 2014-ieji: sėkmingas kibernetinės erdvės saugumizavimas

Nors apie informacinį (kibernetinį) saugumą ar ryšių sistemų apsaugą buvo kalbama nuo 1996-ųjų, labiau sisteminga prieiga pasitelkta nuo 2006-ųjų, priėmus Elektroninių ryšių tinklų ir informacijos saugumo įstatymą, kuriame išsamiau apibrėžti ir saugotini objektai. Visgi, mokslininkų vertinimu net ir tai nebuvo pakankamas žingsnis. Tą rodo ir faktas, kad lietuviški internetiniai puslapiai tapo kibernetiniais taikiniais. 2012 metais DDoS (angl. *Distributed Denial of Service*) ataka įvykdyta prieš Lietuvos banką,[53] laikinai sutrikdant internetinės bankininkystės operacijų veikimą, o 2013-aisiais tokio paties tipo išpuolis įvykdytas prieš vieną iš didžiausių naujienų portalų šalyje delfi.lt.[54] Visgi, ne atakų faktas, o politikų reakcija po jų geriau atskleidžia šalies nepasiruošimą gintis

[51] Lietuvos Respublikos Vyriausybė, Nutarimas dėl Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepcijos patvirtinimo, Vilnius, 2006, https://www.e-tar.lt/acc/legalAct.html?documentId=TAR.522926ED3AA1 (žiūrėta 2023 m. balandžio 20 d.)

[52] Lietuvos Respublikos Seimas, Seimo NUTARIMO dėl Lietuvos Respublikos Seimo nutarimo "Dėl Nacionalinio saugumo strategijos patvirtinimo" pakeitimo PROJEKTAS + strategija, Vilnius, 2012, https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/TAIS.428241 (žiūrėta 2023 m. balandžio 24 d.)

[53] Lietuvos bankas, „Kibernetinėmis atakomis bandyta sutrikdyti Lietuvos banko paslaugų teikimą internetu“, pranešimas žiniasklaidai, 2012, https://www.lb.lt/lt/naujienos/kibernetinemis-atakomis-bandyta-sutrikdyti-lietuvos-banko-paslaugu-teikima-internetu (žiūrėta 2023 m. balandžio 24 d.)

[54] Eglė Samoškaitė, „Politikai: kibernetinės atakos prieš DELFI – atakos prieš valstybę“, LRT, https://www.lrt.lt/naujienos/lietuvoje/2/18644/politikai-kibernetines-atakos-pries-delfi-atakos-pries-valstybe (žiūrėta 2023 m. balandžio 24 d.)

nuo kibernetinių atakų. Tuometis Nacionalinio saugumo ir gynybos komiteto (NSGK) pirmininkas A. Paulauskas po atakos prieš delfi.lt sakė: „...valstybinės institucijos ir verslas turi rimtai suprasti, atsižvelgti ir finansuoti tas saugumo sistemas. Šiuo konkrečiu atveju negaliu atsakyti, ką daro CERT-LT, žinau, kad policija pradėjo tyrimą...“ bei „DELFI atvejis – kaip pavyzdys, ryškiausias, bet jeigu kalbėtume atvirai, tai tų puolimų yra buvę dar sunkesnių ir daug žalos pridariusių, tik tiek, kad mūsų institucijos tyli, nenori skelbtis.“[55] Toks neapibrėžtumas po kibernetinės atakos patvirtina ir Štitilio ir Klišausko mintį apie teisinio kibernetinės erdvės apsaugos reglamentavimo nenuoseklumą ir trūkumus.

Situacija iš esmės pasikeitė 2014-aisiais: NSGK pirmininko Artūro Paulausko teigimu šiandien karuose pasitelkiamos ne tik karinės, diplomatinės ar kitos priemonės, bet ir kibernetiniai išpuoliai, kuriomis siekiama destabilizuoti padėtį valstybėje, todėl kibernetinis saugumas turi tapti viena iš sudedamųjų krašto gynybos dalių.[56] Besikeičianti kibernetinio saugumo situacija, augantis incidentų skaitmeninėje erdvėje skaičius (A. Paulausko teigimu, 2013-aisiais jų fiksuota per 20 tūkstančių, 2014-aisiais – dar daugiau)[57] bei prastai iki tol reglamentuotas kibernetinės erdvės saugumas sudarė prielaidas saugumizuoti šią sritį. A. Palausko ir NSGK pastangas vainikavo metų pabaigoje priimtas Lietuvos Respublikos Kibernetinio saugumo įstatymas. Jame ne tik dar kartą išsamiai išdėstyta visa kibernetinio saugumo strategija, įskaitant saugotinus objektus, bet ir aiškus teisinis reguliavimas. Pagal įstatymą taip pat įkuriamos dvi naujos institucijos, skirtos tik kibernetinės erdvės saugojimui – jau minėtas NKSC bei Kibernetinio saugumo taryba (KST).[58]

Naujai įkurtam NKSC paskirtas funkcijas galima dėti į dvi atskiras kategorijas: ypatingos svarbos (kritinės) infrastruktūros apsauga ir darbas su visuomene. Į pirmąją kategoriją patenka tokios užduotys kaip kibernetinės saugumo strategijos nacionaliniu mastu vystymas bei implementavimas, kritinės infrastruktūros apsauga rengiant planus, stebint ir analizuojant kibernetinę erdvę ir kt. Tuo tarpu su visuomene dirbama edukuojant piliečius ir IT ekspertus kibernetinio saugumo klausimais, padedant organizacijoms, patyrusioms kibernetinę ataką ir kt.[59] KST, kurią sudaro verslo, mokslo, atstovai kritinės infrastruktūros valdytojai ir kiti asmenys, bei kuriai vadovauja KAM viceministras, teigia išvadas ir rekomendacijas, dėl kibernetinio saugumo stiprinimo, naujausių tendencijų ar galimo verslo, mokslo ir viešojo sektoriaus bendradarbiavimo šioje srityje.[60] Be šių dviejų įstaigų,

[55] *Ibid.*
[56] Lietuvos Respublikos Seimas, Seimo NSGK pirmininko A. Paulausko pranešimas: „Kibernetinė gynyba turi tapti krašto gynybos dalimi“, Vilnius, 2014, https://www3.lrs.lt/pls/inter/w5_show?p_r=618&p_d=147140&p_k=1 (žiūrėta 2023 m. balandžio 24 d.)
[57] Lietuvos Respublikos Seimas, A. Paulausko kalba Seimo vakarinio posėdžio Nr.203 metu, https://e-seimas.lrs.lt/portal/legalAct/lt/TAK/0f03aec0755f11e4b615a833d6e7da3d (žiūrėta 2023 m. balandžio 24 d.)
[58] Lietuvos Respublikos Seimas, Kibernetinio saugumo įstatymas, Vilnius, 2014, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee#part_cb4294571a7c40b080dac0a832505c40 (žiūrėta 2023 m. balandžio 24 d.)
[59] *Ibid*., 10 straipsnis (žiūrėta 2023 m. balandžio 24 d.)
[60] *Ibid*., 9 straipsnis (žiūrėta 2023 m. balandžio 24 d.)

Kibernetinio saugumo įstatyme atskiros funkcijos numatytos ir Vyriausybei, KAM, Vidaus reikalų ministerijai (VRM), Ryšių reguliavimo tarnybai (RRT), Valstybinei duomenų apsaugos inspekcijai (VDAI) bei policijai.

Kibernetinės erdvės apsauga buvo akcentuojama ir kituose dokumentuose. 2014-ųjų Valstybės saugumo departamento (VSD) paskelbtame Grėsmių nacionaliniam saugumui vertinime kibernetiniam saugumui skiriamas atskiras poskyris.[61] Svarbu paminėti, kad čia grėsmės matomos ne kaip potencialiai galinčios sukelti žalą kritinei infrastruktūrai – akcentuojamas šnipinėjimo ir galimo labai jautrių duomenų nutekėjimo aspektas. Nors kibernetinės grėsmės, akcentuojamas ataskaitoje, neaprėpia to, kas buvo įtraukta į Kibernetinio saugumo įstatymą (pvz., kritinė infrastruktūra), dokumente minimas aiškus grėsmės šaltinis – Rusija, o toks paminėjimas, žvelgiant iš teorinės perspektyvos, yra naudingas saugumizuojant. 2015-aisiais išėjusioje ataskaitoje taip pat plėtojamas šnipinėjimo naratyvas, tačiau čia taip pat paminima, kad Rusijos vykdoma veikla kibernetinėje erdvėje kelia pavojų ir kritinei Lietuvos infrastruktūrai.[62] Taigi, įstatymuose plėtojamas kibernetinio saugumo naratyvas bent dalinai atkartojamas ir pavojus šalies saugumui vertinančiuose dokumentuose.

Toks kibernetinės erdvės saugumo institucionalizavimas įstatymuose, aiškių **grėsmių** (šalies ūkiui, santvarkai ir kt.), **referentinio objekto** (kritinė infrastruktūra), **nepaprastųjų priemonių** (NKSC, KST įkūrimas ir kt.) artikuliavimas rodo, kad tuo metu kibernetinė erdvė buvo sėkmingai saugumizuota. Tą laikotarpį tyrusi ir 50 saugumizuojančių veikėjų pasisakymų išanalizavusi I. Juknevičiūtė, pastebi, kad prie to prisidėjo ir tuometinė šalies Prezidentė Dalia Grybauskaitė bei NSGK, viešajame diskurse prioretizavę kibernetinės erdvės saugumą.[63]

[61] Lietuvos Respublikos Valstybės saugumo departamentas, „Grėsmių nacionaliniam saugumui vertinimas“, Vilnius, 2014, https://www.vsd.lt/wp-content/uploads/2016/10/gresmes-2013.pdf (žiūrėta 2023 m. balandžio 24 d.)
[62] Lietuvos Respublikos Valstybės saugumo departamentas, „Grėsmių nacionaliniam saugumui vertinimas“, Vilnius, 2015, https://www.vsd.lt/wp-content/uploads/2016/10/Gresmiu-vertinimas-2014.pdf (žiūrėta 2023 m. balandžio 24 d.)
[63] Juknevičiūtė, p. 40

3. Kibernetinės erdvės saugumizavimas po Kibernetinio saugumo įstatymo priėmimo

Kibernetinės erdvės grėsmės, saugumizavus šią sritį 2013-2015 metais, niekur nedingo – Rusija, o vėliau ir Kinija (VSD saugumo ataskaitose kaip kibernetinė grėsmė figūruoja nuo maždaug 2016 metų) lėmė tolimesnį saugumizavimo procesą. Tai lėmė, kad tiek dokumentuose, tiek viešojoje erdvėje kibernetinės erdvės saugumas buvo eskaluojamas ir toliau. Prieš pereinant prie saugumizuojančių veikėjų diskurso tyrimo ir tolimesnių darbo pradžioje išsikeltų tikslų įgyvendinimo, būtina apžvelgti ir *kaip* kibernetinė erdvė saugumizuojama strateginiuose ir kituose dokumentuose (referentiniai objektai, grėsmių šaltiniai, priemonės ir kt.). Tai leis išsikelti tyrimui būtinus kriterijus, kuriais remiantis bus galima lyginti politikų ir pareigūnų naudojamo diskurso atitikimą ar neatitikimą su minėtais dokumentais.

3.1 Laikotarpis iki 2018 metų (2015-2017)

3.1.1 VSD, NKSC ir CERT ataskaitos

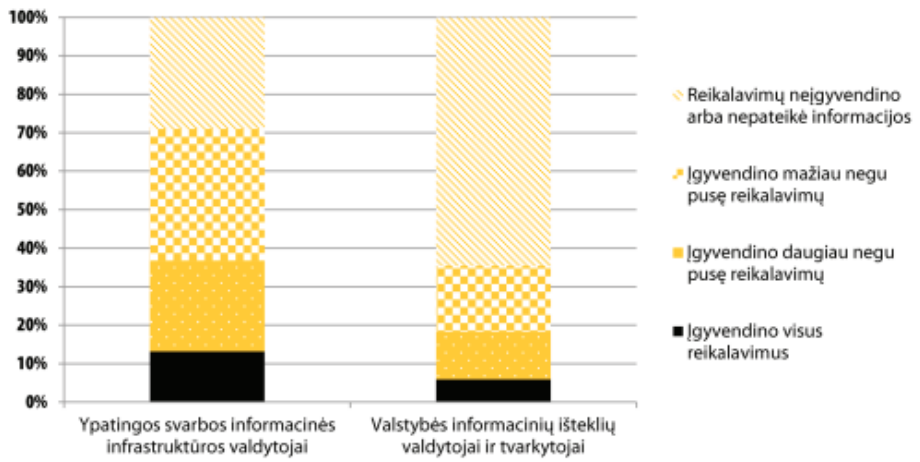
Laikotarpiu iki 2018-ųjų taip pat pasirodė keletas dokumentų, reikšmingai prisidėjusių prie kibernetinio saugumo strategijos ir po 2018-ųjų. Visų pirma, Rusijos ir Kinijos keliamų kibernetinių grėsmių naratyvas ir toliau buvo tęsiamas VSD ataskaitose. 2016-ųjų ataskaitoje daug dėmesio skiriama su Lietuvai priešiškai nusiteikusiomis valstybėmis siejamomis kibernetinėmis grupuotėmis. VSD ataskaitoje akcentuojamas ne tik kibernetinis šnipinėjimas, bet ir bandymas pasinaudoti valstybės institucijų kibernetiniais pažeidžiamumais, įskaitant ir tuos, randamus kritinėje infrastruktūroje, taip sukuriant galimybę reikšmingai paveikti žmonių kasdienybę ar sumenkinti šalies gynybinius pajėgumus. Be to, užsimenama ir apie galimybę sukelti neatitaisoma žalą šalies IT infrastruktūrai, atakuojant subjektus, nesirūpinančius kibernetiniu saugumu (tiek verslo, tiek valstybiniai taikiniai) nors bent tuo metu tokia galimybė buvo vertinama kaip maža.[64]

Tuo tarpu 2017-ųjų ataskaitoje jau minimi konkretūs pavyzdžiai, kai Lietuvos institucijos (KAM, Seimas, Prezidentūra, VSD ir kitos) bei žiniasklaida („Delfi“, „Alfa media“) patyrė didelio masto kibernetinius išpuolius, kurių metu siekta apriboti šalies informacinę erdvę. Ataskaitoje taip pat paminima, kad šią strategija Rusija jau taikė Sakartvele (2008 m.) ir Ukrainoje (2014 m.), tačiau prieš Lietuvą įvykdytos atakos veikiau buvo atsakingų institucijų gebėjimo reaguoti į tokius įvykius patikrinimas ir infrastruktūros atsparumo vertinimas. Be to, ataskaitoje pastebima, kad kritinė infrastruktūra vis dažniau tampa kibernetinių atakų taikiniu – minimos Ukrainos Ivano Frankivsko

[64] Lietuvos Respublikos Valstybės saugumo departamentas, „Grėsmių nacionaliniam saugumui vertinimas“, Vilnius, 2016, p. 25-28 https://www.vsd.lt/wp-content/uploads/2017/03/bendras-2015-gresmiu-vertinimas.pdf (žiūrėta 2023 m. balandžio 26 d.)

(2015) ir Kyjivo (2016) elektros jėgaines, prieš kurias buvo įvykdytos dvi kibernetinės atakos, sutrikdžiusios elektros tiekimą daliai Ukrainos gyventojų.[65] 2016 ir 2017 metų ataskaitose taip pat yra pirmosios, kuriose aiškiai komunikuojama apie potencialią Rusijos keliamą žalą kritinei infrastruktūrai, taip išlaikant tą pačią saugumo liniją, jau matomą kituose strateginiuose dokumentuose.

Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys (CERT-LT) 2017-aisiais užfiksavo 54 414 incidentų pagal pranešimus, gautus iš Lietuvos elektroninių ryšių paslaugų teikėjų, užsienio CERT tarnybų, atliekančių tarptautinius incidentų tyrimus, ir iš Lietuvos interneto naudotojų.[66] Visgi, priešingai nei VSD ataskaitose, čia daugiausiai dėmesio skiriama išsamiam grėsmių, kylančių eiliniams gyventojams ir verslui aprašymui, tiesa, trumpai užsimenama ir apie Kibernetinio saugumo įstatymo pakeitimus, tačiau atskirai kritinė infrastruktūra nėra saugumizuojama.[67] 2017-aisiais pasirodė ir pirmoji Nacionalinio kibernetinio saugumo būklės ataskaita, parengta NKSC. Panašiai kaip ir CERT-LT parengtoje apžvalgoje, čia daug dėmesio skiriama grėsmių tipams, per pastaruosius metus įvykusiems incidentams ir kt. Vis dėlto, NKSC parengtame dokumente daugiau dėmesio skiriama ypatingos svaros informacinei infrastruktūrai. Daug analizės skiriama kritinės infrastruktūros saugumo atitikimui teisės aktams, potencialioms grėsmėms bei pasiruošimui apsaugoti šią sritį.[68]



Šaltinis: Nacionalinis kibernetinio saugumo centras, „2017 Metų nacionalinio kibernetinio saugumo būklės ataskaita“, p. 36

[65] Lietuvos Respublikos Valstybės saugumo departamentas, „Grėsmių nacionaliniam saugumui vertinimas“, Vilnius, 2017, p. 27-28 https://www.vsd.lt/wp-content/uploads/2017/03/2016-gr%C4%97smi%C5%B3-vertinimas.pdf (žiūrėta 2023 m. balandžio 26 d.)
[66] CERT-LT, „2017 Metų veiklos ataskaita“, 2017, p. 1, https://www.nksc.lt/doc/2017.pdf (žiūrėta 2023 m. balandžio 26 d.)
[67] *Ibid*., p. 1-10
[68] Nacionalinis kibernetinio saugumo centras, „2017 Metų nacionalinio kibernetinio saugumo būklės ataskaita“, 2017, https://www.nksc.lt/doc/NKSC_ataskaita_2017_lt.pdf (žiūrėta 2023 m. balandžio 26 d.)

3.1.2 Baltoji knyga

Lietuvos gynybos baltojoje knygoje, apibrėžiančioje Lietuvos gynybos politikos kryptis, pokyčius ir naujoves Lietuvos kariuomenėje taip pat minimas ir kibernetinis saugumas. 2017 metais išleistame dokumente daugiausiai dėmesio skiriama kritinei infrastruktūrai, krašto apsaugos sistemai kylančioms grėsmėms, apžvelgiamas kibernetinio saugumo valdymo institucinis modelis bei reagavimo į pavojus planas. Be to, pabrėžiama ir kritinės infrastruktūros apsaugos didinimo svarba bei kariuomenės pasirengimas kariauti kibernetinėje erdvėje, stiprinant pajėgumus dalyvaujant vietinėse bei tarptautinėse pratybose ar konsultuojantis su NATO partneriais.[69]

3.1.3 2017 metų Nacionalinė saugumo strategija

2017-ųjų metų Nacionalinėje saugumo strategijoje nemažai dėmesio skiriama kibernetiniam saugumui. Kibernetinės grėsmės apibūdinamos kaip veiksmai kibernetinėje erdvėje, kuriais siekiama sutrikdyti ypatingos svarbos informacinių infrastruktūrų funkcionavimą, paveikti nacionaliniam saugumui svarbių valstybės institucijų ir ūkio sektorių veiklą ar išgauti neviešą informaciją, taip pakenkiant šalies ar piliečių saugumui.[70] Strategijoje taip pat akcentuojama bendradarbiavimo su NATO ir ES institucijomis svarba, ypatingos svarbos infrastruktūros apsauga, visuomenės švietimas bei visai kibernetinei erdvei keliama Rusijos grėsmė.[71] Toks kibernetinės erdvės saugumo apibrėžimas, pateikiamas išsamus veiksmų planas didele dalimi atitinka tiek Kibernetinio saugumo įstatyme, tiek VSD ir NKSC ir ataskaitose deklaruojamus siekius, taip veiksmingai prisidedant prie srities saugumizavimo.

3.1.4 Lietuvos Respublikos Karinė strategija ir Lietuvos karinė doktrina

Kiek kitokia situacija matoma Lietuvos karinėje strategijoje ir doktrinoje. Abiejuose strateginiuose dokumentuose, reglamentuojančiuose svarbiausius Lietuvos kariuomenės ir krašto gynybos aspektus minimas ir kibernetinio saugumo dėmuo, tačiau tai daroma gana ribotai. Karinėje doktrinoje teigiama, kad kibernetinio saugumo pajėgumų didinimas yra laikomas prioritetu:[72] ši formuluotė remiasi į įsitikinimą, kad kibernetinės erdvė ateityje taps prioritetine, svarba užgožtama ir konvencines pajėgas.[73] Nepaisant to, nors kibernetinė erdvė tekste paminima dar keletą kartų, nedetalizuojama kaip konkrečiai reikėtų stiprinti kibernetinę erdvę ar kokius objektus reikėtų saugoti. Tuo tarpu Karinėje strategijoje teigiama, kad augant priklausomybei nuo technologijų, neišvengiamai

[69] Lietuvos Respublikos Krašto apsaugos ministerija, „Lietuvos gynybos politikos baltoji knyga“, Vilnius, 2017, p. 55-58 https://kam.lt/wp-content/uploads/2022/03/Baltoji-knyga-2017.pdf (žiūrėta 2023 m. balandžio 26 d.)
[70] Lietuvos Respublikos Seimas, Dėl Lietuvos Respublikos Seimo 2002 m. gegužės 28 d. nutarimo Nr. IX-907 „Dėl Nacionalinio saugumo strategijos patvirtinimo“ pakeitimo, Vilnius, 2017, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/4c80a722e2fa11e6be918a531b2126ab (žiūrėta 2023 m. balandžio 26 d.)
[71] *Ibid.*
[72] Lietuvos Respublikos Krašto apsaugos ministerija, „Lietuvos karinė doktrina“, Vilnius, 2016, 2.3 Saugumo ir gynybos užtikrinimas, 209, https://www.kariuomene.lt/data/public/uploads/2021/03/lkd-2016_patalpinta-svetainese-6.pdf (žiūrėta 2023 m. balandžio 26 d.)
[73] *Ibid*., 4.6 Kariavimo perspektyva, 484

augs ir grėsmės nacionaliniam saugumui, o konvencinio karinio konflikto metu būtų intensyviai naudojamos ir kibernetinės priemonės. [74] Tačiau šiame dokumente taip pat nedetalizuojama ką ir kaip reikėtų saugoti – apsiribojama faktų konstatavimu, be gilesnės analizės.

Atsižvelgiant į bene svarbiausių Lietuvos gynybos dokumentų turinį, galima daryti išvadą, kad čia kibernetinė erdvė ir jos saugumas savo svarba vis dar nusileidžia konvencinėms pajėgoms. Neišsamūs šios srities paminėjimai neprisideda prie sėkmingo saugumizavimo, nors trumpais paminėjimais ir bandoma parodyti šios srities svarbą, detalesnių planų ar koncepcijos trūkumas (saugotini objektai, grėsmės šaltinis) neatitinka pagal teoriją sudarytų sėkmingo saugumizavimo kriterijų. Nepaisant to, VSD, NKSC, CERT-LT ataskaitos, 2017-ųjų Nacionalinė saugumo strategija bei baltoji knyga leidžia papildyti tyrimą reikšmingais duomenimis.

3.2 Kibernetinės erdvės saugumizavimas dokumentuose 2018-2023 metais

3.2.1 VSD, NKSC ataskaitos

Prieš VSD ir NKSC ataskaitų analizę reikėtų pabrėžti, kad nors tai ir nėra teisiškai įpareigojantys dokumentai, tokie kaip strategijos ar teisės aktai, pastaruosiuose, kaip parodys vėlesni tyrimo skyriai, nemaža dalimi atsispiriama nuo ataskaitų turinio (tiek įvardinant grėsmes, tiek saugotinus objektus ar galimas priemones). Todėl VSD ir NKSC ataskaitų analizė pateikiama šioje tyrimo dalyje. Šiuo laikotarpiu paskelbtose VSD ataskaitose dominuoja keli ryškūs kibernetinio saugumo naratyvai. 2019 metų ataskaitoje pabrėžiamos Rusijos pastangos toliau vystyti puolamuosius kibernetinius pajėgumus bei ribotas Vakarų valstybių atsakas į šios valstybės vykdomus išpuolius ir šnipinėjimą, darant išvadą, kad nepakankamas reagavimas į agresyvius veiksmus skatina tęsti šią veiklą.[75] Taip pat, minima ir grėsmė kritinei infrastruktūrai, pasireiškianti ne tik per tiesioginę žalą, bet ir šnipinėjimą, siekiant gauti prieigą prie ypatingos svarbos sistemų, valdančių tokias funkcijas kaip vandens ar elektros energijos tiekimas, eismo reguliavimas ir kt.[76] Įdomu ir tai, kad 2018-ųjų metų ataskaitoje įžvelgiama ir grėsmė būsimiems rinkimams – pasitelkiant Prancūzijos pavyzdį, kai su Rusija siejama grupuotė nutekino kandidato į Prancūzijos prezidentus Emmanuelio Macrono rinkimų kampanijos laiškus, daroma prognozė, kad panaši taktika gali būti taikoma ir Lietuvoje.[77]

[74] Lietuvos Respublikos Krašto apsaugos ministerija, Lietuvos Respublikos Karinė strategija, Vilnius 2016, p. 5, https://kam.lt/wp-content/uploads/2022/03/karine-strategija-LT-2016.pdf (žiūrėta 2023 m. balandžio 26 d.)
[75] Lietuvos Respublikos Valstybės saugumo departamentas, „Grėsmių nacionaliniam saugumui vertinimas“, Vilnius, 2019 p. 35 https://www.vsd.lt/wp-content/uploads/2019/02/2019-Gresmes-internetui-LT.pdf (žiūrėta 2023 m. gegužės 2 d.)
[76] *Ibid., p. 37*
[77] Lietuvos Respublikos Valstybės saugumo departamentas, „Grėsmių nacionaliniam saugumui vertinimas“, Vilnius, 2018 p. 34-35 https://www.vsd.lt/wp-content/uploads/2018/03/LTU.pdf (žiūrėta 2023 m. gegužės 2 d.)

