Vilniaus universitetas

TARPTAUTINIŲ SANTYKIŲ IR POLITIKOS MOKSLŲ INSTITUTAS

Politikos mokslų bakalauro programa

EDVINAS JUSIS

IV kurso studentas

JUDRIOJO PENKTOSIOS KARTOS (5G) RYŠIO SAUGUMIZAVIMAS JAV

BAKALAURO DARBAS

Darbo vadovas: prof. dr. Gediminas Vitkus

Vilnius, 2020

BAKALAURO DARBO PRIEŠLAPIS

Bakalauro/magistro darbo vadovo/ės išvados dėl darbo gynimo:

.....
.....
.....

..... **.....** **.....**

(data) (v., pavardė) (parašas)

Bakalauro darbas įteiktas gynimo komisijai:

..... **.....**

(data) (Gynimo komisijos sekretoriaus/ės parašas)

Bakalauro darbo recenzentas/ė:

.....

(v., pavardė)

Bakalauro darbų gynimo komisijos įvertinimas:

.....

Komisijos pirmininkas/ė:

Komisijos nariai:

PATVIRTINIMAS APIE ATLIKTO DARBO SAVARANKIŠKUMĄ

Patvirtinu, kad įteikiamas darbas (Judriojo penktosios kartos ryšio (5G) saugumizavimas JAV) yra:

1. Atliktas mano pačio 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.

Edvinas Jusis

Vardas, pavardė (parašas)

BIBLIOGRAFINIO APRAŠO LAPAS

Jusis E. ***Judriojo penktosios kartos (5G) ryšio saugumizavimas JAV:*** Politikos mokslų specialybės, bakalauro darbas / VU Tarptautinių santykių ir politikos mokslų institutas; darbo vadovas G. Vitkus – V., 2020. – 62 p.

Reikšminiai žodžiai: JAV, Judrusis penktosios kartos ryšys, 5G, Kinija, Huawei, Kopenhagos mokykla, sugrėsminimas,

Šiame darbe yra tiriamas judriojo penktosios kartos (5G) ryšio saugumizavimo procesas Jungtinėse Amerikos Valstijose 2019-2020 metų kovo mėnesio laikotarpiu. Atsižvelgiant į saugumizacijos teorinius aspektus, kokybinės turinio analizės metodu darbe yra pateikiama penkių JAV pareigūnų kalbos aktų 5G ryšio sugrėsminimo analizė viešoje erdvėje. Taip pat, darbe yra analizuojami trys oficialūs dokumentai/teisės aktai, siekiant išsiaiškinti 5G problematikos saugumizavimą oficialiajame/techniniame lygmenyje.

Turinys

Įvadas

Informacinės ir ryšių technologijos neabejotinai užimą svarbią vietą šiuolaikinėje visuomenėje ir ekonomikoje. Globaliu mastu, telekomunikacinės paslaugos sugeneravo beveik 1,3 trilijonus eurų 2019 m.,[1] o žmonių, kurie gyvena mobiliojo plačiajuosčio ryšio nebuvimo vietovėse, skaičius pasaulyje kasmet mažėja ir siekia apie 750 mln.[2] Spartus pastarojo dešimtmečio informacijos ir komunikacijų technologijų vystymasis veda pasaulį link naujo, penktosios kartos mobilios komunikacijos judriojo ryšio, bendrai žinomo kaip 5G.

5G ryšys bus svarbus ne tik dėl to, jog suteiks kaip niekad greitą mobilių duomenų perdavimą tarp individų. Naujos kartos ryšys bus pasitelktas įrenginių tarpusavio komunikavimui ir prisidės prie naujų technologijų, tokių kaip Dirbtinio Intelekto (angl. *Artificial Intelligence)* sistemų, duomenų talpyklų „debesies“ (angl. *cloud*), Daiktų Interneto (angl. *Internet of Things*) platesnio pritaikymo kasdienybėje. Modernizuotos viešosios paslaugos, telemedicina ir operacijos per atstumą, tikslusis ūkininkavimas, savaeigiai automobiliai keliuose, skaitmenizuotos gamyklos ir kitos naujovės bus naudojamos netolimoje ateityje. Prognozuojama, jog 2020 m. globaliu mastu sugeneruotos pajamos iš 5G ryšio tinklų infrastruktūros sieks 4,2 mlrd. JAV dolerių, o 2021 m. – 6,8 mlrd. JAV dolerių.[3] Apibendrinant, didele sparta ir maža delsa pasižymėsiantis 5G ryšys taps daugelio valstybių kritinių sektorių[4] ir verslo integrali dalis.

Svarbu atkreipti dėmesį, jog būsimą naujosios kartos ryšį reikia vertinti kaip valstybės kritinės infrastruktūros dalį. Nors 5G sukurs stimulą verslo produktyvumui, inovacijoms bei atneš finansinę ir ekonominę naudą, tačiau tuo pat metu atitinkamai lems didesnę ekonominės veiklos priklausomybę nuo šio ryšio. Informacijos tėkmės bei duomenų saugumas ir patikimumas, vagystės bei įsilaužimai bus daug svarbesni nei buvusioje ryšio kartoje. Nėra sudėtinga suprasti, kokį poveikį ir riziką sukeltų iš išorės sutrikdytas ryšys savaeigiam automobiliui eisme, nuotoliniu būdu operaciją atliekančiam chirurgui ar industrinėms kontrolės sistemoms, disponuojančioms jautria, pramonės saugumą užtikrinančia informacija. Atsižvelgiant į tai, 5G ryšys, kaip būsima integrali kritinės infrastruktūros dalis, kelia su

[1] Statista, „Global revenue from telecommunications services from 2005 to 2019“, 2020. <https://www.statista.com/statistics/268628/worldwide-revenue-from-telecommunications-services-since-2005/> [Žiūrėta 2020 03 25]

[2] GSMA, „Mobile Internet Connectivity Global Factsheet“, 2019. <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/07/Mobile-Internet-Connectivity-Global-Factsheet.pdf > [Žiūrėta 2020 03 25]

[3] Gartner, „Wireless Infrastructure Revenue Forecast, Worldwide, 2018-2021“, 2019. < https://www.gartner.com/en/newsroom/press-releases/2019-08-22-gartner-forecasts-worldwide-5g-network-infrastructure > [Žiūrėta 2020 03 35]

[4] Pvz., transportas, bankininkystė, energetika.

kibernetika susijusias rizikas valstybių nacionaliniam bei ekonominiam saugumui.[5] Dėl šios priežasties, būsimų 5G ryšio tinklų saugumas, konfidencialumas ir nenutrūkstamumas įgauna svarbią reikšmę ir aktualumą.

Europos Sąjungos 5G koordinuoto kibernetinio saugumo rizikos vertinime[6] pabrėžiama, jog 5G tinklų kibernetinės grėsmės[7