2020-aisiais, prasidėjus COVID-19 pandemijai ir įvedus fizinių kontaktų ir kitus ribojimus, dar daugiau kasdienio piliečių ir valstybės gyvenimo aspektų persikėlė į internetą. VSD teigimu, prie to prisitaikė ir Rusija, pastebint, kad įvedus ribojimus, sumažėjo fizinės žvalgybos mastai, tačiau tokios veiklos apraiškų skaičius labai padidėjo kibernetinėje erdvėje.[78] Be to, įtariama, kad su Rusija susijusios hakerių grupuotės įvykdė eilę kibernetinių išpuolių prieš kritinę infrastruktūrą (energetikos, sveikatos apsaugos sektorius), švietimo įstaigas (didžiąją dalį 2020-ųjų mokymo procesas vyko nuotoliniu būdu) bei aukščiausias šalies saugumą ir užsienio politiką vykdančias ir užtikrinančias institucijas.[79] Pastebimas ir bendras, prieš sveikatos apsaugos įstaigas vykdomų, kibernetinių atakų skaičiaus augimas, siekiant priversti jų valdytojus sumokėti išpirką už antpuolio metu užšifruojamus duomenis. Neatmestina, kad tokias atakas organizuoja su priešiškomis šalimis siejamos grupuotės.[80] Visose ataskaitose pagrindine grėsme skaitmeninei erdvei ir toliau įvardinama Rusija, tačiau prasidėjus kalboms apie 5G diegimą, Lietuvoje atidarius Taivano atstovybę ir išstojus iš 17+1 formato, išryškėjo ir Kinijos grėsmė.[81]

Panašūs naratyvai vystomi ir NKSC rengiamose apžvalgose – Rusija ir Kinija pateikiamos kaip labiausiai Lietuvos kibernetinę erdvę žvalgančios valstybės (atitinkamai 17% ir 13% fiksuotų elektroninės žvalgybos atvejų), o daugiausiai dėmesio susilaukė ypatingos svarbos objektai krašto apsaugos, energetikos ir kituose sektoriuose.[82] Visgi, NKSC ataskaitose daug dėmesio skiriama ne tik grėsmėms, bet ir veiksmams, būtiniems nuo jų apsisaugoti. Pavyzdžiui 2020-aisiais NKSC specialistai organizavimo bazinius vienos dienos kibernetinio saugumo mokymus viešųjų įstaigų darbuotojams.[83] Tuo tarpu apibendrindami kibernetinio saugumo būklę, NKSC specialistai ragino kurti „sektorinius kibernetinių incidentų valdymo centrus“, padėsiančius atsakyti į vis išmanesnius kibernetinius antpuolius.[84] Vis dėlto, daugiausiai dėmesio buvo skiriama kritinės infrastruktūros apsaugai – ataskaitoje, apžvelgiančioje 2021-2022 metus, akcentuojamas nepatikimos programinės įrangos valstybės institucijose ir nacionaliniam saugumui svarbiuose sektoriuose nenaudojimas, įskaitant ir 5G technologijas iš nepatikimų tiekėjų [Kinijos įmonių].[85] Vertindami ypatingos svarbos informacinės struktūros (YSII) atitikimą kibernetinio saugumo reikalavimais, NKSC specialistai

[78] Lietuvos Respublikos Valstybės saugumo departamentas, „Grėsmių nacionaliniam saugumui vertinimas“, Vilnius, 2021 p. 10 https://www.vsd.lt/wp-content/uploads/2021/03/2021-LT-el_.pdf (žiūrėta 2023 m. gegužės 2 d.)
[79] *Ibid*., p. 45
[80] *Ibid*., p. 48
[81] Lietuvos Respublikos Valstybės saugumo departamentas, „Grėsmių nacionaliniam saugumui vertinimas“, Vilnius, 2022 p. 34 https://www.vsd.lt/wp-content/uploads/2022/04/LT-el-_.pdf (žiūrėta 2023 m. gegužės 2 d.)
[82] Nacionalinis kibernetinio saugumo centras, „2018 Metų nacionalinio kibernetinio saugumo būklės ataskaita“, 2018, p. 30, https://www.nksc.lt/doc/NKSC_ataskaita_2018.pdf (žiūrėta 2023 m. gegužės 2 d.)
[83] Nacionalinis kibernetinio saugumo centras, „2021 Metų nacionalinio kibernetinio saugumo būklės ataskaita“, 2021, p. 56 https://www.nksc.lt/doc/Nacionaline-kibernetinio-saugumo-ataskaita-2021.pdf (žiūrėta 2023 m. gegužės 5 d.)
[84] *Ibid*., p. 50
[85] Nacionalinis kibernetinio saugumo centras, „Svarbiausia Lietuvos kibernetinio saugumo būklės statistika ir tendencijos, 2021 m. – 2022 m. I ketv.“, 2021, p. 14, https://www.nksc.lt/doc/Svarbiausia-Lietuvos-kibernetinio-saugumo-bukles-statistika-ir-tendencijos-2021-2022-I-ketv.pdf (žiūrėta 2023 m. gegužės 5 d.)

nustatė, kad nors ir yra judama didesnio saugumo link, reikalavimai dažnai įgyvendinami formaliai, sporadiškai, taip apsunkinant kibernetinių incidentų aptikimą ir užtikrinant kritinės infrastruktūros veiklos tęstinumą incidentų atveju.[86] Atsižvelgiant į NKSC teiginius apie YSII valdytojų vengimą pasirūpinti, kad jų valdomų įstaigų saugumas atitiktų keliamus reikalavimus, galima daryti išvadą, kad nors saugumizavimas vyksta, auditorija ji priima nenoriai ar bent nepakankamai, kad imtųsi aktyvių veiksmų. Saugumizavimo efektyvumas šiai auditorijai (kritinės svarbos institucijų valdytojams) nėra šio darbo tikslas, tačiau toks tyrimas galėtų būti prasmingas, siekiant įvertinti pasirinktų priemonių ir komunikacijos veiksmingumą. Visgi, apibendrinant, aptarto laikotarpio metu pateiktose NKSC ir VSD ataskaitos tęsiama kibernetinės erdvės saugumizavimo linija – aiškiai formuluojamos grėsmės (Rusijos, Kinijos šnipinėjimas, siekiant gauti prieigą prie kritinės infrastruktūros sistemų ar kitoks priemonės siekiant joms pakenkti), akcentuojama tokių sistemų apsaugos svarba bei siūlomos ar jau įgyvendinamos nepaprastosios priemonės – mokymai darbuotojams, sistemų auditai, nukreipiantys resursus į konkrečias sritis.

3.2.2 Nacionalinė kibernetinio saugumo strategija

Nacionalinė kibernetinio saugumo strategija, patvirtinta Vyriausybės 2018-aisiais penkerių metų laikotarpiui, o jos pagrindinė užduotis: „efektyviai ir laiku identifikuojant kibernetinius incidentus, užkertant kelią jų atsiradimui ir plitimui, valdant kibernetinių incidentų sukeltas pasekmes užtikrinti galimybę Lietuvos visuomenei saugiai naudotis informacinių ir ryšių technologijų teikiamomis galimybėmis.“[87] Tuometis KAM ministras Raimondas Karoblis, priimant strategiją teigė, kad dabartinė (Elektroninės informacijos saugos (kibernetinio saugumo) plėtros programa), priimta 2011 metais nebeatitinka šiandienos realijų ir kibernetinio saugumo iššūkių.[88] Strategijoje daug dėmesio skiriama visos valstybės kibernetinio saugumo užtikrinimui ir pajėgumų plėtrai (pirmasis tikslas), taip pat inovacijoms (trečiasis tikslas), verslo ir privataus sektoriaus bendradarbiavimui (ketvirtasis tikslas) bei tarptautinei partnerystei (penktasis tikslas). Antrasis tikslas apibrėžia nusikaltimų internete užkardymą.[89]

Apie kritinės infrastruktūros apsaugą bene daugiausiai kalbama pirmajame tiksle, kuris remiasi VSD, NKSC ir Antrojo operatyvinio tarnybų departamento prie KAM (AOTD) ataskaitomis. Čia pastebima, kad Lietuva nuolat susiduria su atakomis prieš šalies ypatingos svarbos informacinę

[86] Nacionalinis kibernetinio saugumo centras, „2019 Metų nacionalinio kibernetinio saugumo būklės ataskaita“, 2019, p. 54 https://www.nksc.lt/doc/Nacionalinio_kibernetinio_saugumo_bukles_ataskaita_2019.pdf (žiūrėta 2023 m. gegužės 5 d.)

[87] Lietuvos Respublikos Krašto apsaugos ministerija, „Nacionalinė kibernetinio saugumo strategija“, 2017, p. 4, (žiūrėta 2023 m. gegužės 5 d.)

[88] 15min.lt, „Vyriausybė patvirtino kibernetinio saugumo strategiją“, žiūrėta 2023 m. gegužės 5 d., https://www.15min.lt/verslas/naujiena/mokslas-it/vyriausybe-patvirtino-lietuvos-kibernetinio-saugumo-strategija-1290-1014484

[89] Nacionalinė kibernetinio saugumo strategija, p. 4

infrastruktūrą, todėl atsižvelgiant į tai, būtina stiprinti valstybės kibernetinius pajėgumus, didinti jų efektyvumą skatinti nacionalines ir tarptautines pratybas ir kurti sisteminį požiūrį į šią sritį.[90] Panašios užduotys keliamos ir trečiame, ketvirtame ir penktame tiksluose – pripažįstama, kad viešasis sektorius nėra pajėgus savarankiškai reaguoti į visas kibernetines grėsmes, todėl būtina siekti glaudesnio bendradarbiavimo su privačiu sektoriumi, skatinti mokslą ir inovacijas bei plėtoti partnerystę su ES, NATO šalimis, išskiriant JAV, kaip pagrindinę dvišalę partnerę.[91]

Strategijoje tęsiama dar Kibernetinio saugumo įstatyme įprasminta linija. Ir toliau akcentuojama kritinės infrastruktūros apsaugos svarba, ir egzistuojančios grėsmės, išryškintos remiantis VSD ir kitų institucijų ataskaitomis, be to suformuluojamas ir aiškus planas, skirtas grėsmėms užkirsti, kuriame galima rasti ir tokių priemonių kaip kibernetinio saugumo pratybas, iš esmės atitinkančios Buzan ir kolegų suformuluotus „nepaprastųjų priemonių“ kriterijus.

3.2.3 Teisės aktai

Kartu su 2018-ųjų kibernetinio saugumo strategija pasirodė ir teisės aktas, reglamentuojantis „Ypatingos svarbos informacinės struktūros“ identifikavimą. Dokumente apibrėžiama „Ypatingos svarbos paslaugos“ sąvoka, nurodanti, kad tai „paslauga, kurios neveikimas ar veikimo sutrikimas padarytų didelį neigiamą poveikį nacionaliniam saugumui, šalies ūkiui, valstybės ar visuomenės interesams.[92] Teisės akte taip pat detalizuojami ir konkretūs ūkio sektoriai (energetikos, transporto, finansų, sveikatos apsaugos ir kt.) bei paslaugos (centralizuotas šildymas, pervežimai geležinkeliais, ambulatorinis gydymas ir kt.), patenkantis į ypatingos svarbos infrastruktūros apibrėžimą.[93] Taip gerokai praplečiamas ir potencialių referentinių objektų sąrašas, kuriems kyla kibernetinės grėsmės. Kaip pastebi kibernetinio saugumo ekspertas, Dr. Tomas Jakštas, „...dėl didėjančios skaitmenizacijos ir automatizacijos, ypatingos svarbos sektoriai tampa vis labiau pažeidžiami kibernetinėmis atakomis.“ Mokslininkas taip pat akcentuoja, kad labai svarbu suprasti ką ir kodėl kibernetinėje erdvėje reikia saugoti labiausiai, nes tik taip galima pasiruošti potencialioms plataus masto krizėms, atsirandančioms dėl kibernetinių atakų.[94]

[90] *Ibid.,* p. 7-10
[91] *Ibid.,* p. 15, 17, 18-19
[92] Lietuvos Respublikos Vyriausybė, Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo, Vilnius, 2018, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr (žiūrėta 2023 m. gegužės 5 d.)
[93] *Ibid.*.
[94] NRD Cyber Security, „Ypatingos svarbos infrastruktūros apsauga nuo kibernetinių grėsmių: ką turime žinoti“, vz.lt, žiūrėta 2023 m. gegužės 5 d., https://www.vz.lt/verslo-sprendimai/2020/10/29/ypatingos-svarbos-infrastrukturos-apsauga-nuo-kibernetiniu-gresmiu-ka-turime-zinoti#ixzz80rJKHDIV

3.2.4 Nacionalinė saugumo strategija

Nacionalinėje saugumo strategijoje, Seimo patvirtintoje 2021-ųjų pabaigoje, kibernetinės erdvės naratyvas iš esmės atkartoja sutinkamą Nacionalinėje kibernetinio saugumo strategijoje bei NKSC pateikiamuose grėsmių vertinimuose. Strategijoje akcentuojama bendradarbiavimo su NATO, ES svarba, dvišalė partnerystė su JAV, mokslo inovacijų skatinimas, bendradarbiavimas su privataus sektoriaus atstovais. Tiesa, ypatingos svarbos (kritinė) infrastruktūra kibernetinio saugumo kontekste paminima tik kartą, akcentuojant būtinybę užtikrinti, kad čia būtų naudojama tik patikimų gamintojų tiekiama įranga, siekiant užtikrinti aukščiausius kibernetinio saugumo standartus.[95] Atsižvelgiant į dokumento turinį, galima daryti išvadą, kad kibernetinio saugumo srityje atsiranda nusistovėjimas – tiek grėsmės, tiek referentiniai objektai ar priemonės, kurių reikia imtis jiems apsaugoti kartojasi. Galima teigti, kad taip užtikrinamas saugumizavimo tęstinumas, galimai rodantis ir tai, kad pats procesas jau yra išdirbtas bei įsitvirtinęs.

3.2.5 Saugumizavimo dokumentose apibendrinimas

Aptartu laikotarpiu į kibernetinės erdvės saugumizavimą buvo įnešta daug naujovių, o pati strategijai, kaip rodo vėliausi dokumentai, pradeda nusistovėti. Remiantis VSD, NKSC ir kitų institucijų teikiamomis įžvalgomis (kurios nuolat atkartojamos ir teisės aktuose bei strategijose), buvo aiškiai apibrėžtos grėsmės, kylančios šalies kibernetinei sistemai – programišių grupuotės, siejamos su Rusija, pačios Rusijos žvalgybos institucijos, šnipinėjimas, nepatikimų technologijų, ateinančių daugiausiai iš Kinijos (5G), skvarba į kritinę ir kitą infrastruktūra ir kt. Taip pat, aiškiai įvardinami referentiniai objektai, kolektyviai įvardinami „kritinės infrastruktūros“ sąvoka – energetikos, sveikatos apsaugos, nacionalinio saugumo ir kiti sektoriai, būtini užtikrinti normalų visuomenės ir valstybės funkcionavimą, įskaitant tokias paslaugas kaip elektros ar šildymo tiekimas, gydymas, krašto apsauga ir kt. Be to, ypatingai Nacionalinėje kibernetinio saugumo strategijoje daug dėmesio skiriama priemonių diegimui, skirtų apsaugoti minėtus referentinius objektus – kibernetinio saugumo pratybos, privalomų kriterijų institucijoms suformulavimas, darbuotojų mokymai ir kt. 3 lentelėje pateikiama apibendrinamoji kibernetinės erdvės saugumizavimo dokumentuose 2015 - 2023 metais analizė. Remiantis šiais duomenimis, kaip atskaitos tašku, kitoje tyrimo dalyje bus atliekamas politikų diskurso ir dokumentų palyginimas.

[95] Lietuvos Respublikos Seimas, Dėl Nacionalinio saugumo strategijos patvirtinimo, Vilnius, 2021, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.167925/asr (žiūrėta 2023 m. gegužės 5 d.)

3 Lentelė. Kibernetinės erdvės saugumizavimas dokumentuose 2015 - 2023 metais

Kriterijus	Paaiškinimas
Ar saugumizuojamas objektas yra referentinis?	Dokumentuose saugumizuojami objektai, būtini visuomenei ir valstybei – energijos tiekimas, komunikacijos, sveikatos apsauga, krašto gynyba ir kt. laikytini referentiniais.
Ar siūlomos nepaprastosios priemonės objektui apsaugoti?	Siūlomos priemonės, tokios kaip kibernetinio saugumo pratybos, masiniai darbuotojų mokymai, sektorinių kibernetinio saugumo centrų kūrimas yra visuomenės išteklių alokavimas į specifinę sritį, atitinkantis ir saugumizavimo teoretikų iškeltą kriterijų nepaprastųjų priemonių įvardinimui.
Ar minimas aiškus grėsmės šaltinis?	Dokumentuose, ypatingai VSD ir NKSC ataskaitose aiškiai įvardinami grėsmės Lietuvos kibernetiniui saugumui šaltiniai – kibernetinės grupuotės, siejamos priešiškomis šalimis, šių šalių specialiosios tarnybos, nepatikimų technologijų skvarba.
Ar saugumizuojant naudojamas radikalesnis diskursas (kibernetinės pražūties naratyvas), ar laikomasi nuosaikesnių scenarijų?	VSD ir NKSC ataskaitose, pateiktose minėtu laikotarpiu galima įžvelgti „kibernetinės pražūties“ naratyvus – teigiama, kad sėkmingos atakos prieš šalies kritinę infrastruktūrą gali sutrikdyti gyvybiškai svarbias komunikacijas – elektros, šildymo tiekimą, taip pat sveikatos apsaugos sistemą ar pakenkti konvencinei krašto gynybai, paveikiant transporto sektorių.

Šaltinis: sudaryta autoriaus, remiantis 2015 – 2023 metais išleistų VSD, NKSC ataskaitų ir tuo pačiu laikotarpiu priimtų teisės aktų duomenimis.

Reikėtų pabrėžti ir tai, kad toks įdirbis atsispindi ir tarptautiniu mastu. Tarptautinės telekomunikacijų sąjungos rengiamame „Globalaus kibernetinio saugumo indekse“ Lietuva užima

labai aukštą 6-ąją vietą, surinkusi 97.93 taško iš 100 galimu.[96] Indeksas matuojamas įvertinant valstybių užtikrinamas teisines, technines, organizacines ir korporacines priemones bei pajėgumų vystymą, matuojantį informacinių kampanijų, edukavimo ir kitų aspektų padengimą.[97] Lietuva maksimalų balų skaičių (20 kiekvienai kategorijai) surinko teisinių priemonių ir pajėgumų vystymo kategorijose.[98]

[96] International Telecommunications Union, „Global Cybersecurity Index 2020", žiūrėta 2023 m. gegužės 9 d., p. 25, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf
[97] *Ibid.,* p. vii
[98] *Ibid.,* p. 25

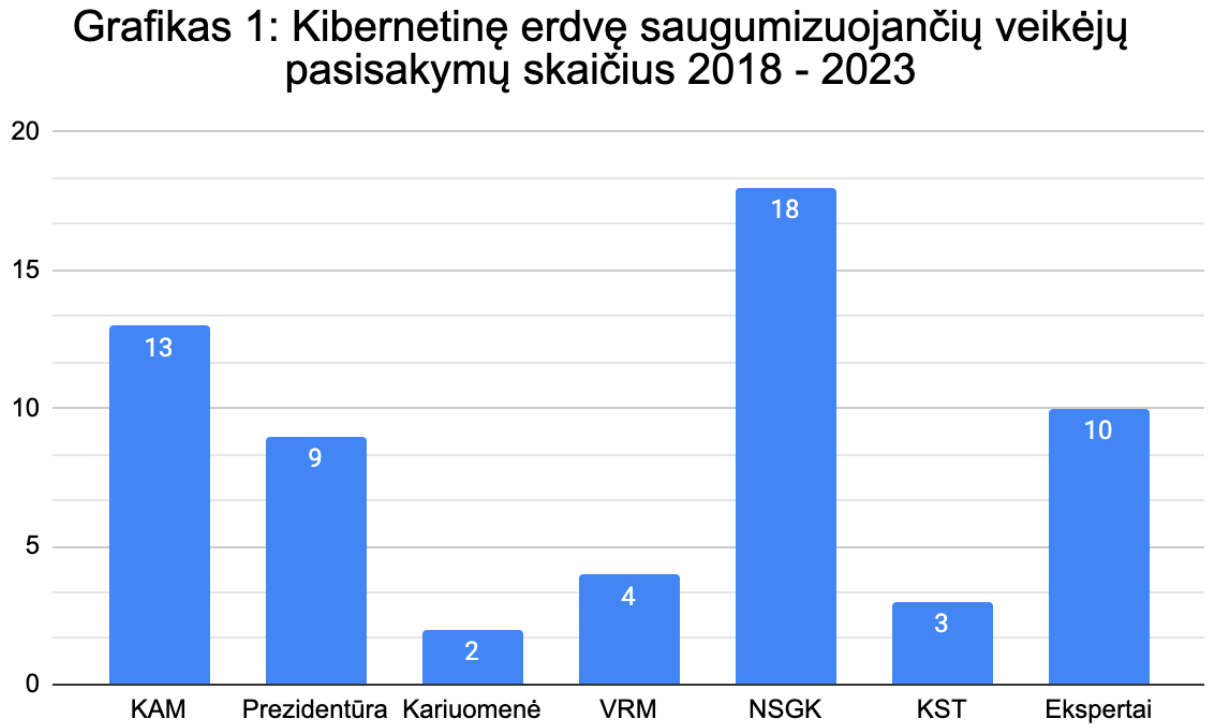
4. Kibernetinės erdvės saugumizavimas politikų, ekspertų ir kariškių diskurse

Tyrimo medžiagą sudaro 49 kalbos, pranešimai žiniasklaidoje ir interviu, pasirodę 2018-01-01 – 2023-04-01. Tyrimui pasirinkti institucijų, atsakingų už krašto apsaugos formavimą atstovai (*žr. grafiką Nr. 1*):

- KAM (ministrai Raimundas Karoblis (iki 2020-ųjų gruodžio), Arvydas Anušauskas);
- Prezidentūra (Dalia Grybauskaitė (iki 2019-ųjų liepos), Gitanas Nausėda);
- Kariuomenė (Jonas Vytautas Žukas (iki 2019-ųjų liepos), Valdemaras Rupšys, kariuomenės atstovai, atsakingi už kibernetinio saugumo sektorių);
- VRM (Rita Tamašunienė (iki 2020-ųjų gruodžio), Agnė Bilotaitė);
- NSGK (komiteto nariai);
- KST (komiteto nariai).

Taip pat, dėl jau minėtos technifikacijos ir kibernetinės erdvės specifiškumo, tyrimui atrinkti 10 kibernetinio saugumo specialistų pasisakymų (*žr. grafiką Nr. 1*). Atrinkti tik tie ekspertų pasisakymai, kuriuose komentuojamas reikšmingas valstybei ar nacionaliniam saugumui klausimas. Visa medžiaga tyrimui buvo renkama naudojantis „Google“ paieškos sistema, įvedant su kibernetiniu saugumu susijusius raktažodžius: „kibernetinis saugumas“, „informacinis saugumas“, „kibernetinės erdvės saugumas“, „skaitmenins saugumas“. Siekiant užtikrinti, kad į tyrimo duomenis patektų ir rezultatai iš Prezidentūros (lrp.lt) ar Seimo (lrs.lt) puslapių, taip pat buvo pasitelktos ir duomenų agregavimo programos „ScreamingFrog“ ir „Ahrefs“, leidžiančios agreguoti visą svetainėse esantį turinį ir jį filtruoti pagal raktažodžius. Šioje duomenų rinkimo dalyje buvo naudojami tie patys, su kibernetine erdve susiję raktažodžiai. Pagal raktažodžius atrinkti tekstai buvo toliau filtruojami, juose ieškant saugumizavimo apraiškų (sugrėsminimo, siūlomų priemonių ir kt.)

Siekiant atspindėti kiekvienos iš institucijų interesus kibernetinės erdvės saugumo lauke, atrinkti straipsniai buvo suskirstyti pagal saugumizuojančio veikėjo priklausomybę vienai iš jų. Atskirais atvejais, kartu su besikeičiančiu veikėjų, ryškiai pasikeičiant ir diskursui, pateikiama papildoma informacija įvykusį pasikeitimą.



Šaltinis: sudaryta autoriaus, remiantis tyrimo duomenimis

Tyrimo laikotarpiu aktyviausiai viešojoje erdvėje kibernernetinę erdvę saugumizavimo Nacionalinio saugumo ir gynybos komiteto atstovai su 18 viešų pasisakymų. Antroje vietoje – Krašto apsaugos ministerija, trečioje – Prezidentūra. Kalbant apie Prezidentūrą, reikėtų pabrėžti, 5 iš 9 pasisakymų priklauso Daliai Grybauskaitei, kurios kadencija pasibaigė dar 2019-ųjų liepą. Tą galima paaiškinti tuo, kad D. Grybauskaitė labai aktyviai veikė, formuojant kibernetinio saugumo politiką. Kaip savo tyrime rodo I. Juknevičiūtė, prieš priimant Kibernetinio saugumo įstatymą, 2013 – 2015 metų laikotarpiu Prezidentė buvo aktyviausia saugumizuojanti veikėja, lenkianti NSGK, KAM ir kitas institucijas – jai priklausė 40% visų to laikotarpio pasisakymų.[99] Tuo tarpu šio tyrimo rėžiuose kariuomenės, Kibernetinio saugumo tarybos ir Vidaus reikalų ministerijos atstovai procese dalyvavo gerokai pasyviau, nepaisant to, kad Kibernetinio saugumo įstatyme yra nurodomi kaip vieni iš pagrindinių šios srities politikos formuotojų ir įgyvendintojų. Tą dalinai galima paaiškinti tuo, kad tiek kariuomenė, tiek KST yra glaudžiai susijusios su KAM, o šios institucijos vadovai (R. Karoblis ir A. Anušauskas) yra labiau matomi viešojoje erdvėje. Tuo tarpu VRM atstovų pasyvumą galimai lėmė Baltarusijos režimo sukelta migrantų krizė ir Covid-19 pandemija, užgožusios kitus klausimus. Ekspertų vertinimai viešojoje erdvėje paprastai pasirodydavo po didelio masto kibernetinių incidentų – atakų prieš Lietuvą ar kitas Rusijai „nedraugiškas“ šalis, ar plačiai nuskambėjusių duomenų nutekėjimų, kurių skaičius pastaruoju metu auga.

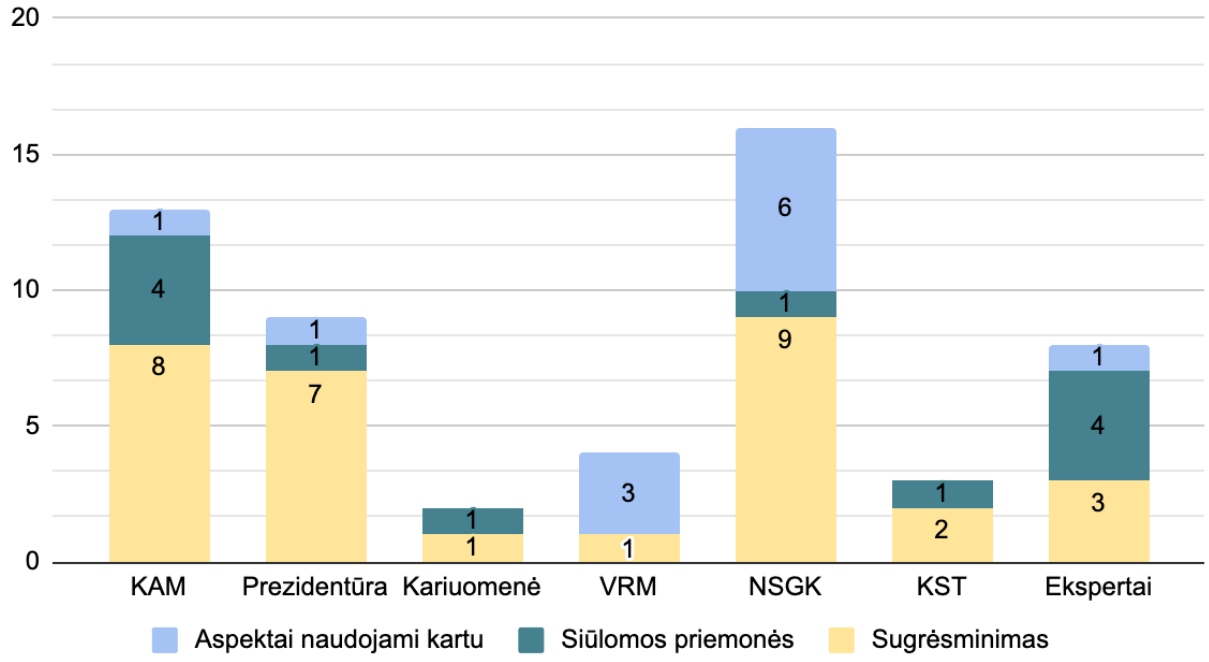
[99] Juknevičiūtė, p. 22

Tyrimo metu taip pat buvo apžvelgtos ir saugumizuojančių veikėjų diskurso panaudojimo aspektai (*žr. grafiką Nr. 2*). Atsižvelgiant į teorinį pagrindą, šie buvo suskirstyti į tris kategorijas:

1. Sugrėsminimas (akcentuojama grėsmė kibernetinei erdvei);
2. Siūlomos nepaprastosios priemonės, grėsmėms užkardyti ar įveikti;
3. Vienu pasisakymu ir sugrėsminama, ir pasiūloma priemonė prieš grėsmę.

Svarbu pabrėžti ir tai, kad kai kurie asmenys veikėjai, kalbėdami apie kibernetines grėsmes nematė jų ten, kur jau yra konsensusas (saugumizuota dokumentuose, kitų veikėjų diskurse) – tą po kartą padarė VRM (A. Bilotaitė) ir kibernetinio saugumo ekspertai Giedrius Meškauskas bei Andrius Šemeškevičius.

Grafikas 2: Saugumizuojančių veikėjų diskursijo panaudojimas



Šaltinis: sudaryta autoriaus, remiantis tyrimo duomenimis

Prezidentūra buvo labiausiai kibernetinę erdvę sugrėsminanti institucija. Tokia retorika aptinkama septyniuose kalbos aktuose, tuo tarpu dviejuose pasiūlomos ar kitaip minimos priemonės grėsmėms užkardyti. NSGK ir KAM taip pat aktyviai naudojo grėsmių diskursą, tačiau daug dėmesio skyrė ir priemonėms. Tuo tarpu kariuomenė, VRM ir KST tiek apie grėsmės, tiek apie priemones kalbėjo maždaug vienodai, visgi dėl mažos imties, negalima daryti išvadų apie šių institucijų atstovų prioritetus. Galiausiai, ekspertai procentaliai pateikė daugiausiai pasiūlymų grėsmių užkardymui. Tą būtų galima aiškinti ir per technifikacijos sąvoką – su kibernetinės erdvės problematika geriau susipažinę asmenys turi daugiau informacijos ir gali lengviau artikuliuoti ne tik problemą, bet ir jos

sprendimo būdus. Detalesnė informacija ir įžvalgos apie saugumizavimo procesą, vykdomą kiekvienai iš šių institucijų priklausančių veikėjų, bus pateikta sekančiuose skyriuose.

4.1. Kibernetinės erdvės saugumizavimas KAM diskurse

Krašto apsaugos ministerija buvo viena iš pagrindinių institucijų, saugumizuojant kibernetinę erdvę 2018 - 2023 metais. Kaip pagrindinės, už šalies gynybai skiriamų resursų alokavimą ir tarptautinį bendradarbiavimą gynybos srityje atsakingos ministerijos, KAM atstovai daug kalbėjo apie priemones, reikalingas stiprinti kibernetinį saugumą. Svarbu pabrėžti ir tai, kad net 12 iš 13 pasisakymų minėtu laikotarpiu priklauso A. Anušausko vyriausybei. Visgi, atsakyti į klausimą kodėl susidarė tokia situacija (kiti R. Karoblio vadovaujamos ministerijos prioritetai, pasyvumas antrojoje kadencijos pusėje ir kt.), reikėtų papildomų diskurso tyrimų, apimančių ilgesnį laikotarpį (nuo 2016-ųjų).

Bene svarbiausias šio laikotarpio pasisakymas buvo apie naują viceministro pareigybę, skirtą kibernetiniam saugumui šalyje kuruoti. Ministro A. Anušausko teigimu, kibernetinis saugumas svarbi sritis visai valstybei, o ministras būtų atsakingas ir už NKSC veiklą, matomą kaip būtiną instituciją komunikacijai šalyje palaikyti.[100] Visgi, bent jau internetinėje erdvėje šis klausimas toliau keliamas nebuvo.

Daugiausiai KAM atstovai akcentavo finansinius klausimus bei specialistų trūkumą: „Iš privataus verslo mums pritraukti specialistus dėl atlyginimų apribojimų, kuriuos numato Krašto apsaugos įstatymas, yra sudėtinga, tačiau mes numatę po poros mėnesių Seimui pateikti įstatymo pakeitimus, kad tiems specialistams, kurie susiję su šitomis sritimis, mes galėtume mokėti rinkos sąlygų atlyginimus.“[101] Ši citata pasakyta likus vos porai savaičių iki Rusijos invazijos į Ukrainą, viešojoje erdvėje aktyviai diskutuojant ir apie Lietuvos saugumą, todėl veikiausiai buvo pasinaudota šiai sričiai išaugusiu dėmesiu. Be to, investicijų klausimas buvo eskaluojamas ir vėliau, teigiant, kad „KAM negali apsaugoti visų šalyje veikiančių institucijų“, taip ir toliau pratęsiant šią liniją.[102] Tarp

[100] Milena Andrukaitytė, , „A.Anušauskas matytų poreikį už kibernetinį saugumą atsakingam viceministrui“, 15min, žiūrėta 2023 m. gegužės 5 d., https://www.15min.lt/naujiena/aktualu/lietuva/a-anusauskas-matytu-poreiki-uz-kibernetini-sauguma-atsakingam-viceministrui-56-1995714

[101] Ramūnas Jakubauskas, „KAM ketina mokėti didesnes algas kibernetinio saugumo specialistams“, BNS, žiūrėta 2023 m. gegužės 5 d., https://m.diena.lt/naujienos/lietuva/salies-pulsas/kam-ketina-moketi-didesnes-algas-kibernetinio-saugumo-specialistams-1063288

[102] Augustas Stankevičius, „Prieš KAM svetainę gegužę įvykdyta masyvi kibernetinė ataka: Lietuvoje jos dažnėja ir sudėtingėja“, BNS, žiūrėta 2023 m. gegužės 5 d., https://www.15min.lt/verslas/naujiena/mokslas-it/pries-kam-svetaine-geguze-ivykdyta-masyvi-kibernetine-ataka-1290-1681544

kitų siūlomų priemonių taip pat buvo tarptautinis bendradarbiavimas,[103] ar nepatikimų technologijų ar programinės įrangos iš Kinijos ribojimas.[104] Pastarąją temą labiausiai eskalavo NKSC atstovai.

Kinija buvo minima ir grėsmių kontekste, dažniausiai kalbant apie nepatikimos technologijos tiekėjus, siejamus su šios šalies valdžia. KAM atstovai akcentavo socialinio tinklo „TikTok“[105] ir populiarių mobiliųjų telefonų „Huawei“ keliamas grėsmes valstybės tarnautojams dėl galimo duomenų rinkimo.[106] Visgi, didžioji dalis ministerijos įžvelgiamų grėsmių buvo susijusios su Rusija. Tai galima paaiškinti tiek per tai, kad tyrimo laikotarpiu su Rusija siejami programišiai įvykdė bent kelias kibernetines atakas prieš Lietuvos įmones ar institucijas, tiek dėl prasidėjusio karo Ukrainoje, bent laikinai užgožusio Kinijos grėsmę kibernetinėje erdvėje. A. Anušausko teigimu, bene didžiausi kibernetinių atakų mastai buvo pastebėti jau prasidėjus karui: „Kiberatakos vyko visą laiką, nesustojamai, jau, sakyčiau, ne vienus metus vyksta. Bet tokio masto, intensyvumo – jei ir nepasiekė aukščiausio intensyvumo, bet sakyčiau, vidutinio intensyvumo – tai taip, tai vyksta, ko gero, pirmą kartą.“[107] Panašus naratyvas buvo išsakytas dar kelis kartus – metų pabaigoje, teigiant, kad ne tik Rusija, bet ir Kinija agresyviau elgiasi kibernetinėje erdvėje[108] ar šių metų kovą, dar kartą primenant apie padažnėjusias kibernetines atakas, siejamas su Rusija.[109]

4 Lentelė. KAM saugumizuojančių veikėjų diskurso naudojimo pobūdis

Grėsmės šaltinis (kartai)	**Grėsmės pobūdis (kartai)**	**Siūloma priemonė (kartai)**
Rusija (5)	Kibernetinės atakos (augantis jų skaičius, sudėtingumas ir kt.) (4)	Finansavimo, pajėgumų didinimas (2)
Kinija (2)	Akcentuojamas pavojus kritinei infrastruktūrai / pamatiniam	Teisinis reglamentavimas (1)

[103] LRT.lt, „Lietuva ir Izraelis sutarė glaudžiau bendradarbiauti kibernetinio saugumo srityje“, žiūrėta 2023 m. gegužės 5 d., https://www.lrt.lt/naujienos/lietuvoje/2/1927501/lietuva-ir-izraelis-sutare-glaudziau-bendradarbiauti-kibernetinio-saugumo-srityje

[104] 15min, „15/15: ar Lietuvos valstybinės institucijos turėtų drausti naudoti „TikTok“?“, 12:25 – 12:45, žiūrėta 2023 m. gegužės 5 d., https://www.15min.lt/ikrauk/video/1515-ar-lietuvos-valstybines-institucijos-turetu-drausti-naudoti-tiktok-235716

[105] *Ibid.*

[106] Nemira Pumprickaitė, „Anušauskas apie pavojus dėl Kinijoje pagamintų telefonų: tūkstančiai nupirkta valstybės institucijoms dėl to, kad pigiau kainuoja“, LRT, žiūrėta 2023 m. gegužės 2 d., https://www.lrt.lt/naujienos/mokslas-ir-it/11/1501190/anusauskas-apie-pavojus-del-kinijoje-pagamintu-telefonu-tukstanciai-nupirkta-valstybes-institucijoms-del-to-kad-pigiau-kainuoja

[107] Ignas Jačauskas, „A.Anušauskas: kiberatakų organizatoriai ieško silpnų vietų, galimi išpuoliai prieš verslą“, BNS, žiūrėta 2023 m. gegužės 5 d., https://www.15min.lt/naujiena/aktualu/lietuva/a-anusauskas-kiberataku-organizatoriai-iesko-silpnu-vietu-galimi-ispuoliai-pries-versla-56-1742794

[108] Arvydas Anušauskas, „Arvydas Anušauskas. 2022 metais sukūrėme stipresnę, modernesnę ir geriau organizuotą krašto apsaugos sistemą“, LRT, , žiūrėta 2023 m. gegužės 3 d., https://www.lrt.lt/naujienos/pozicija/679/1855987/arvydas-anusauskas-2022-metais-sukureme-stipresne-modernesne-ir-geriau-organizuota-krasto-apsaugos-sistema

[109] BNS, „Belgija, Slovėnija jungiasi prie Lietuvos vadovaujamų ES kibernetinių pajėgų“, žiūrėta 2023 m. gegužės 2 d., https://www.lrt.lt/naujienos/lietuvoje/2/1931984/belgija-slovenija-jungiasi-prie-lietuvos-vadovaujamu-es-kibernetiniu-pajegu

	visuomenės ir valstybės gyvenimo aspektui (3)	
Aiškiai nenurodyta (3)	Nepatikimos technologijos (2)	Tarptautinė partnerystė (2)

Šaltinis: sudaryta autoriaus, remiantis tyrimo duomenimis

Iš pateiktų duomenų aišku, kad tyrimo laikotarpiu didžiausia grėsme kibernetinėje erdvėje KAM atstovai matė Rusiją. Trijuose pasisakymuose nėra akcentuojamas aiškus grėsmės šaltinis, tačiau visuose iš jų kibernetinės grėsmės minimos Rusijos karo Ukrainoje kontekste, todėl būtų galima daryti prielaidą, kad šiuose pasisakymuose taip pat saugumizuojama Rusijos grėsmė. Panaši situacija yra ir su įvardijamais grėsmės pobūdžiais – nors tekstuose kritinė infrastruktūra tiesiogiai akcentuojama 3 kartus, pasisakymo kontekstai (išpuoliai prieš Lietuvos geležinkelius, KAM), leidžia teigti, kad bene visais atvejais akcentuojama buvo būtent kritinė infrastruktūra. Galiausiai, KAM dėmesį skyrė ir tiesioginių savo funkcijų (biudžeto alokavimo krašto gynybai, strateginių partnerysčių vykdymui) – būtent su tuo susiję pasiūlymai dažniausiai skambėjo viešojoje erdvėje (*žr. priedą Nr. 5*).

4.2. Kibernetinės erdvės saugumizavimas Prezidentūros diskurse

Kaip jau buvo minėta, Prezidentūra iš kitų institucijų išsiskiria dideliu skaičiumi sugrėsminimo aktų, lyginant su siūlomomis priemonėmis. Be to, vos per pusantrų metų laikotarpį (2018 pradžia – 2019 liepa), D. Grybauskaitė kibernetinę erdvę saugumizavo dažniau, nei G. Nausėda. Iš to galima daryti išvadą, kad jai ši sritis buvo gerokai svarbesnė, todėl buvo imamasi lyderystės. Prezidentė buvo vienintelė iš visų saugumizuojančių veikėjų, įspėjusi apie galimas Rusijos kibernetines atakas, siekiant paveikti trejus rinkimus 2019-aisiais: „Šiais trejų rinkimų Lietuvoje metais tikėtinos agresyvesnės trečiųjų šalių, pirmiausiai – Rusijos kibernetinės atakos, siekiant paveikti rinkimų eigą ir rezultatus.“[110] Apie tai buvo paskelbta ir vienoje iš VSD ataskaitų. Be to, Grybauskaitė akcentavo kibernetinės erdvės saugumo svarbą demokratijai: „...saugi ir patikima kibernetinė erdvė – demokratijos išlikimo sąlyga. Sparčiai augant industrinei ir technologinei pažangai, kibernetinis saugumas tampa gyvybiškai svarbia nacionalinio saugumo dalimi.“[111] Taip pat teigiama, kad kibernetinės atakos „..dažniausiai yra nukreiptos prieš valstybės gyvavimui svarbius sektorius – strateginius energetikos, transporto ir finansų tinklus.“[112] Galiausiai, D. Grybauskaitė siūlė Lietuvai imtis lyderystės visoje užtikrinant kibernetinį saugumą visoje Europoje: „Nebijokime būti ir

[110] BNS, „Prezidentūra: per rinkimus tikėtinos Rusijos kibernetinės atakos“, 15min, žiūrėta 2023 m. gegužės 3 d., https://www.15min.lt/naujiena/aktualu/lietuva/preizdentura-per-rinkimus-tiketinos-rusijos-kibernetines-atakos-56-1084732

[111] Prezidentės spaudos tarnyba, „Davose – Lietuvos kibernetinio saugumo patirtis“, žiūrėta 2023 m. gegužės 3 d., https://grybauskaite.lrp.lt/lt/spaudos-centras/pranesimai-spaudai/31744

[112] *Ibid.*

Europos Sąjungos integracijos smaigalyje, nes tik suvieniję pastangas karinio, energetinio, kibernetinio ir ekonominio saugumo srityse jausimės stiprūs. Atgimstanti stiprios ir vieningos Europos idėja grąžina pasitikėjimą savimi <...> Lietuva jau prisideda prie Europos saugumo stiprinimo: mūsų iniciatyva kuriamos greitojo reagavimo pajėgos kibernetinėms grėsmėms atremti ir kovoti su priešiška propaganda, patvirtinti bendri standartai ES išorės sienos apsaugai.“[113]

Tuo tarpu prezidentu tapus G. Nausėdai, kibernetinei erdvei skiriamas prezidentūros dėmesys akivaizdžiai sumažėjo. Be to, atsižvelgiant į pasisakymų pobūdį, galima daryti išvadą, kad Prezidentui kibernetinis saugumas aktualesnis gerovės valstybės, ne tarptautinio saugumo kontekste: „...Lietuvos požiūriu, rimčiausiomis kliūtimis turėtų būti laikomi taisyklėmis grįstos pasaulinės tvarkos pažeidimai, kibernetinės erdvės virsmas nauju ginklavimosi lauku, tarptautinių aplinkosaugos bei branduolinės saugos standartų nepaisymas, klimato kaitos ignoravimas.“,[114] „Bendras nusikalstamumo lygio mažėjimas, stebimas nuo 2017 metų, nuteikia pozityviai. Tačiau turime daugiau dėmesio skirti korupcinių ir kibernetinių nusikaltimų tyrimams, plėtoti tarptautinį bendradarbiavimą.“[115] Visgi, reikia pastebėti, kad G. Nausėda akcentavo ir nacionaliniam saugumui aktualius klausimus, susijusius su kibernetine erdve, reaguodamas į išpuolį prieš Užsienio reikalų ministeriją (URM), Prezidentas teigė: „...nutekėjusi informacija gali padaryti didelės žalos pirmiausia sąjungininkų atžvilgiu.“[116] (*žr. priedą Nr. 3*).

5 Lentelė. Prezidentūros saugumizuojančių veikėjų diskurso naudojimo pobūdis (D. Grybauskaitė)

Grėsmės šaltinis (kartai)	**Grėsmės pobūdis (kartai)**	**Siūloma priemonė (kartai)**
Rusija (2)	Kibernetinės atakos (augantis jų skaičius, sudėtingumas ir kt.) (1)	Finansavimo, pajėgumų didinimas (0)
Kinija (0)	Akcentuojamas pavojus kritinei infrastruktūrai / pamatiniam visuomenės ir valstybės gyvenimo aspektui (2)	Teisinis reglamentavimas (0)

[113] Prezidentės spaudos tarnyba, „Lietuvos Respublikos Prezidentės Dalios Grybauskaitės metinis pranešimas“, žiūrėta 2023 m. gegužės 3 d., https://grybauskaite.lrp.lt/lt/spaudos-centras/pranesimai-spaudai/30197

[114] Prezidento žiniasklaidos centras: „Prezidento kalba JTGA: kurti visuotinę gerovę mums yra aukščiausias priesakas“, žiūrėta 2023 m. gegužės 1 d., https://www.lrp.lt/lt/ziniasklaidos-centras/naujienos/prezidento-kalba-jtga-kurti-visuotine-gerove-mums-yra-auksciausias-priesakas/33141

[115] Milena Andrukaitytė, „G. Nausėda ragina atidžiau tirti korupcinius ir kibernetinius nusikaltimus“, BNS, žiūrėta 2023 m. gegužės 1 d., https://m.kauno.diena.lt/naujienos/lietuva/politika/g-nauseda-susitinka-su-generaline-prokurore-aptars-nusikalstamumo-tendencijas-1070959

[116] TV3, „DIENOS PJŪVIS. Kibernetinės atakos prieš Lietuvą: kokie pavojai ir kaip reaguoti?“, žiūrėta 2023 m. gegužės 1 d.,https://www.tv3.lt/naujiena/video/dienos-pjuvis-kibernetines-atakos-pries-lietuva-kokie-pavojai-ir-kaip-reaguoti-n1109634

Aiškiai nenurodyta (3)	Nepatikimos technologijos (0)	Tarptautinė partnerystė (1)

Šaltinis: sudaryta autoriaus, remiantis tyrimo duomenimis

6 Lentelė. Prezidentūros saugumizuojančių veikėjų diskurso naudojimo pobūdis (G. Nausėda)

Grėsmės šaltinis (kartai)	**Grėsmės pobūdis (kartai)**	**Siūloma priemonė (kartai)**
Rusija (0)	Kibernetinės atakos (augantis jų skaičius, sudėtingumas ir kt.) (1)	Finansavimo, pajėgumų didinimas (0)
Kinija (0)	Akcentuojamas pavojus kritinei infrastruktūrai / pamatiniam visuomenės ir valstybės gyvenimo aspektui (1)	Teisinis reglamentavimas (0)
Aiškiai nenurodyta (4)	Kibernetiniai nusikaltimai (2)	Nusikaltimų prevencija (1)

Šaltinis: sudaryta autoriaus, remiantis tyrimo duomenimis

Apibendrinant, matomas gana aiškus skirtumas tarp D. Grybauskaitės ir G. Nausėdos kibernetinės erdvės saugumizavimo. Grybauskaitė šios srities saugumą mato kaip pamatinį, būtiną normaliam demokratiškos valstybės funkcionavimui (tiek per rinkimus, tiek per kritinę infrastruktūrą) užtikrinti, todėl buvo ryški saugumizuojanti veikėja, nepaisant ganėtinai trumpo jos prezidentavimo laikotarpio, patekusio į tyrimo rėžius. Tuo tarpu G. Nausėda kibernetinės erdvės saugumą mato kaip vieną iš sudėtinių jo propaguojamos gerovės valstybės idėjos dalių, neišskirdamas šios srities svarbos iš korupcijos, aplinkosaugos ir kt.

4.3. Kibernetinės erdvės saugumizavimas kariuomenės diskurse

Nepaisant vaidmens, saugant kibernetinę erdvę, tyrimo laikotarpiu aptikti tik 2 pasisakymai, kuriais kariuomenės atstovai saugumizuoja kibernetinę erdvę. Šią situaciją galima aiškinti tuo, kad viešojoje erdvėje kibernetinės erdvės saugumizavimas paliekamas kitoms institucijoms – KAM ir NKSC, kurių atstovai komentavo ir tokias naujienas kaip kariuomenės kibernetinio saugumo pratybos, tuo tarpu kariuomenės vadas V. Rupšys aktyviai pasisakė apie konvencines pajėgas, karą Ukrainai ir paramą kariaujančiai šaliai. Nepaisant to, aptiktuose pasisakymuose galima rasti kritinės infrastruktūros saugumizavimo: „Didelio masto kibernetinės atakos gali sutrikdyti ne tik valstybinių įstaigų veiklą, bet ir ypatingos svarbos infrastruktūros įmonių veiklą, kas gali iššaukti masinius nepasitenkinimo protestus ir chaosą valstybėse. Tam, kad užkardyti priešiškų jėgų veiklą ir yra

kuriami bei vystomi kibernetinio saugumo pajėgumai.“[117] ar pareiškimą apie dvišalės partnerystės su JAV svarbą, akcentuojamą ir Nacionalinėje kibernetinio saugumo strategijoje.[118] (*žr. priedą Nr. 2*).

4.4. Kibernetinės erdvės saugumizavimas VRM diskurse

VRM diskurse dominavo nusikaltimų kibernetinėje erdvėje naratyvas, be to pati sritis įprastai minima kitų pavojų ar grėsmių kontekste. Nusikaltimai skaitmeninėje erdvėje saugumizuojami trijuose iš keturių pasisakymų (*žr. priedą Nr. 4*). Visgi, reikia pabrėžti, kad A. Bilotaitė mėgino saugumizuoti ir kritinę infrastruktūrą: „Tiesioginių grėsmių valstybei svarbiems objektams nėra. Tačiau, įvertinus Ukrainos patirtis, negalime atmesti, kad Lietuvai priešiškos jėgos eskaluos valstybės strateginių objektų saugumo temą...“[119] Visgi, pasakymas, kad „tiesioginių grėsmių valstybei svarbiems objektams nėra“ neatitinka nei to, kas akcentuojama dokumentuose, nei to, ką šneka kitos institucijos, kur pabrėžiama, kad Rusijos ir Kinijos veiksmai agresyvėja, o pavojus kritinei infrastruktūrai ar kitiems pamatiniams visuomenės ar politinio gyvenimo aspektams išlieka. Be to, tame pačiame tekste A. Bilotaitė pažymi, kad visgi reikia daugiau investuoti į valstybei svarbių objektų apsaugai būtinas priemones ar darbuotojų atitikimo reikalavimus,[120] tačiau žvelgiant iš saugumizavimo teorijos perspektyvos, teiginys, kad „tiesioginių grėsmių svarbiems objektams nėra“, yra kontrproduktyvus.

4.5. Kibernetinės erdvės saugumizavimas NSGK diskurse

Iš kitų institucijų NSGK labiausiai išsiskyrė dėmesiu Kinijai ir nepatikimoms technologijoms – iš 17 kalbos aktų, dešimtyje kaip grėsmė nurodyta Kinija, su šia šalimi susijusios technologijos ar programinė įranga. Tą galima paaiškinti tuo, kad 2020 - 2021 metais viešojoje erdvėje buvo daug diskusijų apie 5G technologijos plėtrą, akcentuojant galimus technologijų iš Kinijos keliamus privatumo ir kitus klausimus. Tai lėmė ir aukštą papildomo teisinio reglamentavimo pasiūlymų kiekį: „...Viena iš idėjų, kurią būtų galima įgyvendinti stipriais Vyriausybės sprendimais, tai yra labai konkrečiai įvardinti konkrečius gamintojus, nedemokratinių valstybių konkrečius gamintojus, kurių informacijos ir ryšių technologijų įranga kelia potencialią grėsmę mūsų šalies saugumui ir neturi būti naudojama Lietuvoje diegiant penktos kartos vadinamąjį 5 G judrųjį ryšį.“[121] Panašus naratyvas buvo

[117] Lietuvos kariuomenė, „Gynybos štabas organizavo kibernetinės gynybos pratybas“, žiūrėta 2023 m. balandžio 27 d., https://www.kariuomene.lt/kas-mes-esame/naujienos/gynybos-stabas-organizavo-kibernetines-gynybos-pratybas/21402

[118] LRT, „Rupšys: JAV Pensilvanijos gvardija – vienas saugumo garantų Baltijos regione“ BNS, žiūrėta 2023 m. gegužės 1 d., https://www.lrt.lt/naujienos/lietuvoje/2/1834193/rupsys-jav-pensilvanijos-gvardija-vienas-saugumo-garantu-baltijos-regione

[119] VRM, „VST ir policija stiprina bendradarbiavimą dėl strateginių objektų apsaugos“, žiūrėta 2023 m. gegužės 1 d., https://vrm.lrv.lt/lt/naujienos/vst-ir-policija-stiprina-bendradarbiavima-del-strateginiu-objektu-apsaugos

[120] *Ibid.*

[121] Jadvyga Bieliavska, „L. Kasčiūnas: grėsmių saugumui pristatymas – savotiškas priešnuodis“, ELTA, žiūrėta 2023 m. balandžio 19 d. https://www.diena.lt/naujienos/lietuva/politika/l-kasciunas-gresmiu-saugumui-pristatymas-savotiskas-priesnuodis-1014647

naudojamas ir komentuojant naujienas apie geležinkeliuose naudojamą rusišką technologiją „Jeigu į Lietuvą atvyktų NATO sąjungininkai, būtų naudojami geležinkeliai, apie kurių veiksmus rusai žinotų viską.“[122] Pastarasis atvejis įdomus ir tuo, kad NSGK primininkas Laurynas Kasčiūnas kritikavo A. Anušauską neveiksnumu „Grėsmės akivaizdžios, bet dabar krašto apsaugos ministrui tai visiškai nesvarbu.“[123] Nors KAM kaip vieną iš grėsmių taip pat matė nepatikimas technologijas, ministerijos atstovai labiau akcentavo kibernetinių atakų ir kritinės infrastruktūros reikšmę. Atsižvelgiant į NSGK aktyvumą bei į tai, kokią svarbą rusiškos ir kiniškos technologijos turi NSGK darbotvarkėje, galima daryti išvadą, kad taip buvo siekiama šiai sričiai pritraukti dėmesio ir iš kitų institucijų.

Nors NSGK diskurse buvo aptariamos ir kitos grėsmės (augantis kibernetinių atakų skaičius) ar siūlomos priemonės (finansavimo, pajėgumų didinimas, kvalifikacijos darbuotojams kėlimas), nepatikimų technologijų skvarba į visus šalies gyvenimo aspektus, įskaitant kritinę infrastruktūrą, buvo saugumizuojama labiausiai. Toks susitelkimas į konkrečią sritį taip pat yra ir ryškiausiais iš visų apžvelgtų institucijų, todėl, atsižvelgiant į saugumizavimo teorines prielaidas, galima daryti išvadą, kad NSGK tyrimo laikotarpiu saugumizavo tikslingiausiai (*žr. priedą Nr. 7*).

7 Lentelė. NSGK saugumizuojančių veikėjų diskurso naudojimo pobūdis

Grėsmės šaltinis (kartai)	**Grėsmės pobūdis (kartai)**	**Siūloma priemonė (kartai)**
Rusija (3)	Kibernetinės atakos (augantis jų skaičius, sudėtingumas ir kt.) (2)	Finansavimo, pajėgumų didinimas (2)
Kinija (10)	Akcentuojamas pavojus kritinei infrastruktūrai / pamatiniam visuomenės ir valstybės gyvenimo aspektui (2)	Teisinis reglamentavimas (5)
Aiškiai nenurodyta (3)	Nepatikimos technologijos (13)	Kibernetinio saugumo mokymai (1)

Šaltinis: sudaryta autoriaus, remiantis tyrimo duomenimis

4.6. Kibernetinės erdvės saugumizavimas KST diskurse

Kibernetinio saugumo taryba buvo tarp pasyviausių organizacijų saugumizuojant kibernetinę erdvę. Tą galima paaiškinti tuo, kad KST sudaryta iš įvairių institucijų atstovų, pvz., KAM ar NKSC, todėl saugumizuojantys veikėjai renkasi komunikuoti nuo šių įstaigų, o pati KST veikia kitaip nei

[122] Indrė Naureckaitė, „Atskleidus apie valstybinės įmonės pirkimo iš Rusijos planą – sujudimas: Seimo nariai imasi veiksmų“, žiūrėta 2023 m. gegužės 1 d., https://www.lrytas.lt/lietuvosdiena/aktualijos/2023/02/21/news/atskleidus-apie-valstybines-imones-pirkimo-is-rusijos-plana-sujudimas-seimo-nariai-imasi-veiksmu-26200127
[123] *Ibid.*

kitos institucijos ir renkasi tik kelis kartus per metus. Tyrimo laikotarpiu buvo aptikti tik trys pasisakymai viešojoje erdvėje (visi paskelbti KAM internetiniame puslapyje), tačiau reikėtų pabrėžti, kad visi jie paskelbti praėjusių metų antrojoje pusėje – šiemet, todėl galima tikėtis KST suaktyvėjimo viešojoje erdvėje ateityje (*žr. priedą Nr. 6*).

4.7. Kibernetinės erdvės saugumizavimas ekspertų diskurse

Ekspertai į šį tyrimą įtraukti kaip kontrolinė grupė – jau minėta, kad kibernetinės erdvės specifiškumas, polinkis technifikacijai gali sukelti problemų ją saugumizuojant žmonėms, neturintiems daug žinių apie kibernetinį saugumą. Kibernetinio saugumo ekspertai iš kitų grupių išsiskyrė pasiūlymais dėl kibernetinio specialistų rengimo, pabrėžiant tiek pačių specialistų, tiek finansavimo trūkumą. Nors galima kelti klausimą dėl tokio diskurso tikslo (kibernetinio saugumo specialistų trūksta ir privačiame sektoriuje), kritika valstybei dėl nepasiruošimo kibernetinėms atakoms rodo susirūpinimą ir dėl viešojo sektoriaus: „Nereikia tikėtis, kad kibernetinio saugumo sistemos gali būti padarytos pigiai ir kokybiškai, nupirktos iš kaimyno ar studento, (...) reikia rimtai į šiuos klausimus pasižiūrėti, samdyti specialistus, daryti auditus, ruoštis galimai atakai.“[124] Tarp kitų siūlomų priemonių verta išskirti naujausių technologijų (automatizavimas, dirbtinis intelektas, daiktų internetas virtuali/alternatyvi realybė) panaudojimą rengiantis gintis nuo kibernetinių atakų[125] ar net rezervinio interneto, skirto palaikyti kritinės infrastruktūros veikimą užpuolimo atveju.[126] (*žr. priedą Nr. 1*).

Visgi, kai kuriais klausimais kibernetinio saugumo specialistai nepritaria tam, kas saugumizuojama kitų institucijų atstovų. Bene dažniausiai pasisakančio eksperto Giedriaus Meškausko teigimu, su Rusijos tarnybos siejama „Killnet“ grupuotė yra „panaši į rusų kariuomenę – daug kalbų, bet kai ateina laikas veikti, iš didelio debesies susidaro labai nedidelis lietus.“[127] Tuo tarpu A. Anušauskas apie šią grupę akcentavo jos pavojingumą, teigdamas, kad „programišiai ieško silpnų vietų.“[128] Kitas nesutarimas įvyko dėl kiniškų technologijų, ryšio tiekėjo „Telia“ atstovui Andriui Šemeškevičiui pareiškus, kad bendrovės Huawei telefonai negalėtų šnipinėti, nes įmonei tai

[124] LRT, „Ekspertas apie kibernetinį saugumą: Lietuvoje yra du tipai įmonių – nulaužtos ir tos, kurios dar bus nulaužtos“, žiūrėta 2023 m. gegužės 1 d., https://www.lrt.lt/naujienos/mokslas-ir-it/11/1733755/ekspertas-apie-kibernetini-sauguma-lietuvoje-yra-du-tipai-imoniu-nulauztos-ir-tos-kurios-dar-bus-nulauztos

[125] 15min, „Ekspertai: energetikos sektoriui teks įveikti ne tik tiekimo, bet ir kibernetinio saugumo krizę“, žiūrėta 2023 m. gegužės 1 d., https://www.15min.lt/verslas/naujiena/energetika/ekspertai-energetikos-sektoriui-teks-iveikti-ne-tik-tiekimo-bet-ir-kibernetinio-saugumo-krize-664-1927278

[126] Sniegė Balčiūnaitė, „M.Pareščius: reikia rezervinio interneto, geresnės kompiuterių apsaugos“, BNS, žiūrėta 2023 m. gegužės 1 d., https://www.15min.lt/verslas/naujiena/mokslas-it/m-parescius-reikia-rezervinio-interneto-geresnes-kompiuteriu-apsaugos-1290-1650516

[127] Giedrius Meškauskas, „Giedrius Meškauskas: „Killnet“ kibernetinė ataka – kokia kariuomenė, tokie ir hakeriai“, 15min, žiūrėta 2023 m. gegužės 1 d., https://www.15min.lt/naujiena/aktualu/nuomones/giedrius-meskauskas-killnet-kibernetine-ataka-kokia-kariuomene-tokie-ir-hakeriai-18-1742384

[128] Ignas Jačauskas, „A.Anušauskas: kiberatakų organizatoriai ieško silpnų vietų, galimi išpuoliai prieš verslą“, 15min

„tolygu mirčiai.“[129] Tokį pareiškimą būtų galima aiškinti ir verslo interesais („Telia“ prekiauja šio gamintojo įrenginiais), tačiau tai gana ryškus nuomonių išsiskyrimas su kitomis institucijomis, pirmiausia NSGK, daug dėmesio skyrusiai kiniškų technologijų grėsmei.

8 Lentelė. Ekspertų saugumizuojančio diskurso naudojimo pobūdis

Grėsmės šaltinis (kartai)	Grėsmės pobūdis (kartai)	Siūloma priemonė (kartai)
Rusija (3)	Kibernetinės atakos (augantis jų skaičius, sudėtingumas ir kt.) (3)	Finansavimo, pajėgumų didinimas (5)
Kinija (0)	Akcentuojamas pavojus kritinei infrastruktūrai / pamatiniam visuomenės ir valstybės gyvenimo aspektui (1)	Teisinis reglamentavimas (0)
Aiškiai nenurodyta (6)	Nepatikimos technologijos (0)	Kibernetinio saugumo mokymai (0)

Šaltinis: sudaryta autoriaus, remiantis tyrimo duomenimis

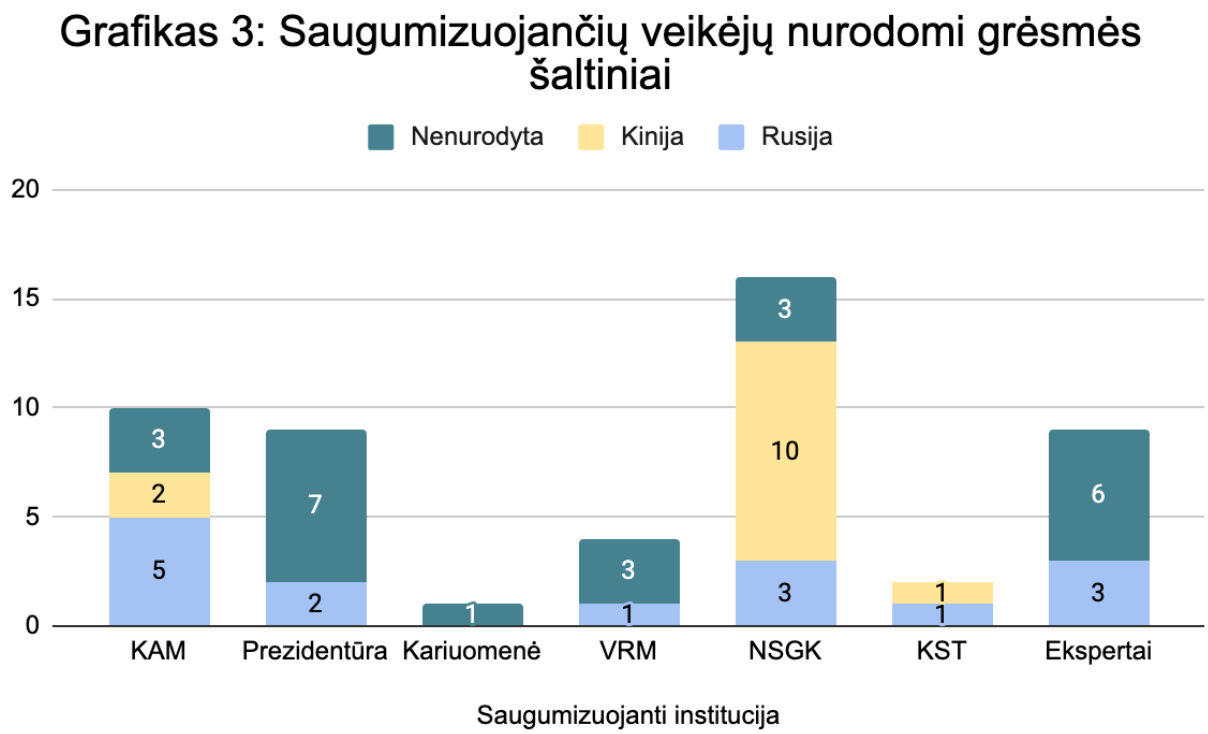
Apibendrinant, reikėtų pasakyti, kad kibernetinio saugumo ekspertų diskursas gali būti labai naudingas saugumizuojant šį lauką, ypatingai per siūlomas priemones, akcentuojant ir viso sektoriaus (darbuotojų, lėšų trūkumą) problemas ar per pateikiant kitų veikėjų neaptartas idėjas (naujausių technologijų pasitelkimas, stiprinant kibernetinį saugumą). Visgi, kai kurie pasiūlymai ar sugrėsminimai gali būti kontrproduktyvūs, galimai vedini verslo interesų.

4.8. Saugumizuojančių veikėjų analizės išvados

Apibendrinant tyrimo metu surinktus duomenis, galima teigti, kad nors saugumizavimo procesas ir vyko, ne visos institucijos jame dalyvavo pakankamai aktyviai, nepaisant to, kad yra įstatymiškai įpareigotos kurti ir įgyvendinti kibernetinės saugos planus. Pati aktyviausia buvo NSGK: jų kibernetinės erdvės saugumizavimas didele dalimi buvo vieno klausimo (nepatikimų kiniškų technologijų) eskalavimas. Visgi, žvelgiant iš saugumizavimo teorijos perspektyvos, tai galima laikyti teigiamu veiksmu, nes buvo siekiama užtikrinti pakankamą matomumą ir auditorijos pritarimą artikuliuojamai grėsmei. Svarbu pabrėžti, kad NSGK saugumizavimas buvo sėkmingas – Seimas uždraudė nepatikimų gamintojų ir tiekėjų technologijų naudojimą, įskaitant ir reikalingas 5G ryšiui

[129] Vaidas Neverauskas, „Telia“ technikos vadovas: naujas „Huawei“ saugesnis nei senas „iPhone“, 15min, žiūrėta 2023 m. gegužės 1 d., https://www.15min.lt/verslas/naujiena/mokslas-it/telia-technikos-vadovas-naujas-huawei-saugesnis-nei-senas-iphone-1290-929746

diegti.[130] Be to, ši institucija taip pat saugumizavo ir Rusijos keliamas grėsmes, naudojo diskursą apie kritinę infrastruktūrą ir augantį kibernetinių atakų skaičių ir intensyvumą.



Šaltinis: sudaryta autoriaus, remiantis tyrimo duomenimis

KAM taip pat buvo aktyvi proceso dalyvė, ne tik saugumizavusi Rusijos ir Kinijos (ar su jomis siejamų grupuočių) keliamą pavojų, bet ir akcentavusi pavojų kritinei infrastruktūrai. Be to, kaip pagrindinė už šalies gynybos resursus atsakinga institucija, KAM aktyviai komunikavo būtinybę skirti šiai sričiai daugiau dėmesio, minėjo tarptautinių partneryščių svarbą, matomą ir Nacionalinėje kibernetinio saugumo strategijoje. Tyrimo laikotarpiu KAM tikslingai saugumizavo kibernetinę erdvę, atkartodama tai, kas jau buvo minėta kibernetinio saugumo strategijoje ir kituose strateginiuose dokumentuose. Be to, reikėtų pabrėžti ir tai, kad 2018 – 2023 metais KAM atstovai buvo gerokai aktyvesni, negu 2013 – 2015 metais. Buvusi bene pasyviausia institucija (5 pasisakymai),[131] šio tyrimo rėžiuose ministerija šovę į viršų.

Tuo tarpu Prezidentūra, nepaisant trumpo, besibaigiančios antrosios D. Grybauskaitės kadencijos laikotarpiu, patekusio į tyrimą, vis tiek buvo aktyviausia valdant Prezidentei. D. Grybauskaitė matė ir komunikavo apie Rusijos keliamą grėsmę kritinei infrastruktūrai. Prezidentu tapus G. Nausėdai, kibernetinio saugumo klausimų Prezidentūros diskurse gerokai sumažėjo. Pradėta

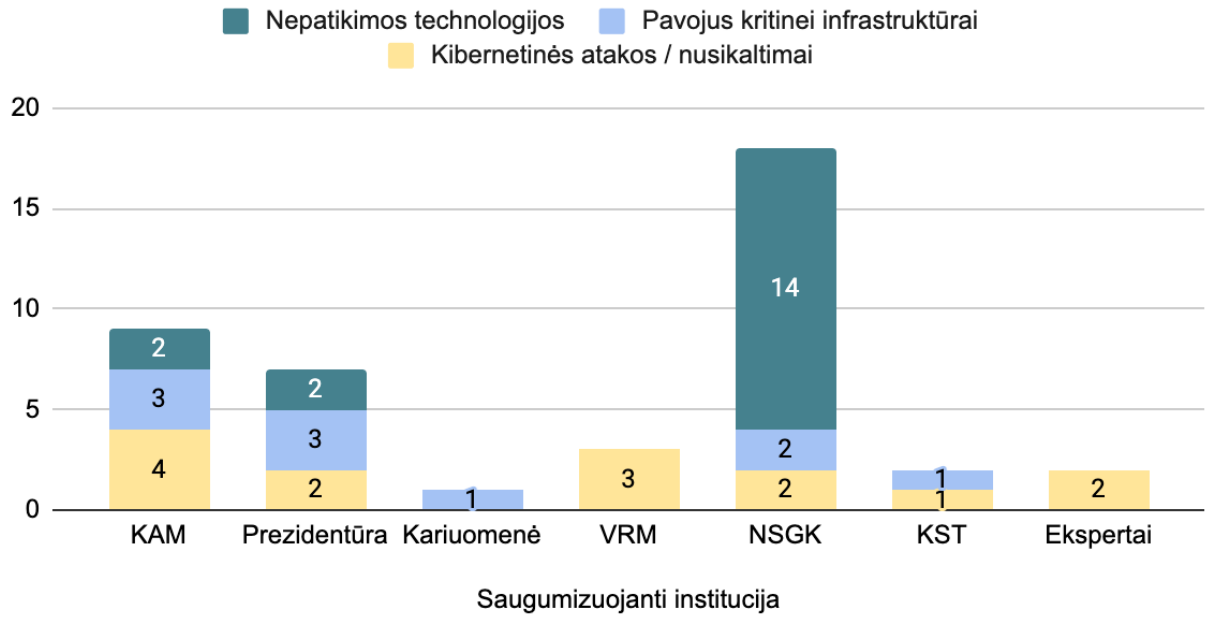
[130] Lietuvos Respublikos Seimas, „Seimas pritarė, kad nepatikimi gamintojai ir tiekėjai Lietuvoje negalėtų dalyvauti elektroninių ryšių rinkoje, ypač diegiant penktos kartos mobiliųjį 5G ryšį“, žiūrėta 2023 gegužės 9 d., https://www.lrs.lt/sip/portal.show?p_r=35435&p_k=1&p_t=276622
[131] Juknevičiūtė, p. 23

akcentuoti ne tarptautinės, kitų valstybių ar su jomis susijusių veikėjų grėsmės, bet kibernetinių nusikaltimų klausimai, nekeliantys valstybei egzistencinės grėsmės, tačiau labiau tinkantys Prezidento gerovės valstybės vizijai.

Likusios institucijos – KST, VRM ir kariuomenė buvo gerokai pasyvesnės. Nors kiekvienos iš jų neįsitraukimą galima aiškinti skirtingai, nei VRM, nei kariuomenė, turinčios dideles platformas ir galinčios pasiekti didelę auditoriją, to nedarė, nukreipdamos išteklius į kitas sritis.

Galiausiai, ekspertai gana aktyviai komentavo visus su kibernetinės erdvės saugumu susijusius įvykius. Nepaisant mažos tyrimo imties, atsižvelgus į unikalius teikiamus pasiūlymus (technologijų pasitelkimas) ar nuolatinis tos pačios problemos akcentavimas (talentų, trūkumas tiek privačiame, tiek viešajame sektoriuose), galima teigti, kad technifikacija veikia ir Lietuvos kibernetinės erdvės saugumizavime. Per mažos politikų žinios apie šios srities saugumą ar susifokusavimas į vieną aspektą (grėsmę), neleidžia jiems pakankamai įsigilinti ir perprasti visų kibernetinės erdvės saugumo aspektų.

Grafikas 4: Saugumizuojančių veikėjų matomi grėsmės pobūdžiai



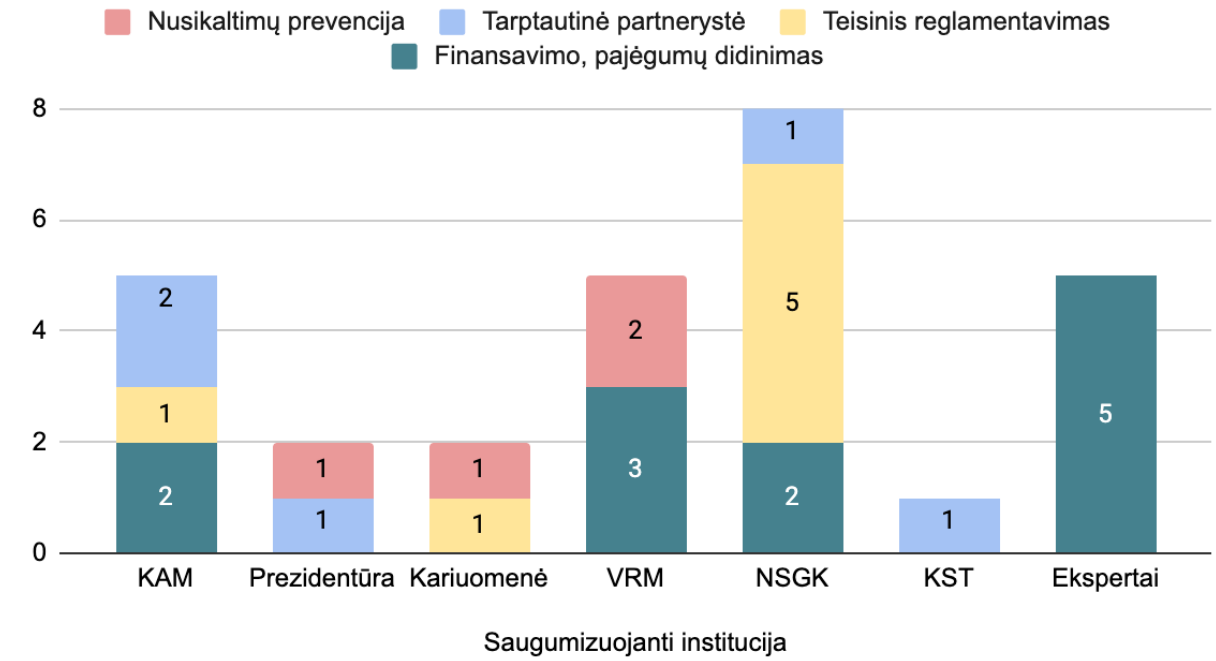
Šaltinis: sudaryta autoriaus, remiantis tyrimo duomenimis

Atsižvelgiant į agreguotus tyrimo duomenis, galima daryti išvadą, kad saugumizuojantys veikėjai taip pat per mažai dėmesio skiria referentiniams objektams – procentaliai apie tai daugiausiai kalba KAM, Prezidentūra, kariuomenė ir KST. Visgi, šiuo atveju reikėtų atsižvelgti ir į platesnį kontekstą, kuriame buvo panaudotas vienas ar kitas grėsmę apibūdinantis diskursas. Kai kuriais atvejais, net ir tiesiogiai neišreiškus pavojaus kritinei infrastruktūrai, demokratijos ar valstybės santvarkos pamatams, galima daryti išvadą, kad saugumizuojantis veikėjas mintyje visgi turėjo

referentinį objektą. Tokių atvejų galima aptikti pvz., NSGK diskurse, kalbant apie 5G ar kitų kiniškų bei rusiškų technologijų keliamą pavojų – čia sugrėsminama potenciali tokių technologijų žala tokiai infrastruktūrai kaip geležinkeliai, interneto ryšys ir kt.

Panaši situacija yra ir su siūlomomis priemonėmis. Nors teisinis reguliavimas ar finansavimo didinimas gali atrodyti kaip „kasdienė politika“, atsižvelgiant į kontekstus, kuriuose šios priemonės buvo pasiūlytos, jas galima laikyti „išeinančiomis iš kasdienės politikos rėmų“, t.y. atitinkančiomis saugumizavimo teorijos keliamus kriterijus. Tai ryškiausiai matoma su siūlomu teisiniu reglamentavimu – pavojingos technologijos draudimas iš Lietuvai nedraugiškų valstybių yra beprecedentis, o siūlomas finansavimo ar pajėgumų didinimas apima ir tokias veiklas kaip nauja ministro pareigybė ar net naujas kariuomenės padalinys.

Grafikas 5: saugumizuojančių institucijų siūlomos priemonės



Šaltinis: sudaryta autoriaus, remiantis tyrimo duomenimis

5. Saugumizuojančių institucijų ir dokumentų diskurso palyginimas

Šioje darbo dalyje bus siekiama atsakyti į pagrindinį darbo pradžioje iškeltą klausimą – ar saugumizuojančių veikėjų diskursas kibernetinės erdvės saugumo klausimais sutampa su tuo, kas deklaruojama oficialiuose dokumentuose? Kaip jau buvo minėta, tikslingas diskurso vartojimas yra viena iš esminių sąlygų būtinų sėkmingam saugumizavimui. Esantys prieštaravimai tarp to, kas jau deklaruota dokumentuose, ir to, ką kalba svarbiausios šalies gynybos politiką formuojančios, ir vykdančios institucijos gali trukdyti šiam procesui. Atvirkštinis variantas gali reikšmingai prisidėti prie to, kas jau deklaruojama dokumentuose, įgyvendinimo ir tolesnio kibernetinės erdvės saugumizavimo.

Kibernetinė erdvė buvo sėkminga saugumizuota dokumentuose. Visgi, 2015-aisiais priimtas Kibernetinio saugumo įstatymas nors ir išsamus ir puikiai teisiškai reglamentuojantis, turi būti pildomas naujais teisės aktais ar strateginiais dokumentais – kibernetinė erdvė ir joje esančios grėsmės sparčiai evoliucionuoja, o tą lemia tiek besikeičianti geopolitinė situacija, tiek technologijos. Atsižvelgiant į šį bei vėliau pasirodžiusius dokumentus, galima išskirti referentinius objektus, siūlomas nepaprastąsias priemones bei grėsmės šaltinius (*žr. lentelę nr. 9*).

9 Lentelė. Saugumizavimas dokumentuose

Referentiniai objektai	**Papildoma informacija**
• Energetika (elektra, nafta dujos, šildymas) • Transportas (geležinkeliai, keliai oro susisiekimas ir kt.) • Sveikatos apsauga • Finansų sektorius • Vandens tiekimas (geriamasis vanduo, nuotekos) • Informacinės technologijos ir ryšiai (interneto prieiga, debesija, duomenų centrai ir kt.) • Civilinė sauga • Krašto apsauga • Užsienio reikalai ir saugumas • Valstybės valdymas	Visi išvardinti objektai yra nurodyti Kibernetinio saugumo įstatymo priede „Ypatingos svarbos sektoriai, subsektoriai, paslaugos ir atsakingos institucijos“ ir patenka po kritinės infrastruktūros sąvoka. Jie taip pat yra saugumizuojami įvairiuose 2018 - 2023 metais pasirodžiusiuose dokumentuose, ypač VSD ir NKSC ataskaitose.
Siūlomos nepaprastosios priemonės	**Papildoma informacija**
• Kibernetinio saugumo pratybos • Darbuotojų mokymai • Tarptautinis bendradarbiavimas (ES, NATO, dvišalės partnerystės) • Sektoriniai kibernetinio saugumo centrai • Mokslinės inovacijos • Verslo ir viešojo sektoriaus partnerystė • Kibernetinių pajėgumų stiprinimas • Griežtesnis teisinis reguliavimas	Nepaisant to, kad kai kurios priemonės gali būti ir „kasdienės politikos“ dalimi, čia akcentuojamas ne tik jų pobūdis, bet ir mastas (tūkstančiams darbuotojų skirti mokymai, pratybos su strateginiais partneriais, naujas kariuomenės dalinys, visiškas technologijų draudimas ir kt.)
Matomos grėsmės	**Papildoma informacija**

• Kibernetinės grupuotės, tiek pavienės, tiek siejamos su Rusija, Kinija ar Iranu • Kibernetiniai nusikaltėliai • Nepatikimos technologijos • Kibernetinis šnipinėjimas • Kibernetinio saugumo reikalavimų neužtikrinimas institucijose	Šios grėsmės aptinkamos beveik visuose strateginiuose dokumentuose, nors konkrečios valstybės, keliančios kibernetinį pavojų gali būti ir neminimos, kontekstas, kuriame įvardinamos grėsmės (nepatikimos technologijos, kibernetinės atakos) leidžia teigti, kad būtent Rusija ir Kinija yra matomos pagrindinėmis agresorėmis prieš Lietuvą.

Šaltinis: sudaryta autoriaus, remiantis tyrimo duomenimis

Tuo tarpu saugumizuojantys veikėjai referentinius objektus mato kiek kitaip. Nors iš konteksto ir galima suprasti, kad saugumizuoti siekiama referentinį objektą (transporto, ryšių, krašto apsaugos ar kitą sektorių, būtiną valstybės ir visuomenės gyvenimui), šie objektai tiesiogiai paprastai neįvardinami. Visgi, tikslingiausiai kritinę infrastruktūrą saugumizavo KAM, Prezidentūra (D. Grybauskaitės laikotarpiu) ir NSGK. KAM akcentavo pavojų informacinėms technologijoms ir ryšiams, valstybės institucijoms, D. Grybauskaitė saugumizavo energetikos, transporto, finansų sektorius, valstybės valdymo pagrindus (demokratinius rinkimus), NSGK iš kitų institucijų išsiskyrė dėmesiu nepatikimoms technologijoms ir jų keliamu pavojumi interneto ir ryšių sektoriui. VRM ir Prezidentūra G. Nausėdos laikotarpiu skyrė daug dėmesio nusikaltimams kibernetinėje erdvėje, įskaitant ir vieną finansų sektoriaus (Fintech) paminėjimą. Galiausiai, kariuomenė akcentavo pavojų kritinei infrastruktūrai, nedetalizuojant konkrečių sektorių, o KST, nors ir dalyvavo saugumizavimo procese, nenurodė nei vieno ginamo objekto. Visiškai nepaminėti liko sveikatos apsaugos sistema, vandens tiekimas ir civilinė sauga.

Dokumentuose ir institucijų diskurse siūlomos priemones didele dalimi sutapo. Kibernetinio saugumo pratybas ar tarptautines partnerystes, kaip galimas priemones grėsmės užkardyti labiausiai akcentavo KAM, KST ir kariuomenė, institucijos tiesiogiai koordinuojančios ar dalyvaujančios šiose veiklose. Griežtesnis teisinis reguliavimas buvo pagrindinė NSGK komunikacijos linija, kuri kartu su KAM pasisakė ir už finansavimo ir / ar kibernetinių pajėgumų didinimą. Šioje kategorijoje atskirai reikėtų paminėti ekspertų grupę, iš kurios pasisakymų, galima teigti, kad didinamas finansavimas ir žmogiškieji ištekliai turėtų būti prioritetinė priemonė kibernetinio saugumo srityje, o viešasis ir privatus sektorius turėtų bendradarbiauti. Saugumizuojančių veikėjų nepaminėti liko sektoriniai kibernetinio saugumo valdymo centrai ir mokslinės inovacijos. Visgi, pirmasis pasiūlymas gana retai

sutinkamas ir strateginiuose dokumentuose (paminėtas tik VSD ataskaitose), tuo tarpu mokslinių inovacijų svarba turėtų būti akcentuojama labiau.

Galiausiai, dėl grėsmės šaltinių galima rasti visišką sutarimą tarp dokumentų ir to, ką akcentuoja institucijos. Rusija, Kinija ar su jomis siejomis programišių grupuotės, taip pat pavieniai veikėjai ar kibernetiniai nusikaltėliai matomi kaip pagrindiniai grėsmės šaltiniai visų institucijų atstovų.

Apibendrinant, galima pasakyti, kad **egzistuoja dalinis sutarimas tarp to, kas deklaruojama dokumentuose ir to, ką komunikuoja institucijos**. Ginamųjų ar referentinių objektų srityje tiek dokumentuose, tiek institucijų atstovų pasisakymuose įvardinami informacinių technologijų ir ryšių, transporto, krašto gynybos sektoriai, kuriems saugumizuojantys veikėjai skyrė daugiausiai dėmesio. Taip pat reikėtų paminėti ir valstybės valdymą ir energetiką – šie objektai taip pat buvo paminėti, tačiau jiems nebuvo skirtas pakankamas dėmesys (konkreti grėsmė jiems komunikuota tik viename D. Grybauskaitės pasisakyme). Visgi, reikėtų pabrėžti ir tai, kad nors iš konteksto ir galima suprasti, kad minimas vienas ar kitas referentinis objektas, konkrečių įvardinimų, tokių, kaip D. Grybauskaitės, buvo mažai. Žvelgiant iš saugumizavimo teorijos perspektyvos, tokie paminėjimai veikiausiai nebus pakankamai efektyvūs saugumizuojant dėl per mažo apibrėžtumo. Kiek geresnė situacija yra su siūlomomis priemonėmis. Gynybinių pajėgumų ar finansavimo didinimas buvo akcentuojami bene visų institucijų atstovų, tuo tarpu aktyvus teisinio reglamentavimo, kurį aktyviai minėjo NSGK, buvo sėkmingas ir nepatikimos technologijos buvo uždraustos įstatymiškai. Galiausiai, ryškiausias sutarimas matomas tarp grėsmės šaltinių: Kinija ir Rusija bei su jomis siejamos grupuotės buvo įvardinamos ir saugumizuojnačių veikėjų, ir akcentuojamos dokumentuose. Nors dėl grėsmės šaltinių ir siūlomų priemonių egzistuojantis sutarimas prisideda prie sėkmingo saugumizavimo proceso, ne visada aiškus institucijų referentinių objektų formulavimas gali tam trukdyti. Aiškiai neformuluojami ginamieji objektai gali klaidinti auditoriją, o ši – atmesti saugumizavimo bandymą, įskaitant artikuliuojamas grėsmes ir siūlomas priemones.

Reikėtų paminėti ir tai, kad kibernetinės erdvės saugumui nebuvo skiriamas pakankamas dėmesys viešojoje erdvėje. Iš tirtų institucijų labiau išsiskyrė tik NSGK, KAM ir Prezidentūra. Didžiąją dalį NSGK diskurso sudarė nepatikimos kiniškos technologijos ir su jomis siejami pasiūlymai, KAM aktyvumas nors ir padidėjęs nuo 2013 – 2015 metų laikotarpių vis tiek yra mažas, atsižvelgiant į tai, kad ši institucija yra pagrindinė krašto apsaugos politikos įgyvendintoja, o Prezidentūra, postą užėmus G. Nausėdai, kibernetinės erdvės saugumui beveik nebeskyrė dėmesio.

Išvados

Darbe pasitelkta saugumizavimo teorinė prieiga leido ištirti kibernetinės erdvės saugumizavimo procesą dokumentuose (įstatymai, strateginės koncepcijos, ataskaitos) ir pagrindinių šalies saugumo politiką formuojančių ir vykdančių institucijų diskurse 2018 – 2023 metais. Tyrimo metu buvo išanalizuoti šie dokumentai: Kibernetinio saugumo įstatymas, Nacionalinės saugumo strategijos, Nacionalinė kibernetinio saugumo strategija, grėsmių vertinimai ir kt. Tyrimui pasirinktos institucijos: KAM, Prezidentūra, NSGK, KST, VRM, kariuomenė ir kibernetinio saugumo ekspertai.

Saugumizavimo teorinė prieiga leido įvardinti referentinius (saugotinus) objektus, grėsmių šaltinius ir siūlomas nepaprastąsias priemones referentiniams objektams apsaugoti, nurodytus minėtuose dokumentuose ir aptiktus tiriamų institucijų diskurse. Pagal šiuos kriterijus buvo atliktas palyginimas, siekiant išsiaiškinti ar tai, kas deklaruojama dokumentuose ir tai, ką komunikuoja tirtos institucijos sutampa. Saugumizavimas yra kalbos aktas, todėl siekiant sėkmingo rezultato tai turi būti daroma tikslingai – aiškiai formuluojant referentinius objektus, grėsmes ir siūlomas priemones.

Atsižvelgiant į tai, darbo pradžioje iškeltus tikslus galima apibendrinti:

1) Saugumizavimo studijos jau yra pakankamai pažengusios kibernetinės erdvės saugumo tyrimuose. Pasitelkiant šią teorinę prieigą, buvo tiriami Estijos, JAV ir kitų valstybių kibernetinės erdvės saugumizavimo procesai. Šių tyrimų metu mokslininkai pastebėjo, kad kibernetinės erdvės saugumizavimo specifika turi savų niuansų – hipersaugumizavimą, nurodantį polinkį hiperbolizuoti galimas problemas ir atsirandantį iš empirinių atvejų trūkumo, kasdienes saugumo praktikas, kurias akcentuojant siekiama parodyti, kad kibernetinės atakos palies ir eilinius gyventojus, bei technifikaciją, nurodančią kibernetinės erdvės sudėtingumą ir neprieinamumą asmenims, nesantiems šios srities ekspertais.
2) **Pirmasis ginamasis teiginys** („Nepaisant sėkmingo saugumizavimo 2015-aisiais, kibernetinė erdvė oficialiuose dokumentuose saugumizuojama ir toliau“), atsižvelgus į tyrimo rezultatus, **laikomas apgintu**. Strateginių dokumentų analizė parodė, kad ir po 2015-ųjų kibernetinė erdvė ir toliau buvo saugumizuojama, įvardinant referentinius objektus, grėsmės bei siūlant nepaprastąsias priemones grėsmėms užkardyti. Kibernetinės erdvės saugumas kaip prioritetinis ir toliau buvo akcentuojamas Nacionalinėse saugumo strategijose, KAM strategijoje ir doktrinoje, Nacionalinėje kibernetinio saugumo strategijoje ir kituose dokumentuose. Šį procesą lėmė ne tik niekur nedingusios, bet ir išaugusios kibernetinės grėsmės iš Kinijos, Rusijos ar programišių grupuočių, taip pat sparčiai besikeičianti geopolitinė situacija ir technologinė raida.
3) **Antrasis ginamasis teiginys** („Krašto saugumo politiką formuojančios ir įgyvendinančios institucijos ir jų atstovai viešojoje erdvėje prisideda prie tolesnio

kibernetinės erdvės saugumizavimo“) **laikomas dalinai apgintu**. Tyrimo rezultatai parodė, kad krašto apsaugos politiką formuojančios ir įgyvendinančios institucijos prisideda prie šio proceso, tačiau tai daro ganėtinai ribotai – tik NSGK, KAM ir D. Grybauskaitės laikotarpio Prezidentūra tai darė aktyviau. Likusios institucijos komunikavo ganėtinai pasyviai ar kibernetinės erdvės saugumo neprioretizavo, šią sritį laikant kaip dar viena iš daugelio grėsmių, su kuria susiduria Lietuva. Tuo tarpu ganėtinai mažas bendras pareiškimų viešojoje erdvėje apie kibernetinį saugumą skaičius ir pasyvus kai kurių institucijų komunikavimas neleidžia daryti išvados, kad tai daroma pakankamai efektyviai.

4) Lietuvos kibernetinę erdvę saugumizuoti pavyko tik 2015-aisiais, įsigaliojus Kibernetinio saugumo įstatymui, nors pirmieji bandymai įtvirtinti šį klausimą įstatymuose ir kituose dokumentuose atsirado dar 1996-aisiais. Visgi, iki pat minėto įstatymo priėmimo, tai buvo gana padriki bandymai, su nepakankamai apibrėžtu teisiniu reguliavimu ir kitomis problemomis.
5) Institucijų ir strateginių dokumentų panašumai buvo labiausiai matomi įvardinant grėsmes (Rusija, Kinija, programišių grupuotės, nepatikimos technologijos, naudojamos ir kritinėje infrastruktūroje). Taip pat, sutapo ir nemažai siūlomų priemonių grėsmėms užkardyti – griežtesnis teisinis reguliavimas, kibernetinių pajėgumų ar finansavimo didinimas. Šios priemonės dėl siūlomo masto laikytinos išeinančiomis iš kasdienės politikos rėmų, taigi atitinkančiomis saugumizavimo teorijoje nurodomus kriterijus. Visgi, reikėtų pabrėžti, kad institucijų atstovai gana aptakiai įvardino referentinius objektus. Vos keli saugumizuojantys veikėjai, tarp kurių yra ir D. Grybauskaitė, NSGK ar KAM atstovai tiksliau ir aktyviau komunikavo apie tokius referentinius objektus kaip energetikos, transporto, krašto apsaugos sektoriai ar demokratinė santvarka. Tokia situacija gali lemti saugumizavimo nesėkmę – nepakankamas konkrečių grėsmių artikuliavimas, neparodymas kaip jos paveiks eilinius piliečius gali trukdyti auditorijos paramos užsitikrinimą, šiai nepripažįstant konkretaus referentinio objekto. Tai apsunkintų ir priemonių, skirtų grėsmių užkardymui, diegimą.

Nors dalinis sutarimas tarp institucijų diskurso ir to, kas užtvirtinta dokumentuose yra, vienareikšmiškai negalima teigti, kad politikų, ekspertų ar kariškių naudojamas diskursas prisideda prie kibernetinės erdvės saugumizavimo. Per penkerių metų laikotarpį aptikti tik 49 vieši institucijų atstovų pasisakymai rodo, kad šiai sričiai dėmesio nėra skiriama pakankamai, pati komunikacija (su keliomis išimtimis) yra ganėtinai padrika.

Atsižvelgiant į tyrimo rezultatus, augančią Rusijos, Kinijos ir kitų valstybių ar su jomis siejamų programišių grupuočių agresyvią veiklą kibernetinėje erdvėje, rekomenduojama:

1) Lietuvos institucijoms, formuojančioms ir įgyvendinančioms krašto apsaugos politiką aktyviau komunikuoti apie kibernetines grėsmes viešojoje erdvėje. Kariuomenė, Prezidentūra (valdant G. Nausėdai), KST ir VRM kibernetinės erdvės saugumo neakcentuoja kaip prioritetinio klausimo, nepaisant augančios grėsmės, kaip nurodo VSD ir kitos ataskaitos.
2) Komunikuojant apie kibernetinės erdvės saugumą, siūlytina dažniau tiesiogiai nurodyti referentinius objektus (kritinę infrastruktūrą) bei kaip išpuoliai prieš juos paveiktų eilinių piliečių kasdienybę. Aiškus referentinių objektų įvardinimas yra būtina saugumizavimo sąlyga, o paralelės tarp atakos prieš kritinę infrastruktūrą ir poveikį žmonių kasdienybei (kasdienės saugumo praktikos), kaip rodo kibernetinės erdvės saugumizavimo tyrimai, gali prisidėti prie sėkmingo saugumizavimo.
3) Glaudesnis darbas ir konsultacijos su kibernetinio saugumo ekspertais leistų institucijoms saugumizuojant kibernetinę erdvę pateikti platesnį pasiūlymų spektrą, taip prisidedant prie grėsmių užkardymo.

Summary

The master thesis "Securitization of cyberspace in Lithuania 2018 – 2023" aims to study how well the institutions, responsible for shaping and implementing national security strategies, align their public cyber security discourse with what is already embedded in strategic documents. From the perspective of the theory of securitization, this aspect plays a major role in further securitization, since incoherent use of discourse can tamper the whole process. Due to evolving threats and everchanging geopolitical position, resulting in significant threats from Russia, China and other international actors, it is held that the process of cyberspace securitization in Lithuania is continuous rather than already finished. This claim was also proven during the analysis part of the document.

The paper first analyses the theoretical background on securitization, starting with its beginnings in the Copenhagen school, criticism of the theory, and the adaptations of it in the field in cybersecurity. This has also allowed for creation of criteria, which was used to identify referential objects, existential threats and extraordinary measures, which were later used for studying documents and institutional discourse. The paper then analyzes how cyberspace was securitized in strategic documents and laws in Lithuania in 2015, with the passing of the National law on cybersecurity, as well as prior unsuccessful attempts, starting with 1996, to have a full understanding of the process in the country. The analysis part concludes with an analysis of strategic documents and laws passed between 2018 and 2023. They were later compared to the public institutional discourse of the same period – 49 public statements from institutions and 10 from cybersecurity experts were analyzed.

The findings of the analysis are as follows:

- Despite the successful securitization back in 2015, Lithuanian cyberspace is being continuously securitized, as it appears as an important aspect of national security in all major documents that determine Lithuanian national security.
- Various institutions that shape and implement Lithuanian national security politics also participate in the process, however, rather vaguely. Only three out of seven that were studied did it more actively. This includes the President (during D. Grybauskaitė's presidency), the Committee for National Security and Defense, and the Ministry of Defense. The rest were rather idle or did not see cybersecurity as a matter of priority. This partially confirms the hypothesis that said institutions are an important factor in securitizing cyberspace.
- The discourse of these institutions also partially matches to what is laid out in strategic documents. The threat of China, Russia and hacker groups appears both in the documents and discourse of representatives of institutions. The same can be said about suggest measures (suggested increase of funding, defensive capabilities, stricter judicial regulations). However, there are some discrepancies on referential objects: strategic documents tend to emphasize

critical infrastructure more often, while the institutional discourse was broader, except for D. Grybauskatė, the Committee for National Security and Defense, and the Ministry of Defense, which mostly emphasized the same referential object.

The findings allowed for recommendations to be made, which include more frequent communication and securitizing of cyberspace from all analyzed institutions, as well as more coherent and accurate discourse on referential objects.

Literatūros sąrašas

Akademinė literatūra

1. Balzacq, Thierry, Léonard, Sarah, Ruzicka, Jan, „'Securitization' revisited: theory and cases", *International Relations*, Vol. 30(4), 2016 m.
2. Buzan, Barry, Waever, Ole, de Wilde, Jaap, „Security: a New Framework for Analysis, Lynne Rienner Publishers", 1998 m.
3. Cavelty, Myriam Dunn, Egloff, Florian J., „Hyper-Securitization, Everyday Security Practice and Technification: Cyber-Security Logics in Switzerland", *Swiss Political Science Review 27(1)*
4. Collins, Alan, „Securitization, Frankenstein's Monster and Malaysian education", *The Pacific Review*, 18:4, 2005 m.
5. Gomez, Miguel Alberto, Whyte, Christopher, „Breaking the Myth of Cyber Doom: Securitization and Normalization of Novel Threats", *International Studies Quarterly* 65, 2021 m.
6. Hansen, Hansen, Nissenbaum, Helen, „Digital Disaster, Cyber Security, and the Copenhagen School", *International Studies Quarterly*, Vol. 53, Nr. 4, 2009 m.
7. Juknevičiūtė, Ieva, „Kibernetinės erdvės saugumizavimas Lietuvoje" (Bakalauro darbas, Vilniaus universitetas, Tarptautinių santykių ir politikos mokslų institutas, 2016)
8. Lobato, Luisa Cruz, Kenkel, Kai Michael, „Discourses of cyberspace securitization in Brazil and in the United States", internete: <https://www.scielo.br/j/rbpi/a/zDC3D9BWxQvBxk56CmLdckJ/?lang=en>
9. Orenius , Algirdas, „1990–2002 m. Lietuvos krašto apsaugos politikos raidos analizė", *Viešoji politika ir administravimas*, Nr. 6 (2003), Lietuvos teisės universitetas
10. Ottis, Rain, „Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective", *Cooperative Cyber Defence Centre of Excellence,* Talinas, 2008, žiūrėta 2023 m. sausio 12 d., https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf
11. Salter, Mark B., „When securitization fails: The hard case of counter-terrorism programs", *Securitization Theory,* Routledge, 2010 m.
12. Štitilis, Darius, Klišauskas, Valdas, „Aspets of cybersecurity: the case of legal regulation in Lithuania", *Journal of security and sustainability issues*, Volume 5, No 1 (2015)

13. Waever, Ole, Chapter 3, „Securitization and Desecuritization“, „On Security“, sud. Ronnie D Lipschutz, New York: Columbia University Press, 1995 m.

Straipsniai naujienų portaluose

14. 15min, „15/15: ar Lietuvos valstybinės institucijos turėtų drausti naudoti „TikTok“?“, 12:25 – 12:45, žiūrėta 2023 m. gegužės 5 d., https://www.15min.lt/ikrauk/video/1515-ar-lietuvos-valstybines-institucijos-turetu-drausti-naudoti-tiktok-235716
15. 15min, „Ekspertai: energetikos sektoriui teks įveikti ne tik tiekimo, bet ir kibernetinio saugumo krizę”, žiūrėta 2023 m. gegužės 1 d., https://www.15min.lt/verslas/naujiena/energetika/ekspertai-energetikos-sektoriui-teks-iveikti-ne-tik-tiekimo-bet-ir-kibernetinio-saugumo-krize-664-1927278
16. 15min, „Lietuvos geležinkeliai“ susiduria su kibernetinėmis atakomis: bendrovių svetainės gali būti laikinai nepasiekiamos“, BNS, žiūrėta 2023 m. gegužės 1 d., https://www.15min.lt/verslas/naujiena/mokslas-it/lietuvos-gelezinkeliai-susiduria-su-kibernetinemis-atakomis-bendroviu-svetaines-gali-buti-laikinai-nepasiekiamos-1290-1733878
17. 15min, „Nacionalinio kibernetinio saugumo centre Kaune apsilankęs prezidentas ragino nesustoti“, BNS, žiūrėta 2023 m. gegužės 1 d., https://www.15min.lt/naujiena/aktualu/lietuva/nacionalinio-kibernetinio-saugumo-centre-kaune-apsilankes-prezidentas-ragino-nesustoti-56-1256878
18. 15min, „Saugumo ekspertas: Lietuva – Rusijos kibernetinių atakų taikinių dešimtuke”, žiūrėta 2023 m. gegužės 3 d., https://www.15min.lt/verslas/naujiena/mokslas-it/saugumo-ekspertas-lietuva-rusijos-kibernetiniu-ataku-taikiniu-desimtuke-1290-1024966
19. 15min.lt, „Vyriausybė patvirtino kibernetinio saugumo strategiją“, žiūrėta 2023 m. gegužės 5 d., https://www.15min.lt/verslas/naujiena/mokslas-it/vyriausybe-patvirtino-lietuvos-kibernetinio-saugumo-strategija-1290-1014484
20. Andrukaitytė, Milena, „A.Anušauskas matytų poreikį už kibernetinį saugumą atsakingam viceministrui“, 15min, žiūrėta 2023 m. gegužės 5 d., https://www.15min.lt/naujiena/aktualu/lietuva/a-anusauskas-matytu-poreiki-uz-kibernetini-sauguma-atsakingam-viceministrui-56-1995714
21. Andrukaitytė, Milena, „G. Nausėda ragina atidžiau tirti korupcinius ir kibernetinius nusikaltimus“, BNS, žiūrėta 2023 m. gegužės 1 d., https://m.kauno.diena.lt/naujienos/lietuva/politika/g-nauseda-susitinka-su-generaline-prokurore-aptars-nusikalstamumo-tendencijas-1070959

22. Anušauskas, Arvydas, „Arvydas Anušauskas. 2022 metais sukūrėme stipresnę, modernesnę ir geriau organizuotą krašto apsaugos sistemą“, LRT, , žiūrėta 2023 m. gegužės 3 d., https://www.lrt.lt/naujienos/pozicija/679/1855987/arvydas-anusauskas-2022-metais-sukureme-stipresne-modernesne-ir-geriau-organizuota-krasto-apsaugos-sistema
23. Aušra, Mindaugas, „Uždrausti kiniški rentgenai įdarbinti Lietuvos muitinėje, gamintojai ruošia ieškinį teismui“, LRT, žiūrėta 2023 m. gegužės 1 d., https://www.lrt.lt/naujienos/lrt-tyrimai/5/1367222/uzdrausti-kiniski-rentgenai-idarbinti-lietuvos-muitineje-gamintojai-ruosia-ieskini-teismui
24. Balčiūnaitė, Sniegė, „M.Pareščius: reikia rezervinio interneto, geresnės kompiuterių apsaugos“, BNS, žiūrėta 2023 m. gegužės 1 d., https://www.15min.lt/verslas/naujiena/mokslas-it/m-parescius-reikia-rezervinio-interneto-geresnes-kompiuteriu-apsaugos-1290-1650516
25. Balčūnas, Andrius, „Krašto apsaugos viceministras: silpniausia kibernetinio saugumo grandis yra žmonės“, LRT, žiūrėta 2023 m. gegužės 1 d., https://www.lrt.lt/naujienos/lietuvoje/2/720113/krasto-apsaugos-viceministras-silpniausia-kibernetinio-saugumo-grandis-yra-zmones
26. Bieliavska, Jadvyga, „L. Kasčiūnas: grėsmių saugumui pristatymas – savotiškas priešnuodis“, ELTA, žiūrėta 2023 m. balandžio 19 d. https://www.diena.lt/naujienos/lietuva/politika/l-kasciunas-gresmiu-saugumui-pristatymas-savotiskas-priesnuodis-1014647
27. BNS, „Belgija, Slovėnija jungiasi prie Lietuvos vadovaujamų ES kibernetinių pajėgų“, žiūrėta 2023 m. gegužės 2 d., https://www.lrt.lt/naujienos/lietuvoje/2/1931984/belgija-slovenija-jungiasi-prie-lietuvos-vadovaujamu-es-kibernetiniu-pajegu
28. BNS, „Prezidentūra: per rinkimus tikėtinos Rusijos kibernetinės atakos“, 15min, žiūrėta 2023 m. gegužės 3 d., https://www.15min.lt/naujiena/aktualu/lietuva/preizdentura-per-rinkimus-tiketinos-rusijos-kibernetines-atakos-56-1084732
29. Delfi, „Kasčiūnas: kibernetinio saugumo kartelę reikia kelti ne baudomis, o sveika verslo konkurencija“, žiūrėta 2023 m. gegužės 2 d., https://www.delfi.lt/verslo-poziuris/diskusijos/kasciunas-kibernetinio-saugumo-kartele-reikia-kelti-ne-baudomis-o-sveika-verslo-konkurencija-86874991
30. Gutauskaitė, Irtautė, Masiokaitė-Liubinienė, Austėja, „NSGK pirmininkas siūlo neleisti pareigūnams naudotis „Tik Tok“: asmeninė informacija gali būti panaudota šantažui“, ELTA, BNS, 2023 m. balandžio 29 d., https://www.lrt.lt/naujienos/lietuvoje/2/1926029/nsgk-pirmininkas-siulo-neleisti-pareigunams-naudotis-tik-tok-asmenine-informacija-gali-buti-panaudota-santazui

31. Jačauskas, Ignas, „A.Anušauskas: kiberatakų organizatoriai ieško silpnų vietų, galimi išpuoliai prieš verslą“, BNS, žiūrėta 2023 m. gegužės 5 d., https://www.15min.lt/naujiena/aktualu/lietuva/a-anusauskas-kiberataku-organizatoriai-iesko-silpnu-vietu-galimi-ispuoliai-pries-versla-56-1742794
32. Jačauskas, Ignas, „NSGK vadovas: nesaugios kameros turi būti išmontuotos, jei spragų pašalinti neįmanoma“, BNS, 2023 m. balandžio 29 d., https://www.15min.lt/naujiena/aktualu/lietuva/nsgk-vadovas-nesaugios-kameros-turi-buti-ismontuotos-jei-spragu-pasalinti-neimanoma-56-1324280
33. Jakubauskas, Ramūnas, „KAM ketina mokėti didesnes algas kibernetinio saugumo specialistams“, BNS, žiūrėta 2023 m. gegužės 5 d., https://m.diena.lt/naujienos/lietuva/salies-pulsas/kam-ketina-moketi-didesnes-algas-kibernetinio-saugumo-specialistams-1063288
34. Jūratė Skėrytė, „Partijų susitarime – nauja kariuomenės rūšis, pasirengimas priimti diviziją“, žiūrėta 2023 m. gegužės 1 d., https://www.lrt.lt/naujienos/lietuvoje/2/1674746/partiju-susitarime-nauja-kariuomenes-rusis-pasirengimas-priimti-divizija
35. Login.lt, „Didėjantys kibernetinio saugumo iššūkiai verčia IT specialistus keisti profesiją“, žiūrėta 2023 m. gegužės 3 d., https://www.delfi.lt/login/progresas/kibernetinis-saugumas/didejantys-kibernetinio-saugumo-issukiai-vercia-it-specialistus-keisti-profesija.d?id=90785649
36. Lrytas, „Pristatomi svarbiausi Lietuvos kibernetinio saugumo skaičiai ir tendencijos“, žiūrėta 2023 m. gegužės 2 d., https://www.lrytas.lt/it/ismanyk/2022/05/17/news/pristatomi-svarbiausi-lietuvos-kibernetinio-saugumo-skaiciai-ir-tendencijos-23381002
37. LRT, „Ekspertas apie kibernetinį saugumą: Lietuvoje yra du tipai įmonių – nulaužtos ir tos, kurios dar bus nulaužtos“, žiūrėta 2023 m. gegužės 1 d., https://www.lrt.lt/naujienos/mokslas-ir-it/11/1733755/ekspertas-apie-kibernetini-sauguma-lietuvoje-yra-du-tipai-imoniu-nulauztos-ir-tos-kurios-dar-bus-nulauztos
38. LRT, „Kibernetinio saugumo specialistas: daugelis valstybinių institucijų sėdi tarsi ant tiksinčios bombos“, žiūrėta 2023 m. gegužės 3 d., https://www.lrt.lt/naujienos/mokslas-ir-it/11/1521165/kibernetinio-saugumo-specialistas-daugelis-valstybiniu-instituciju-sedi-tarsi-ant-tiksincios-bombos
39. LRT, „Rupšys: JAV Pensilvanijos gvardija – vienas saugumo garantų Baltijos regione“ BNS, žiūrėta 2023 m. gegužės 1 d., https://www.lrt.lt/naujienos/lietuvoje/2/1834193/rupsys-jav-pensilvanijos-gvardija-vienas-saugumo-garantu-baltijos-regione
40. LRT.lt, „Lietuva ir Izraelis sutarė glaudžiau bendradarbiauti kibernetinio saugumo srityje“, žiūrėta 2023 m. gegužės 5 d., https://www.lrt.lt/naujienos/lietuvoje/2/1927501/lietuva-ir-izraelis-sutare-glaudziau-bendradarbiauti-kibernetinio-saugumo-srityje

41. Meškauskas, Giedrius, „Giedrius Meškauskas: „Killnet“ kibernetinė ataka – kokia kariuomenė, tokie ir hakeriai“, 15min, žiūrėta 2023 m. gegužės 1 d., https://www.15min.lt/naujiena/aktualu/nuomones/giedrius-meskauskas-killnet-kibernetine-ataka-kokia-kariuomene-tokie-ir-hakeriai-18-1742384
42. Naprys, Ernestas, „Lietuvos oro erdvę stebi rusiški radarai ir sistemos – NSGK nurodo jas keisti, kainuos 15 milijonų“, žiūrėta 2023 m. gegužės 1 d., https://www.15min.lt/verslas/naujiena/finansai/lietuvos-oro-erdve-stebi-rusiski-radarai-ir-sistemos-nsgk-nurodo-jas-keisti-kainuos-15-milijonu-662-979342
43. Naureckaitė, Indrė, „Atskleidus apie valstybinės įmonės pirkimo iš Rusijos planą – sujudimas: Seimo nariai imasi veiksmų“, žiūrėta 2023 m. gegužės 1 d., https://www.lrytas.lt/lietuvosdiena/aktualijos/2023/02/21/news/atskleidus-apie-valstybines-imones-pirkimo-is-rusijos-plana-sujudimas-seimo-nariai-imasi-veiksmu-26200127
44. Neverauskas, Vaidas, „Telia“ technikos vadovas: naujas „Huawei“ saugesnis nei senas „iPhone“, 15min, žiūrėta 2023 m. gegužės 1 d., https://www.15min.lt/verslas/naujiena/mokslas-it/telia-technikos-vadovas-naujas-huawei-saugesnis-nei-senas-iphone-1290-929746
45. NRD Cyber Security, „Ypatingos svarbos infrastruktūros apsauga nuo kibernetinių grėsmių: ką turime žinoti“, vz.lt, žiūrėta 2023 m. gegužės 5 d., https://www.vz.lt/verslo-sprendimai/2020/10/29/ypatingos-svarbos-infrastrukturos-apsauga-nuo-kibernetiniu-gresmiu-ka-turime-zinoti#ixzz80rJKHDIV
46. Okmanas, Tomas, „T.Okmanas: 5 svarbiausios kibernetinio saugumo idėjos iš šių metų Davoso“, žiūrėta 2023 m. gegužės 3 d., https://www.15min.lt/verslas/naujiena/mokslas-it/penki-svarbiausi-t-okmano-ispudziai-po-renginio-1290-1687206
47. Pumprickaitė, Nemira, „Anušauskas apie pavojus dėl Kinijoje pagamintų telefonų: tūkstančiai nupirkta valstybės institucijoms dėl to, kad pigiau kainuoja“, LRT, žiūrėta 2023 m. gegužės 2 d., https://www.lrt.lt/naujienos/mokslas-ir-it/11/1501190/anusauskas-apie-pavojus-del-kinijoje-pagamintu-telefonu-tukstanciai-nupirkta-valstybes-institucijoms-del-to-kad-pigiau-kainuoja
48. Samoškaitė, Eglė, „Politikai: kibernetinės atakos prieš DELFI – atakos prieš valstybę“, LRT, https://www.lrt.lt/naujienos/lietuvoje/2/18644/politikai-kibernetines-atakos-pries-delfi-atakos-pries-valstybe (žiūrėta 2023 m. balandžio 24 d.)
49. Skamarkaitė, Agnė, „Ekspertas apie Rusijos programišių paskelbtą kibernetinį karą: rimtesnėms atakoms visiškai pasiruošusi nėra nė viena Baltijos valstybė“, žiūrėta 2023 m. gegužės 3 d., https://www.lrt.lt/naujienos/mokslas-ir-it/11/1697582/ekspertas-apie-rusijos-

programisiu-paskelbta-kibernetini-kara-rimtesnems-atakoms-visiskai-pasiruosusi-nera-ne-viena-baltijos-valstybe

50. Stankevičius, Augustas, „Prieš KAM svetainę gegužę įvykdyta masyvi kibernetinė ataka: Lietuvoje jos dažnėja ir sudėtingėja“, BNS, žiūrėta 2023 m. gegužės 5 d., https://www.15min.lt/verslas/naujiena/mokslas-it/pries-kam-svetaine-geguze-ivykdyta-masyvi-kibernetine-ataka-1290-1681544
51. TV3, „DIENOS PJŪVIS. Kibernetinės atakos prieš Lietuvą: kokie pavojai ir kaip reaguoti?“, žiūrėta 2023 m. gegužės 1 d.,https://www.tv3.lt/naujiena/video/dienos-pjuvis-kibernetines-atakos-pries-lietuva-kokie-pavojai-ir-kaip-reaguoti-n1109634
52. Venckūnas, Vilmantas, „Kasčiūnas – apie pandemijos apnuogintas spragas, Rusijos žingsnį į priekį ir kodėl nepirktų „Huawei“ telefono“, žiūrėta 2023 m. balandžio 28 d., https://www.tv3.lt/naujiena/lietuva/kasciunas-apie-pandemijos-apnuogintas-spragas-rusijos-zingsni-i-prieki-ir-kodel-nepirktu-huawei-telefono-n1090368
53. Venckūnas, Vilmantas, „Kelią skinasi kiniškos įrangos draudimas – apsaugotų nuo nesaugaus 5G ryšio“, BNS, žiūrėta 2023 gegužės 9 d., https://www.tv3.lt/naujiena/lietuva/kelia-skinasi-kiniskos-irangos-draudimas-apsaugotu-nuo-nesaugaus-5g-rysio-n1092524

Valstybės institucijų pranešimai

1. CERT-LT, „2017 Metų veiklos ataskaita“, 2017, žiūrėta 2023 m. balandžio 26 d. https://www.nksc.lt/doc/2017.pdf
2. KAM, „Įsigalioja ES direktyva, kuria bus siekiama didinti atsparumą kibernetinėms grėsmėms“, žiūrėta 2023 m. gegužės 1 d., https://kam.lt/isigalioja-es-direktyva-kuria-bus-siekiama-didinti-atsparuma-kibernetinems-gresmems/
3. KAM, „Kibernetinio saugumo taryboje aptarti svarbiausi metų įvykiai ir būsimi pokyčiai“, žiūrėta 2023 m. gegužės 1 d., https://kam.lt/kibernetinio-saugumo-taryboje-aptarti-svarbiausi-metu-ivykiai-ir-busimi-pokyciai/
4. KAM, „Nauju teisės aktu ES bus siekiama didinti techninės ir programinės įrangos kibernetinį saugumą“ žiūrėta 2023 m. gegužės 1 d., https://kam.lt/nauju-teises-aktu-es-bus-siekiama-didinti-technines-ir-programines-irangos-kibernetini-sauguma/
5. Lietuvos bankas, „Kibernetinėmis atakomis bandyta sutrikdyti Lietuvos banko paslaugų teikimą internetu“, pranešimas žiniasklaidai, 2012, https://www.lb.lt/lt/naujienos/kibernetinemis-atakomis-bandyta-sutrikdyti-lietuvos-banko-paslaugu-teikima-internetu (žiūrėta 2023 m. balandžio 24 d.)

6. Lietuvos kariuomenė, „Gynybos štabas organizavo kibernetinės gynybos pratybas“, žiūrėta 2023 m. balandžio 27 d., https://www.kariuomene.lt/kas-mes-esame/naujienos/gynybos-stabas-organizavo-kibernetines-gynybos-pratybas/21402
7. Lietuvos Respublikos Seimas, „Nacionalinio saugumo ir gynybos komitetas išklausė informaciją apie penktosios kartos judriojo ryšio (5G) plėtrą Lietuvoje ir galimus saugumo iššūkius“, žiūrėta 2023 gegužės 9 d., https://www.lrs.lt/sip/portal.show?p_r=36014&p_k=1&p_t=271506
8. Lietuvos Respublikos Seimas, „Nacionalinio saugumo ir gynybos komitetas priėmė sprendimą dėl valstybės institucijose naudojamos nesaugios vaizdo stebėjimo įrangos“, žiūrėta 2023 gegužės 9 d., https://www.lrs.lt/sip/portal.show?p_r=36014&p_k=1&p_t=271401
9. Lietuvos Respublikos Seimas, „Nacionalinio saugumo ir gynybos komitetas inicijuoja Nacionalinio saugumo strategijos peržiūrą “, žiūrėta 2023 gegužės 9 d., https://www.lrs.lt/sip/portal.show?p_r=38447&p_k=1&p_t=273457
10. Lietuvos Respublikos Seimas, „NSGK prašo įvertinti „Huawei“ telefonų patikimumą“, žiūrėta 2023 gegužės 9 d., https://www.lrs.lt/sip/portal.show?p_r=36014&p_k=1&p_t=255710
11. Lietuvos Respublikos Seimas, „Seimas pritarė, kad nepatikimi gamintojai ir tiekėjai Lietuvoje negalėtų dalyvauti elektroninių ryšių rinkoje, ypač diegiant penktos kartos mobiliųjį 5G ryšį“, žiūrėta 2023 gegužės 9 d., https://www.lrs.lt/sip/portal.show?p_r=35435&p_k=1&p_t=276622
12. Lietuvos Respublikos Seimas, „Seime bus aptariamos hibridinės grėsmės ir Vakarų valstybių pasirengimas jas atremti“, žiūrėta 2023 gegužės 9 d., https://www.lrs.lt/sip/portal.show?p_r=38447&p_k=1&p_t=275488
13. Lietuvos Respublikos Seimas, „Seimo NSGK pirmininkas V. Bakas: „Energetikos sektoriuje būtinas ypatingas dėmesys kibernetiniam saugumui“, žiūrėta 2023 gegužės 9 d., https://www.lrs.lt/sip/portal.show?p_r=36014&p_k=1&p_t=256561
14. Lietuvos Respublikos Seimas, „Seimo NSGK pirmininko V. Bako pranešimas: „Rusijos hibridinio karo arsenalas apima visą priemonių kompleksą“, žiūrėta 2023 gegužės 9 d., https://www.lrs.lt/sip/portal.show?p_r=36014&p_k=1&p_t=265425
15. Lietuvos Respublikos Seimas, A. Paulausko kalba Seimo vakarinio posėdžio Nr.203 metu, https://e-seimas.lrs.lt/portal/legalAct/lt/TAK/0f03aec0755f11e4b615a833d6e7da3d (žiūrėta 2023 m. balandžio 24 d.)
16. Lietuvos Respublikos Seimas, Seimo NSGK pirmininko A. Paulausko pranešimas: „Kibernetinė gynyba turi tapti krašto gynybos dalimi“, Vilnius, 2014,

https://www3.lrs.lt/pls/inter/w5_show?p_r=618&p_d=147140&p_k=1 (žiūrėta 2023 m. balandžio 24 d.)

17. LRV, „Vyriausybei išplėtus ypatingos svarbos informacinės infrastruktūros sąrašą, daugiau įmonių privalės skirti ypatingą dėmesį savo kibernetinio saugumo užtikrinimui“, žiūrėta 2023 m. gegužės 1 d., https://lrv.lt/lt/naujienos/vyriausybei-ispletus-ypatingos-svarbos-informacines-infrastrukturos-sarasa-daugiau-imoniu-privales-skirti-ypatinga-demesi-savo-kibernetinio-saugumo-uztikrinimui
18. Prezidentės spaudos tarnyba, „Davose – Lietuvos kibernetinio saugumo patirtis“, žiūrėta 2023 m. gegužės 3 d., https://grybauskaite.lrp.lt/lt/spaudos-centras/pranesimai-spaudai/31744
19. Prezidentės spaudos tarnyba, „Lietuvos Respublikos Prezidentės Dalios Grybauskaitės metinis pranešimas“, žiūrėta 2023 m. gegužės 3 d., https://grybauskaite.lrp.lt/lt/spaudos-centras/pranesimai-spaudai/30197
20. Prezidentės spaudos tarnyba, „Lietuvos Respublikos Prezidentės Dalios Grybauskaitės metinis pranešimas“, žiūrėta 2023 m. gegužės 3 d., https://www.lrp.lt/lt/lietuvos-respublikos-prezidentes-dalios-grybauskaites-metinis-pranesimas/32606
21. Prezidentės spaudos tarnyba, „Prezidentė paragino stiprinti taiką Europoje“, žiūrėta 2023 m. gegužės 3 d., https://grybauskaite.lrp.lt/lt/spaudos-centras/pranesimai-spaudai/30487
22. Prezidento žiniasklaidos centras: „Prezidento kalba JTGA: kurti visuotinę gerovę mums yra aukščiausias priesakas“, žiūrėta 2023 m. gegužės 1 d., https://www.lrp.lt/lt/ziniasklaidos-centras/naujienos/prezidento-kalba-jtga-kurti-visuotine-gerove-mums-yra-auksciausias-priesakas/33141
23. VRM, „Susitikime su Europolo direktore aptartos nusikalstamumo tendencijos“, žiūrėta 2023 m. gegužės 1 d., https://vrm.lrv.lt/lt/naujienos/susitikime-su-europolo-direktore-aptartos-nusikalstamumo-tendencijos
24. VRM, „Vidaus reikalų ministras pasirašė memorandumą dėl rizikų valdymų „fintech“ srityje“, žiūrėta 2023 m. gegužės 1 d., https://vrm.lrv.lt/lt/naujienos/vidaus-reikalu-ministras-pasirase-memoranduma-del-riziku-valdymu-fintech-srityje
25. VRM, „VRM: prekyba žmonėmis – didžiausi pavojai tyko skaitmeninėje erdvėje“, žiūrėta 2023 m. gegužės 1 d., https://vrm.lrv.lt/lt/naujienos/vrm-prekyba-zmonemis-didziausi-pavojai-tyko-skaitmenineje-erdveje
26. VRM, „VST ir policija stiprina bendradarbiavimą dėl strateginių objektų apsaugos“, žiūrėta 2023 m. gegužės 1 d., https://vrm.lrv.lt/lt/naujienos/vst-ir-policija-stiprina-bendradarbiavima-del-strateginiu-objektu-apsaugos

Teisės aktai, strateginiai dokumentai

27. Krašto apsaugos ministerija, „Nacionalinė kibernetinio saugumo strategija", 2018, žiūrėta 2023 m. sausio 13 d., https://kam.lt/wp-content/uploads/2022/03/nacionaline-kibernetinio-saugumo-strategija.pdf
28. Lietuvos Respublikos Krašto apsaugos ministerija, „Lietuvos gynybos politikos baltoji knyga", Vilnius, 2017 https://kam.lt/wp-content/uploads/2022/03/Baltoji-knyga-2017.pdf (žiūrėta 2023 m. balandžio 26 d.)
29. Lietuvos Respublikos Krašto apsaugos ministerija, „Lietuvos karinė doktrina", Vilnius, 2016, 2.3 Saugumo ir gynybos užtikrinimas , https://www.kariuomene.lt/data/public/uploads/2021/03/lkd-2016_patalpinta-svetainese-6.pdf (žiūrėta 2023 m. balandžio 26 d.)
30. Lietuvos Respublikos Krašto apsaugos ministerija, „Nacionalinė kibernetinio saugumo strategija", 2017, https://kam.lt/wp-content/uploads/2022/03/nacionaline-kibernetinio-saugumo-strategija.pdf (žiūrėta 2023 m. gegužės 5 d.)
31. Lietuvos Respublikos Krašto apsaugos ministerija, Lietuvos Respublikos Karinė strategija, Vilnius 2016, https://kam.lt/wp-content/uploads/2022/03/karine-strategija-LT-2016.pdf (žiūrėta 2023 m. balandžio 26 d.)
32. Lietuvos Respublikos Seimas, *„Lietuvos Respublikos kibernetinio saugumo įstatymas",* Vilnius, 2014, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee (žiūrėta 2023 m. sausio 13 d.)
33. Lietuvos Respublikos Seimas, Dėl Lietuvos Respublikos Seimo 2002 m. gegužės 28 d. nutarimo Nr. IX-907 „Dėl Nacionalinio saugumo strategijos patvirtinimo" pakeitimo, Vilnius, 2017, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/4c80a722e2fa11e6be918a531b2126ab (žiūrėta 2023 m. balandžio 26 d.)
34. Lietuvos Respublikos Seimas, Dėl nacionalinio saugumo strategijos patvirtinimo, Vilnius, 2002, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.167925?jfwid=wqwn5jplo (žiūrėta 2023 m. balandžio 17 d.)
35. Lietuvos Respublikos Seimas, Dėl Nacionalinio saugumo strategijos patvirtinimo, Vilnius, 2021, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.167925/asr (žiūrėta 2023 m. gegužės 5 d.)
36. Lietuvos Respublikos Seimas, Dėl Seimo nutarimo "Dėl Nacionalinio saugumo strategijos patvirtinimo" priedo pakeitimo, Vilnius, 2005, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.249438 (žiūrėta 2023 m. balandžio 19 d.)

37. Lietuvos Respublikos Seimas, Kibernetinio saugumo įstatymas, Vilnius, 2014, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee#part_cb4294571a7c40b080dac0a832505c40 (žiūrėta 2023 m. balandžio 24 d.)
38. Lietuvos Respublikos Seimas, Lietuvos Respublikos nacionalinio saugumo pagrindų įstatymas, Vilnius, 1996, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.34169?jfwid=wqwn5jq6k (žiūrėta 2023 m. balandžio 17 d.)
39. Lietuvos Respublikos Seimas, Seimo NUTARIMO dėl Lietuvos Respublikos Seimo nutarimo "Dėl Nacionalinio saugumo strategijos patvirtinimo" pakeitimo PROJEKTAS + strategija, Vilnius, 2012, https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/TAIS.428241 (žiūrėta 2023 m. balandžio 24 d.)
40. Lietuvos Respublikos Vyriausybė, Dėl Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo", Vilnius, 2011, https://www.e-tar.lt/portal/lt/legalAct/TAR.1ABB945646B7 (žiūrėta 2023 m. balandžio 20 d.)
41. Lietuvos Respublikos Vyriausybė, Dėl Informacijos technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo, Vilnius, 2001, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.157225?jfwid=rivwzvpvg (žiūrėta 2023 m. balandžio 17 d.)
42. Lietuvos Respublikos Vyriausybė, Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo, Vilnius, 2018, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr (žiūrėta 2023 m. gegužės 5 d.)
43. Lietuvos Respublikos Vyriausybė, Nutarimas dėl Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepcijos patvirtinimo, Vilnius, 2006, https://www.e-tar.lt/acc/legalAct.html?documentId=TAR.522926ED3AA1 (žiūrėta 2023 m. balandžio 20 d.)

Ataskaitos

1. Lietuvos Respublikos Valstybės saugumo departamentas, „Grėsmių nacionaliniam saugumui vertinimas“, Vilnius, 2014, https://www.vsd.lt/wp-content/uploads/2016/10/gresmes-2013.pdf (žiūrėta 2023 m. balandžio 24 d.)
2. Lietuvos Respublikos Valstybės saugumo departamentas, „Grėsmių nacionaliniam saugumui vertinimas“, Vilnius, 2015, https://www.vsd.lt/wp-content/uploads/2016/10/Gresmiu-vertinimas-2014.pdf (žiūrėta 2023 m. balandžio 24 d.)

3. Lietuvos Respublikos Valstybės saugumo departamentas, „Grėsmių nacionaliniam saugumui vertinimas“, Vilnius, 2016, https://www.vsd.lt/wp-content/uploads/2017/03/bendras-2015-gresmiu-vertinimas.pdf (žiūrėta 2023 m. balandžio 26 d.)
4. Lietuvos Respublikos Valstybės saugumo departamentas, „Grėsmių nacionaliniam saugumui vertinimas“, Vilnius, 2017, https://www.vsd.lt/wp-content/uploads/2017/03/2016-gr%C4%97smi%C5%B3-vertinimas.pdf (žiūrėta 2023 m. balandžio 26 d.)
5. Lietuvos Respublikos Valstybės saugumo departamentas, „Grėsmių nacionaliniam saugumui vertinimas“, Vilnius, 2019 https://www.vsd.lt/wp-content/uploads/2019/02/2019-Gresmes-internetui-LT.pdf (žiūrėta 2023 m. gegužės 2 d.)
6. Lietuvos Respublikos Valstybės saugumo departamentas, „Grėsmių nacionaliniam saugumui vertinimas“, Vilnius, 2018 https://www.vsd.lt/wp-content/uploads/2018/03/LTU.pdf (žiūrėta 2023 m. gegužės 2 d.)
7. Lietuvos Respublikos Valstybės saugumo departamentas, „Grėsmių nacionaliniam saugumui vertinimas“, Vilnius, 2021 https://www.vsd.lt/wp-content/uploads/2021/03/2021-LT-el_.pdf (žiūrėta 2023 m. gegužės 2 d.)
8. Lietuvos Respublikos Valstybės saugumo departamentas, „Grėsmių nacionaliniam saugumui vertinimas“, Vilnius, 2022 https://www.vsd.lt/wp-content/uploads/2022/04/LT-el-_.pdf (žiūrėta 2023 m. gegužės 2 d.)
9. Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos, „Svarbiausia Lietuvos kibernetinio saugumo būklės statistika ir tendencijos, 2021 m. – 2022 m. I ketv., 2022, žiūrėta 2023 m. sausio 13 d., https://kam.lt/wp-content/uploads/2022/05/Kibernetinio-saugumo-santrauka-1.pdf,
10. Nacionalinis kibernetinio saugumo centras, „2017 Metų nacionalinio kibernetinio saugumo būklės ataskaita“, 2017, https://www.nksc.lt/doc/NKSC_ataskaita_2017_lt.pdf (žiūrėta 2023 m. balandžio 26 d.)
11. Nacionalinis kibernetinio saugumo centras, „2018 Metų nacionalinio kibernetinio saugumo būklės ataskaita“, 2018, p. 30, https://www.nksc.lt/doc/NKSC_ataskaita_2018.pdf (žiūrėta 2023 m. gegužės 2 d.)
12. Nacionalinis kibernetinio saugumo centras, „2019 Metų nacionalinio kibernetinio saugumo būklės ataskaita“, 2019, https://www.nksc.lt/doc/Nacionalinio_kibernetinio_saugumo_bukles_ataskaita_2019.pdf (žiūrėta 2023 m. gegužės 5 d.)
13. Nacionalinis kibernetinio saugumo centras, „2021 Metų nacionalinio kibernetinio saugumo būklės ataskaita“, 2021, p. 56 https://www.nksc.lt/doc/Nacionaline-kibernetinio-saugumo-ataskaita-2021.pdf (žiūrėta 2023 m. gegužės 5 d.)

14. Nacionalinis kibernetinio saugumo centras, „Svarbiausia Lietuvos kibernetinio saugumo būklės statistika ir tendencijos, 2021 m. – 2022 m. I ketv.“, 2021, https://www.nksc.lt/doc/Svarbiausia-Lietuvos-kibernetinio-saugumo-bukles-statistika-ir-tendencijos-2021-2022-I-ketv.pdf (žiūrėta 2023 m. gegužės 5 d.)

Kita

1. International Telecommunications Union, „Global Cybersecurity Index 2020”, žiūrėta 2023 m. gegužės 9 d., https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf
2. Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos, „Veikla“, žiūrėta 2023 m. sausio 12 d., https://www.nksc.lt/veikla.html
3. NATO, „Prague Summit Declaration“, Praha, 2002, pranešimas spaudai, https://www.nato.int/cps/en/natohq/official_texts_19552.htm (žiūrėta 2023 m. balandžio 17 d.)
4. NATO, „Study on NATO Enlargement“, 1995, https://www.nato.int/cps/en/natohq/official_texts_24733.htm, (žiūrėta 2023 m. balandžio 17 d.)
5. Oficialios statistikos portalas, Skaitmeninė ekonomika ir visuomenė Lietuvoje (2020 m. leidimas), žiūrėta 2023 m. sausio 12 d., https://osp.stat.gov.lt/skaitmenine-ekonomika-ir-visuomene-lietuvoje-2020/gyvenimas-internete
6. The NATO Cooperative Cyber Defence Centre of Excellence, žiūrėta 2023 m. sausio 12 d., https://ccdcoe.org/about-us/

Priedai

Priedas Nr. 1

Ekspertai			
Saugumizavimo aspektas	**Citata**	**Šaltinis**	**Data**
Sugrėsminimas / Siūloma priemonė (nepasiruošimas kibernetinėms atakoms, specialistų samdymas, saugumo sistemų auditai)	„Bendrai kalbant, mes vis dar gyvename viltimi ir tikėjimu, o ne darbais ir pasiruošimu, tą parodo praeitos savaites kibernetinės atakos prieš valstybės institucijas. Nepaisant to, kad kai kurie ekspertai sakė kad ataką atlaikėme, mes nieko neatlaikėme, mes neatlaikėm net vaikiškos atakos.“ „Nereikia tikėtis, kad kibernetinio saugumo sistemos gali būti padarytos pigiai ir kokybiškai, nupirktos iš kaimyno ar studento, (...) reikia rimtai į šiuos klausimus pasižiūrėti, samdyti specialistus, daryti auditus, ruoštis galimai atakai.“	https://www.lrt.lt/naujienos/mokslas-ir-it/11/1733755/ekspertas-apie-kibernetini-sauguma-lietuvoje-yra-du-tipai-imoniu-nulauztos-ir-tos-kurios-dar-bus-nulauztos	2022-07-05
Siūloma priemonė (kibernetinio saugumo specialistų rengimas)	„Kibernetinio saugumo sektoriaus darbo rinkoje jaučiamas didžiulis talentų trūkumas. Tačiau tuo pat metu sulaukiame pranešimų apie darbo vietų perkėlimą ir didėjančią nelygybę. Todėl pusei pasaulinės darbo jėgos, kuri reikalauja naujų darbo vietų su geresnėmis galimybėmis, reikės persikvalifikuoti. Tai gali skambėti kaip problema, kurią dažnai paliekama spręsti pasaulio vyriausybėms. Tačiau šiuo atveju laikas nėra sąjungininkas, o kibernetinio saugumo pramonei būtų naudinga rodyti iniciatyvą ir veikti aktyviai. Bet koks perkvalifikavimas, kvalifikacijos kėlimas ir švietimo pertvarka atneš patenkintą ir atsinaujinusią darbo jėgą, bendrai kuriant ir plečiant iniciatyvas, kurios didina žmonių perspektyvas.“	https://www.15min.lt/verslas/naujiena/mokslas-it/penki-svarbiausi-t-okmano-ispudziai-po-renginio-1290-1687206	2022-05-31
Siūloma priemonė (pasiruošimas kibernetinėms atakoms)	„Ateityje technologijos taps dar svarbesnės rizikos ir atsparumo srityje, nes automatizavimas, dirbtinis intelektas, daiktų internetas ir virtuali arba alternatyvi realybė padės imituoti galimų atakų ir oro reiškinių poveikį, ir taip leis geriau joms pasirengti, sustiprinti tinklų kontrolę ir pagerinti stebėjimą, nustatyti pažeidimus, greitai prisitaikyti ir atstatyti tiekimą.“	https://www.15min.lt/verslas/naujiena/energetika/ekspertai-energetikos-sektoriui-teks-iveikti-ne-tik-tiekimo-bet-ir-kibernetinio-saugumo-krize-664-1927278	2022-09-05
Siūloma priemonė (kibernetinio saugumo specialistų rengimas)	„Nebijokite samdyti jaunų profesionalų, kurie galėtų perimti patirtį iš jūsų IT specialistų, o drauge sumažinti darbo krūvį. Jeigu turite po keletą skirtingos specializacijos IT specialistų, pasirūpinkite, kad jie laiku gautų pagalbą. Kitaip rizikuojate prarasti labiausiai patyrusius IT profesionalus ir jų potencialą ugdant naujus darbuotojus.“	https://www.delfi.lt/login/progresas/kibernetinis-saugumas/dideja ntys-kibernetinio-saugumo-issukiai-vercia-it-specialistus-keisti-profesija.d?id=90785649	2022-07-21
-	„...kiek tai rimta? Tiesą pasakius, man prieš pat karo Ukrainoje pradžią apie save paskelbusios „Killnet“ veikla kol kas kiek panaši į rusų kariuomenę. Labai daug kalbų apie savo galybę ir galimybes, bet kai ateina laikas veikti, iš didelio debesies susidaro labai nedidelis lietus. Tik jei	https://www.15min.lt/naujiena/aktualu/nuomones/giedrius-meskauskas-	2022-06-28

	kariuomenė tikrai padarė daug nepataisomos žalos, tiesa, labai toli nuo pažadų per dvi dienas užimti Kyjivą, „Killnet“ ne tik nepadarė realios žalos, bet ir patys operatyviai gavo į kaulus, kai „Anonymous“ po grasinimų Lietuvai uždarė jų pačių interneto puslapį.“ „Šiuo metu virtuali erdvė kiek primena 90-uosius, kai buvo vagiama viskas, kas ne vietoje padėta, kiekvienas automobilio savininkas buvo patyręs bent po kelias automagnetolos vagystes, o kiekvienos parduotuvės savininkas samdydavo sargą, kuris budėdavo parduotuvei nedirbant. Dabar kiekviena įmonė turi pasirūpinti kibernetiniu saugumu, nes klausimas yra ne „ar“ tapsite nusikaltėlių taikinių, o „kada“ tapsite.“	killnet-kibernetine-ataka-kokia-kariuomene-tokie-ir-hakeriai-18-1742384	
Sugrėsminimas (nepasiruošimas kibernetinėms atakoms)	„Deja, matome tendenciją, kad po tokių įvykių, kaip „CityBee“ ar Užsienio reikalų ministerijos duomenų vagystės, daugėja besikreipiančių dėl įsilaužimų testavimo ar kitų kibernetinio saugumo paslaugų, tačiau iš visuomenės, žiniasklaidos akiračio dingus tokiems įvykiams, nurimsta ir organizacijos. Lietuvoje vis dar neskiriamas pakankamas dėmesys kibernetiniam saugumui. Saugumo spragų taisymas jau po įsilaužimų yra skaudžiausia pamoka. Spragas gali „užtaisyti“, tačiau žalos, kurią padarė įsilaužėliai, nebeatitaisyti.“	https://www.lrt.lt/naujienos/mokslas-ir-it/11/1521165/kibernetinio-saugumo-specialistas-daugelis-valstybiniu-instituciju-sedi-tarsi-ant-tiksinciosbombos	2021-10-05
Sugrėsminimas (Rusijos keliama grėsmė kibernetinėje erdvėje, pavojus kritinei infrastruktūrai)	„Jei kalbame apie Rusiją, manau, Lietuva yra jos taikinių dešimtuke, kaip ir kitos Baltijos šalys. Esame panašioje padėtyje kaip Ukraina, Gruzija, kai kurios Balkanų, „Sovietų lagerio“ šalys. Tai reikia suprasti ir kasdien apie tai galvoti. Vis dėlto esame nepatogi šalis, todėl turime didesnę riziką, kad vieną gražią dieną mus vienaip ar kitaip atakuos – ar programiškai, ar techniškai, galbūt bandys išjungti elektros tiekimą kaip tai įvyko Ukrainoje ar tiesiog bandys užblokuoti interneto ryšio kanalus kaip Estijoje. Pasiruošus tokioms ar panašioms atakoms galime be didesnių nuostolių jas atremti.“	https://www.15min.lt/verslas/naujiena/mokslas-it/saugumo-ekspertas-lietuva-rusijos-kibernetiniu-ataku-taikiniu-desimtuke-1290-1024966	2018-09-05
Siūloma priemonė (rezervinis internetas kritinės infrastruktūros veikimui užtikrinti)	„Lietuvai reikia nepriklausomo papildomo ryšio tiekėjo rezerviniam internetui“, – pirmadienį Seimo Ekonomikos komiteto Aukštųjų technologijų, inovacijų ir skaitmeninės ekonomikos pakomitetyje, kur aptarta kibernetinio saugumo situacija Lietuvoje vertinant įvykių Ukrainoje pamokas.“ <...>„Ukrainiečiai dabar pajunginėja nacionalinį banką, pavienius energetinius, ministerijų vienetus, kelis bankus, kurie arčiau valstybės, kad vartotojai turėtų galimybę, kad ir mažu srautu, bet prisijungti prie svetainės ir sužinoti informaciją, nes jos nepateikimas vartotojui, tai yra gyventojui sėja paniką.“	https://www.15min.lt/verslas/naujiena/mokslas-it/m-parescius-reikia-rezervinio-interneto-geresnes-kompiuteriu-apsaugos-1290-1650516	2022-03-27
Sugrėsminimas (nepasiruošimas aukšto lygio kibernetinėms atakoms)	„Jeigu prieš keletą metų vertinimo skalėje iš 10 balų rašydavau 7, šiandien galiu duoti 8. Mums vis dar labai trūksta vartotojų edukacijos. Mūsų žmonės labai nori padėti, nori kai kuriuos dalykus išsaugoti, nori patys apsiginti, bet jiems kol kas trūksta žinių. Žiūrint iš valstybės pusės, ji savo kritinę infrastruktūrą yra gana rimtai apsaugojusi, tačiau pažvelgus į rimtesnes atakas, manau, kad nei viena iš Baltijos valstybių nėra tam visiškai pasiruošusi.“	https://www.lrt.lt/naujienos/mokslas-ir-it/11/1697582/ekspertas-apie-rusijos-programisiu-paskelbta-kibernetini-kara-rimtesnems-atakoms-visiskai-	2022-05-19

		pasiruosusi-nera-ne-viena-baltijos-valstybe	
- (prieštaraujama technologijų iš Kinijos saugumizavimui)	„Akivaizdu, kad tokio lygio gamintojui, kaip „Huawei“, jeigu pas juos būtų kažkas tokio [šnipinėjančio – red.], būtų tolygu mirčiai. Įsivaizduokime: vienas iš didžiausių pasaulyje elektronikos gamintojų, turintis milijardinę apyvartą, padaro tokį dalyką. Jie gi sau, kaip įmonei, pasirašytų mirties nuosprendį.“	https://www.15min.lt/verslas/naujiena/mokslas-it/telia-technikos-vadovas-naujas-huawei-saugesnis-nei-senas-iphone-1290-929746	2018-02-22

Priedas Nr. 2

Kariuomenė			
Saugumizavimo aspektas	**Citata**	**Šaltinis**	**Data**
Sugrėsminimas (kibernetinis karas ir grėsmė kritinei infrastruktūrai)	„Per penkerius metus šios pratybos iš nacionalinių išaugo į tarptautines ir pakilo į naują kokybinį lygmenį. Ypatingai svarbu suderinti tarpusavio veiksmus ir procedūras sprendžiant kibernetinius incidentus ne tik Lietuvos kariuomenės valdomose sistemose, bet ir ypatingos svarbos infrastruktūros objektuose.“ „Didelio masto kibernetinės atakos gali sutrikdyti ne tik valstybinių įstaigų veiklą, bet ir ypatingos svarbos infrastruktūros įmonių veiklą, kas gali iššaukti masinius nepasitenkinimo protestus ir chaosą valstybėse. Tam, kad užkardyti priešiškų jėgų veiklą ir yra kuriami bei vystomi kibernetinio saugumo pajėgumai.“	https://www.kariuomene.lt/kas-mes-esame/naujienos/gynybos-stabas-organizavo-kibernetines-gynybos-pratybas/21402	2019-11-19
Priemonė (kibernetinio saugumo pratybos, tarptautinis bendradarbiavimas)	„...viena svarbiausių JAV ir Lietuvos bendradarbiavimo sričių yra kibernetinis saugumas ir kibernetinės gynybos pajėgumų vystymas.“	https://www.lrt.lt/naujienos/lietuvoje/2/1834193/rupsys-jav-pensilvanijos-gvardija-vienas-saugumo-garantu-baltijos-regione	2022-12-01

Priedas Nr. 3

Prezidentūra (Grybauskaitė, Nausėda)			
Saugumizavimo aspektas	**Citata**	**Šaltinis**	**Data**
Sugrėsminimas (Rusijos kišimasis į rinkimus)	„Šiais trejų rinkimų Lietuvoje metais tikėtinos agresyvesnės trečiųjų šalių, pirmiausiai – Rusijos kibernetinės atakos, siekiant paveikti rinkimų eigą ir rezultatus.“	https://www.15min.lt/naujiena/aktualu/lietuva/preizdentura-per-rinkimus-tiketinos-rusijos-kibernetines-atakos-56-1084732	2019-01-08
Sugrėsminimas (kibernetinis karas)	„...Todėl šiandien, kai žodis „karas“ – prekybos, informacinis, kibernetinis – girdimas dažniau nei „taika“, kai tęsiama agresija Ukrainoje, Europa turi išlikti vieninga.“	https://grybauskaite.lrp.lt/lt/spaudos-centras/pranesi	2018-07-13

		mai-spaudai/30487	
Sugrėsminimas (kibernetinis saugumas – demokratijos išlikimo sąvoka, aukštas kibernetinių atakų skaičius, pavojus kritinei infrastruktūrai)	„...saugi ir patikima kibernetinė erdvė – demokratijos išlikimo sąlyga. Sparčiai augant industrinei ir technologinei pažangai, kibernetinis saugumas tampa gyvybiškai svarbia nacionalinio saugumo dalimi.“ „Kibernetinės atakos tampa nauju karo ginklu. Europos Sąjungoje vien per dieną fiksuojama apie 4 tūkstančius, o Lietuvoje – apie 55 tūkstančius kibernetinių atakų per metus. Jos dažniausiai yra nukreiptos prieš valstybės gyvavimui svarbius sektorius – strateginius energetikos, transporto ir finansų tinklus. Siekiama paralyžiuoti valstybės institucijų darbą, pasitelkiant jas skelbti melagingas naujienas objektyvios žiniasklaidos portaluose. Daugelyje šalių pastebėti piktybiški išorės jėgų bandymai paveikti demokratinių rinkimų rezultatus.“	https://grybauskaite.lrp.lt/lt/spaudos-centras/pranesimai-spaudai/31744	2019-01-24
Siūloma priemonė (tarpvalstybinis bendradarbiavimas kibernetinio saugumo srityje)	„Nebijokime būti ir Europos Sąjungos integracijos smaigalyje, nes tik suvieniję pastangas karinio, energetinio, kibernetinio ir ekonominio saugumo srityse jausimės stiprūs. Atgimstanti stiprios ir vieningos Europos idėja grąžina pasitikėjimą savimi.“ „Lietuva jau prisideda prie Europos saugumo stiprinimo: mūsų iniciatyva kuriamos greitojo reagavimo pajėgos kibernetinėms grėsmėms atremti ir kovoti su priešiška propaganda, patvirtinti bendri standartai ES išorės sienos apsaugai.“	https://grybauskaite.lrp.lt/lt/spaudos-centras/pranesimai-spaudai/30197	2018-06-12
Priemonė (tarpvalstybinis bendradarbiavimas kibernetinio saugumo srityje)	„Mūsų idėjos dalyvauja kuriant ES kibernetinį saugumo skydą, unikalūs Lietuvos produktai, tokie kaip „Demaskuok“ projektas, padeda visai ES kovoti su dezinformacija ir priešiška propaganda.“	https://www.lrp.lt/lt/lietuvos-respublikos-prezidentes-dalios-grybauskaites-metinis-pranesimas/32606	2019-06-11
Sugrėsminimas (kibernetinis erdvės ginklavimosi varžybos)	„...Lietuvos požiūriu, rimčiausiomis kliūtimis turėtų būti laikomi taisyklėmis grįstos pasaulinės tvarkos pažeidimai, kibernetinės erdvės virsmas nauju ginklavimosi lauku, tarptautinių aplinkosaugos bei branduolinės saugos standartų nepaisymas, klimato kaitos ignoravimas.“	https://www.lrp.lt/lt/ziniasklaidos-centras/naujienos/prezidento-kalba-jtga-kurti-visuotine-gerove-mums-yra-auksciausias-priesakas/33141	2019-09-26
Sugrėsminimas (kibernetinis šnipinėjimas)	..“nutekėjusi informacija „gali padaryti didelės žalos pirmiausia sąjungininkų atžvilgiu“.	https://www.tv3.lt/naujiena/video/dienos-pjuvis-kibernetines-atakos-pries-lietuva-kokie-pavojai-ir-kaip-reaguoti-n1109634	2021-08-13
Sugrėsminimas / siūloma priemonė (kibernetiniai nusikaltimai,	„Bendras nusikalstamumo lygio mažėjimas, stebimas nuo 2017 metų, nuteikia pozityviai. Tačiau turime daugiau	https://m.kauno.diena.lt/naujienos/lietuva/politika/g-nauseda-susitinka-su-	2022-03-30

tarptautinis bendradarbiavimas)	dėmesio skirti korupcinių ir kibernetinių nusikaltimų tyrimams, plėtoti tarptautinį bendradarbiavimą.“ Šalies vadovas taip pat pabrėžė sparčiai augantį kibernetinių nusikaltimų skaičių, domėjosi tokių tyrimų efektyvumo problemų priežastimis. Susitikimo metu aptartas aktyvesnės prevencijos bei kibernetinio saugumo stiprinimo poreikis.	generaline-prokurore-aptars-nusikalstamumo-tendencijas-1070959	
Sugrėsminimas (kibernetinio saugumo inovacijų būtinumas)	„Bet svarbiausia yra tai, kad nesustotume, kad judėtume į priekį, kad keltumėme sau aukščiausius tikslus, nes šitoje srityje, jeigu sustoji, tuoj pralenks kiti.“	https://www.15min.lt/naujiena/aktualu/lietuva/nacionalinio-kibernetinio-saugumo-centre-kaune-apsilankes-prezidentas-ragino-nesustoti-56-1256878	2020-01-07

Priedas Nr. 4

VRM			
Saugumizavimo aspektas	**Citata**	**Šaltinis**	**Data**
Sugrėsminimas (nusikaltimai kibernetinėje erdvėje)	„Migracijos krizės, terorizmas, pasaulinė pandemija, hibridiniai ir kariniai išpuoliai mūsų kaimynystėje – tai skatina teisėsaugos institucijas daug aktyviau bendradarbiauti užtikrinant piliečių ir valstybės saugumą. Neabejotina, kad dėl pasikeitusios saugumo situacijos regione Europolo vaidmuo ateinančiais metais ir toliau augs, užtikrinant tarpvalstybinį bendradarbiavimą, nustatant bendras grėsmes ir teikiant operatyvią paramą. Tai itin aktualu kovojant su nusikalstamomis schemomis, kurios pradėjo keltis į elektroninę erdvę ir tampa vis sudėtingesnės.“	https://vrm.lrv.lt/lt/naujienos/susitikime-su-europolo-direktore-aptartos-nusikalstamumo-tendencijos	2022-11-24
-	„Daugiau investuoti į valstybei svarbių objektų apsaugai būtinas technines priemones ir darbuotojų atitikties reikalavimus bus skatinami ir jų valdytojai, nes pagal Nacionaliniam saugumui svarbių objektų įstatymą pareiga užtikrinti saugumą pirmiausia tenka objektų valdytojams.“ „Tiesioginių grėsmių valstybei svarbiems objektams nėra. Tačiau, įvertinus Ukrainos patirtis, negalime atmesti, kad Lietuvai priešiškos jėgos eskaluos valstybės strateginių objektų saugumo temą...“	https://vrm.lrv.lt/lt/naujienos/vst-ir-policija-stiprina-bendradarbiavima-del-strateginiu-objektu-apsaugos	2022-11-24
Sugrėsminimas / siūloma priemonė (kibernetinės atakos ir tarptautinė partnerysė)	„Kadangi skaitmeninė erdvė panaikina visas valstybių sienas, turime glaudžiai bendradarbiauti regioniniu lygmeniu, kad padidintume sąmoningumą ir užtikrintume neišvengiamos prekybos žmonėmis baudžiamosios atsakomybės principą, taip pat teiktume paramą aukoms.“	https://vrm.lrv.lt/lt/naujienos/vrm-prekyba-zmonemis-didziausi-pavojai-tyko-skaitmenineje-erdveje	2021-05-06

Sugrėsminimas / siūloma priemonė (nusikaltimai kibernetinėje erdvėje ir tarptautinė partnerysė)	„Memorandumo pasirašymas prisidės prie sklandesnio tarpinstitucinio bendradarbiavimo, leis įstaigoms operatyviau dalintis informacija siekiant suvaldyti galimas rizikas finansinių technologijų ir inovacijų srityje. Aktyvus ir savalaikis pasirašiusiųjų šalių keitimasis duomenimis padės efektyviau ir tarnyboms reaguoti siekiant užkirsti kelią nusikalstamoms veikoms šioje srityje.“	https://vrm.lrv.lt/lt/naujienos/vidaus-reikalu-ministras-pasirase-memorandumа-del-riziku-valdymu-fintech-srityje	2019-03-18

Priedas Nr. 5

KAM			
Saugumizavimo aspektas	**Citata**	**Šaltinis**	**Data**
Sugrėsminimas (Rusijos vykdomos kibernetinės atakos)	„Kibernetinės atakos yra vienas iš tų įrankių, kuriuos Rusija turi. Neatmesčiau, kad taip gali būti.“	https://www.15min.lt/verslas/naujiena/mokslas-it/lietuvos-gelezinkeliai-susiduria-su-kibernetinemis-atakomis-bendroviu-svetaines-gali-buti-laikinai-nepasiekiamos-1290-1733878	2022-06-23
Siūloma priemonė (nauja viceministro pareigybė)	„Jeigu būtų ketvirtas, mes jam numatę labai svarbią sritį, vėlgi, ne iš vienos institucijos ji susideda – tai yra kibernetinio saugumo viceministras. Tai yra svarbi valstybei sritis, krašto apsauga atsakinga už Nacionalinį kibernetinį saugumo centrą, atsakinga už kertinį visos valstybės ryšį, ir čia reikalingas žmogus, kuris kuruotų šitą sritį, ir aš ketvirtą matyčiau šitą sritį.“	https://www.15min.lt/naujiena/aktualu/lietuva/a-anusauskas-matytu-poreiki-uz-kibernetini-sauguma-atsakingam-viceministrui-56-1995714	2023-01-17
Sugrėsminimas (Rusijos vykdomos kibernetinės atakos)	...“Prasidėjus karui Ukrainoje priešiška kibernetinė veikla dar labiau išaugo. Tokiais laikais mūsų bendros pastangos mažinti didėjančias grėsmes yra labai svarbios...“	https://www.lrt.lt/naujienos/lietuvoje/2/1931984/belgija-slovenija-jungiasi-prie-lietuvos-vadovaujamu-es-kibernetiniu-pajegu	2023-03-08
Priemonė (tarptautinė partnerystė)	„Kibernetinės grėsmės nepaiso sienų, todėl bendradarbiavimas su Izraeliu ir apsikeitimas aktualia informacija bei žiniomis padės sustiprinti mūsų abiejų šalių kibernetinį saugumą.“	https://www.lrt.lt/naujienos/lietuvoje/2/1927501/lietuva-ir-izraelis-sutare-glaudziau-bendradarbiauti-kibernetinio-saugumo-srityje	2023-03-02
Sugrėsminimas (Rusijos vykdomos kibernetinės atakos)	„Kiberatakos vyko visą laiką, nesustojamai, jau, sakyčiau, ne vienus metus vyksta. Bet tokio masto, intensyvumo – jei ir nepasiekė aukščiausio intensyvumo, bet sakyčiau, vidutinio intensyvumo – tai taip, tai vyksta, ko gero, pirmą kartą.“	https://www.15min.lt/naujiena/aktualu/lietuva/a-anusauskas-kiberataku-organizatoriai-	2022-06-29

	„...atsakomybę už išpuolį prisiimanti grupuotė „Killnet“ yra siejama su Rusijos specialiosiomis. tarnybomis, o atakas galima laikyti Rusijos atsaku į taikomus Kaliningrado tranzito ribojimus“.	iesko-silpnu-vietu-galimi-ispuoliai-pries-versla-56-1742794	
Sugrėsminimas (Rusijos vykdomos kibernetinės atakos)	„Kibernetinių grėsmių tendencijos jau kuris laikas yra intensyvėjančios, jaučiame ne tik Rusijos, bet ir Kinijos „susidomėjimą“. Prasidėjus karui Ukrainoje, priešiška kibernetinė veikla dar labiau išaugo.“	https://www.lrt.lt/naujienos/pozicija/679/1855987/arvydas-anusauskas-2022-metais-sukureme-stipresne-modernesne-ir-geriau-organizuota-krasto-apsaugos-sistema	2022-12-31
Siūloma priemonė (kibernetinio saugumo specialistų atlyginimo didinimas)	„Iš privataus verslo mums pritraukti specialistus dėl atlyginimų apribojimų, kuriuos numato Krašto apsaugos įstatymas, yra sudėtinga, tačiau mes numatę po poros mėnesių Seimui pateikti įstatymo pakeitimus, kad tiems specialistams, kurie susiję su šitomis sritimis, mes galėtume mokėti rinkos sąlygų atlyginimus.“	https://m.diena.lt/naujienos/lietuva/salies-pulsas/kam-ketina-moketi-didesnes-algas-kibernetinio-saugumo-specialistams-1063288	2022-02-09
Sugrėsminimas (išaugęs atakų skaičius ir jų sudėtingumas) **Siūloma priemonė** (didesnis kibernetinio saugumo finansavimas)	„atakų ne tik daugėja bet jos tampa ir sudėtingesnės.“ „Lietuva turėtų daugiau investuoti į kibernetinį saugumą, nes „krašto apsauga negali visų valstybės institucijų aprūpintu tuo, ko reikia.“	https://www.15min.lt/verslas/naujiena/mokslas-it/pries-kam-svetaine-geguze-ivykdyta-masyvi-kibernetine-ataka-1290-1681544	2022-05-18
Sugrėsminimas (nepatikimos technologijos iš Kinijos)	„Iš esmės taip. Ji nukreipia į elektroninę parduotuvę, kur yra tikimybė kartu su parsisiunčiamų duomenų programėle gauti priedą viruso pavidalu. Virusas, vėlgi, nelygu koks. Gali siųsti vartotojo asmeninius duomenis, o ne tuos, kurie susiję su telefono funkcionalumu.“	https://www.lrt.lt/naujienos/mokslas-ir-it/11/1501190/anusauskas-apie-pavojus-del-kinijoje-pagamintu-telefonu-tukstanciai-nupirkta-valstybes-institucijoms-del-to-kad-pigiau-kainuoja	2021-09-21
Sugrėsminimas (kibernetinės atakos prieš kritinę infrastruktūrą)	„Jeigu pandemija ir su tuo susijęs vis dar aukštas kibernetinių incidentų skaičius privertė mus daugiau dėmesio skirti šalies kibernetinio saugumo brandos stiprinimui ir mokymams, tai dėl karo Ukrainoje išaugus kibernetinio saugumo rizikoms, teko imtis skubių papildomų priemonių stiprinant mūsų valstybės ir kritinės infrastruktūros apsaugą.“	https://www.lrytas.lt/it/ismanyk/2022/05/17/news/pristatomi-svarbiausi-lietuvos-kibernetinio-saugumo-	2022-05-17

		skaiciai-ir-tendencijos-23381002	
Sugrėsminimas (priklausomybė nuo kritinės infrastruktūros)	„Pastaraisiais metais daugėja įmonių, kurių veikla ir paslaugų teikimas yra tiesiogiai priklausomas nuo patikimai veikiančios informacinės infrastruktūros. Praplėstas ypatingos svarbos informacinės infrastruktūros ir jos valdytojų sąrašas apima svarbiausias mūsų valstybei įstaigas, kurios nuo šiol privalės skirti ypatingą dėmesį jų valdomų ryšių ir informacinių sistemų kibernetiniam saugumui, taip pat užtikrinti jų atitiktį organizaciniams ir techniniams kibernetinio saugumo reikalavimams“ <...> „tai, kad išplečiamas ypatingos svarbos sektorių sąrašas, leis padidinti dėmesį šių sričių kibernetiniam saugumui, o kartu tai užtikrins ir visos Lietuvos kritinės infrastruktūros saugumą.“	https://lrv.lt/lt/naujienos/vyriausybei-ispletus-ypatingos-svarbos-informacines-infrastrukturos-sarasa-daugiau-imoniu-privales-skirti-ypatinga-demesi-savo-kibernetinio-saugumo-uztikrinimui	2021-03-08
Sugrėsminimas (kibernetinės atakos prieš kritinę infrastruktūrą, žiniasklaidą, auganti kibernetinių atakų rizika)	„Gyvename skaitmeninės visuomenės amžiuje, kuris suteikia mums didelių galimybių ir daro mūsų gyvenimą patogesnį, tačiau su privalumais ateina ir kibernetinių atakų rizikos.“ „Šiandien kibernetinių atakų taikiniu pasirenkama ne tik kritinė infrastruktūra, bet ir žiniasklaida. „Tokios atakos prieš visuomenės informavimo priemones tampa vis labiau koordinuotos, kompleksiškos ir rafinuotos.“	https://www.lrt.lt/naujienos/lietuvoje/2/720113/krasto-apsaugos-viceministras-silpniausia-kibernetinio-saugumo-grandis-yra-zmones	2019-03-08
Sugrėsminimas / siūloma priemonė (nepatikimos technologijos iš Kinijos)	„Tiktokas neturėtų būti tarnybiniuose įrenginiuose.“	https://www.15min.lt/ikrauk/video/1515-ar-lietuvos-valstybines-institucijos-turetu-draustinaudoti-tiktok-235716	2023-03-01

Priedas Nr. 6

KST			
Saugumizavimo aspektas	**Citata**	**Šaltinis**	**Data**
Sugrėsminimas (kibernetinės atakos)	„2022-ieji geriausiai galėtų būti įvardijami kaip iššūkių metai. Visų pirma, dėl šių metų vasarį Rusijos pradėto karo prieš Ukrainą. Žymiausias šio karo atspindys Lietuvoje, žvelgiant iš kibernetinio saugumo perspektyvos, buvo birželio mėnesį nuvilnijusi DDoS tipo atakų banga ir sustiprintas NKSC dėmesys kibernetinio saugumo reikalavimų užtikrinimui.“	https://kam.lt/kibernetinio-saugumo-taryboje-aptarti-svarbiausi-metu-ivykiai-ir-busimi-pokyciai/	2022-09-29
Sugrėsminimas (kibernetinės atakos)	„Lietuvoje 2021 metais buvo užfiksuota 1890 kibernetinio saugumo incidentų, įvykdytų pasitelkiant kenkimo programinę įrangą, bei 1187 duomenų viliojimo (angl. phishing) atvejai.“	https://kam.lt/nauju-teises-aktu-es-bus-siekiama-didinti-technines-ir-programines-irangos-kibernetini-sauguma/	2023-01-04
Priemonė (ES direktyva, skirta stiprinti	„Į naujosios direktyvos apimtį patenka ne tik anksčiau identifikuoti svarbūs sektoriai, tokie kaip energetika, transportas, sveikatos apsauga, bet ir sritys, apimančios	https://kam.lt/isigalioja-es-direktyva-kuria-	2023-01-16

kibernetinį atsparumą)	pašto ir kurjerių paslaugas, atliekų tvarkymo, viešojo administravimo įmones ir kitas.“	bus-siekiama-didinti-atsparuma-kibernetinems-gresmems/	

Priedas Nr. 7

NSGK			
Saugumizavimo aspektas	**Citata**	**Šaltinis**	**Data**
Siūloma priemonė (kibernetinio raštingumo kėlimas) **Sugrėsminimas / siūloma priemonė** (nepatikimos technologijos iš Kinijos)	“…Didesni duomenų kaupėjai turėtų užsiimti darbuotojo kibernetinio saugumo raštingumu – turime labai daug ekspertų, kurie mokymu pavidalu gali kelti raštingumą. Tuo turėtų užsiimti kiekviena įmonė – laikas išeiti iš sovietinio mąstymo, kad tik valstybė baudomis ir reguliavimu nustatinės tam tikras taisykles.“ „Lietuva per kelerius metus turi tapti nepriklausoma nuo nepatikimų technologijų tiekėjų. Mes girdime balsus iš JAV, kurie aiškiai sako, kad 5G ryšys turi būti be Kinijos kompanijų...“	https://www.delfi.lt/verslo-poziuris/diskusijos/kasciunas-kibernetinio-saugumo-kartele-reikia-kelti-ne-baudomis-o-sveika-verslo-konkurencija-86874991	2021-04-07
Sugrėsminimas / siūloma priemonė (nepatikimos technologijos iš Kinijos)	„...Viena iš idėjų, kurią būtų galima įgyvendinti stipriais Vyriausybės sprendimais, tai yra labai konkrečiai įvardinti konkrečius gamintojus, nedemokratinių valstybių konkrečius gamintojus, kurių informacijos ir ryšių technologijų įranga kelia potencialią grėsmę mūsų šalies saugumui ir neturi būti naudojama Lietuvoje diegiant penktos kartos vadinamąjį 5 G judrųjį ryšį.“	https://www.diena.lt/naujienos/lietuva/politika/l-kasciunas-gresmiu-saugumui-pristatymas-savotiskas-priesnuodis-1014647	2021-03-04
Sugrėsminimas (Kinija) **Siūloma priemonė** (kibernetinio raštingumo kėlimas)	„Dabar formuojasi dvi technosferos. Sakyčiau, kad šalia geopolitikos, yra ir technosferų pasidalinimas – Vakarų, kurioje lyderiauja amerikiečiai, ir Kinijos kontroliuojama technosfera. Ir mums reikės apsispręsti, kokioje mes technosferoje norime būti. Nes tai nėra tik galios varžytuvės. Kaip ir minėjau, tai yra asmens duomenys, mūsų visų privatus gyvenimas. Svarbu, kad jis būtų apsaugotas. Mes savo gyvenimą keliame į technolygį, tad to kibernetinio saugumo reikia vis daugiau ir daugiau. O čia yra Kinijos rizika.“ Jeigu žmogus yra kibernetiškai neraštingas ir daro tokius dalykus, mes turėsime ir toliau problemų ir tu nuo neapsisaugosi. Dėl to čia reikia kelti raštingumo klausimą, turi būti mokymai, vidinės vadybos klausimas, kaip įmonė valdoma.	https://www.tv3.lt/naujiena/lietuva/kasciunas-apie-pandemijos-apnuogintas-spragas-rusijos-zingsni-i-prieki-ir-kodel-nepirktu-huawei-telefono-n1090368	2021-04-11
Sugrėsminimas (nepatikimos technologijos iš Kinijos)	„Realiai niekas nežino: jeigu kamera išjungta, ar jinai tikrai išjungta, ar ji tuo metu tikrai nefilmuoja, ar jos negalima nuotoliniu būdu įjungti. Be abejonės, tai kelia nerimą saugumui ir kitoms aplinkybėms.”	https://www.15min.lt/naujiena/aktualu/lietuva/nsgk-vadovas-nesaugios-kameros-turi-buti-ismontuotos-jei-spragu-pasalinti-neimanoma-56-1324280	2020-05-27
Sugrėsminimas (nepatikimos	„Jeigu lietuviškuose lokomotyvuose įdėta rusiška sistema, rusai gali žinoti, kur važiuojama, maršrutus. Jeigu į Lietuvą	https://www.lrytas.lt/lietuvosdie	2023-02-21

technologijos iš Rusijos)	atvyktų NATO sąjungininkai, būtų naudojami geležinkeliai, apie kurių veiksmus rusai žinotų viską. „Grėsmės akivaizdžios, bet dabar krašto apsaugos ministrui tai visiškai nesvarbu. Dar 2017 metais buvo priimtas sprendimas nedelsiant viską išmontuoti, numatytos lėšos, kiek tai kainuos, ir kad tai būtų sutvarkyta čia ir dabar.“	na/aktualijos/2023/02/21/news/atskleidus-apie-valstybines-imones-pirkimo-is-rusijos-plana-sujudimas-seimo-nariai-imasi-veiksmu-26200127	
Sugrėsminimas / siūloma priemonė (nepatikimos technologijos iš Kinijos)	„Ir jeigu tu esi ypač sprendimų priėmėjas, politikas, valstybės tarnautojas, pareigūnas, karys ir mėgsti „Tik Tok“, kai kurie, žinau, iš Seimo narių tą daro, tu gali turėti po to rimtų bėdų. Na, turiu omenyje, čia jau yra šantažo galimybė.“ „Tik Tokas yra rimta tema, aš tikrai girdžiu, girdžiu visus argumentus, ateinančius iš vakarų. Vakar Krašto apsaugos ministerija pasiūlė, na, tokią rekomendaciją nenaudoti „Tik Tok“. Aš manau, reikia eiti dar galbūt žingsniu į priekį dėl tarnybinių telefonų. Ir žiūrėti, kaip klostosi.“	https://www.lrt.lt/naujienos/lietuvoje/2/1926029/nsgk-pirmininkas-siulo-neleisti-pareigunams-naudotis-tik-tok-asmenine-informacija-gali-buti-panaudota-santazui	2023-03-01
Sugrėsminimas (nepatikimos technologijos iš Rusijos)	„Buvusios „Oro navigacijos“ vadovybės ilgalaikiai artimi ryšiai su minėtos [rusiškos] įrangos gamintojų atstovais ir įrangos įdiegimo aplinkybės vertintini kaip galimai turėję poveikį priimant sprendimus strategiškai svarbiame nacionaliniam saugumui sektoriuje ir galimai kėlė grėsmę valstybės interesams.“	https://www.15min.lt/verslas/naujiena/finansai/lietuvos-oro-erdve-stebi-rusiski-radarai-ir-sistemos-nsgk-nurodo-jas-keisti-kainuos-15-milijonu-662-979342	2018-05-30
Sugrėsminimas / siūloma priemonė (nepatikimos technologijos iš Kinijos)	„Rudenį turėsime rimtų pataisų, kur bus aiškiai suformuluoti kriterijai tiekėjams. Aiškiai galėsime atskirti, kas yra patikimas, o kas yra nepatikimas. Tai tikriausiai bus sąsajos su to gamintojo kilmės šalimi ir jos autoritarine, ne demokratine politine sistema, kas vyksta ir Vakaruose“ „Taip per kelis metus, tikiuosi, pasieksime proveržį šioje srityje. Jeigu būtų mano valia, kreipčiausi šiandien į muitinę ir sakyčiau – ištraukite visas tas sistemas kuo greičiau. Bet aš suprantu, kad tai kainuoja. Kad tai yra kaštai, kad valstybė turi suplanuoti lėšas, ir tas truputėlį užtruks.“	https://www.lrt.lt/naujienos/lrt-tyrimai/5/1367222/uzdrausti-kiniski-rentgenai-idarbinti-lietuvos-muitineje-gamintojai-ruosia-ieskiniteismui	2021-03-18
Siūloma priemonė (nauja ginkluotųjų pajėgų rūšis)	„Sutarėme, kad nuo 2024 metų turi būti įkurtos kibernetinės pajėgos, kaip atskira Lietuvos ginkluotųjų pajėgų rūšis.“	https://www.lrt.lt/naujienos/lietuvoje/2/1674746/partiju-susitarime-nauja-kariuomenes-rusis-pasirengimas-priimti-divizija	2022-04-15
Sugrėsminimas / siūloma priemonė (nepatikimos technologijos)	“Komiteto nariai domėjosi priemonėmis, kurios leistų apriboti nepatikimų 5G technologijos tiekėjų įrangos ir paslaugų naudojimą ypatingai nacionaliniam saugumui svarbiuose objektuose ir valstybės institucijose.“	https://www.lrs.lt/sip/portal.show?p_r=36014&p_k=1&p_t=271506	2020-06-10

Sugrėsminimas (nepatikimos technologijos)	"Seimo Nacionalinio saugumo ir gynybos komitetas birželio 3 d. posėdyje priėmė sprendimą kreiptis į NSKC prašydamas įvertinti, ar Seimo kanceliarijoje naudojamos komitetų posėdžių transliacijai vaizdo stebėjimo kameros yra saugios. NKSC taip pat prašoma pateikti rekomendacijas, kuriomis būtų sustiprintas kibernetinis Seimo kanceliarijos naudojamos vaizdo stebėjimo įrangos saugumas."	https://www.lrs.lt/sip/portal.show?p_r=36014&p_k=1&p_t=271401	2020-06-03
Sugrėsminimas (Rusija)	„Hibridinis karas vykdomas ir kibernetikos srityje. Lietuva patenka į padidintos rizikos valstybių grupę ir kibernetinėje erdvėje yra vienas didžiausių Rusijos taikinių. Vien 2018-aisiais susidūrėme su 53 tūkst. kibernetinių incidentų, o dauguma jų buvo iš Rusijos. Akivaizdu, kad kibernetiniai išpuoliai prieš NATO valstybes tapo sudėtine Rusijos agresijos dalimi."	https://www.lrs.lt/sip/portal.show?p_r=36014&p_k=1&p_t=265425	2019-03-22
Sugrėsminimas (pavojus kritinei infrastruktūrai)	„Energetikos sektorius Lietuvoje susidurs su vis didėjančia kibernetinio saugumo rizika, todėl būtina šiai sričiai skirti ypatingą dėmesį. Šioje srityje turime būti itin stiprūs, kad galėtume apsisaugoti nuo galimų provokacijų. Šiais laikais kibernetinė grėsmė – išties reali, tad turime daryti namų darbus."	https://www.lrs.lt/sip/portal.show?p_r=36014&p_k=1&p_t=256561	2018-03-28
Sugrėsminimas (nepatikimos technologijos)	„Turime atsakingai reaguoti į šią situaciją, nes kibernetinis ir informacinis saugumas yra jautri ir itin aktuali tema. Vertinimas gali turėti įtakos ateityje planuojamiems įsigijimams."	https://www.lrs.lt/sip/portal.show?p_r=36014&p_k=1&p_t=255710	2018-03-08
Sugrėsminimas / siūloma priemonė (hibridinės (kibernetinės) grėsmės, valstybės parengties gintis didinimas)	„Turime suvokti, kad gintis nuo hibridinių grėsmių būtina nedelsiant, nelaukiant fizinio puolimo. Hibridinis karas yra kompleksinis reiškinys, todėl jo prevencija ir gynyba taip pat turi būti kompleksinė. Į hibridinių grėsmių specifiką turi būti atsižvelgta ir tobulinant nacionalinę krizių ir ekstremalių situacijų valdymo sistemą, kuri atitiks šiuolaikinius iššūkius, bus nukreipta į valstybės atsparumo stiprinimą ir nuolatinės parengties užtikrinimą."	https://www.lrs.lt/sip/portal.show?p_r=38447&p_k=1&p_t=275488	2021-03-24
Sugrėsminimas (nepatikimos technologijos)	„Su šiomis įstatymo pataisomis Lietuva žengia į saugesnės technologinės pažangos laikotarpį, kai pagaliau galėsime elektroninių ryšių rinkoje turėti tik patikimus ir saugią įrangą siūlančius tiekėjus bei gamintojus. Pritardamas įstatymo pataisoms, Seimas demonstruoja tvirtą ryžtą plėtoti Lietuvos europinę ir transatlantinę integraciją nacionaliniam saugumui strategiškai svarbiame informacinių technologijų ir telekomunikacijų ūkio sektoriuje."	https://www.lrs.lt/sip/portal.show?p_r=35403&p_k=1&p_t=276622	2021-05-25
Sugrėsminimas (nepatikimos technologijos iš Kinijos, auganti Kinijos galia technologijų srityje)	"…augantis Kinijos veiksnys, siekiant ekonominio technologinio dominavimo, artėjantys sprendimai dėl 5G ryšio diegimo..."	https://www.lrs.lt/sip/portal.show?p_r=38447&p_k=1&p_t=273457	2020-11-25
Sugrėsminimas (nepatikimos technologijos iš Kinijos)	„O rizikos susijusios su tuo, kad yra įvairių autoritarinių valstybių, kurios stipriai eina į priekį technologine prasme ir, pavyzdžiui, Kinijos įstatymai numato, kad net ir privačios bendrovės, esant poreikiui Vyriausybės, turėtų jai pateikti surinktus duomenis apie net ir užsienio šalių gyventojus"	https://www.tv3.lt/naujiena/lietuva/kelia-skinasi-kiniskos-irangos-draudimas-apsaugotu-nuo-nesaugaus-5g-rysio-n1092524	2021-04-22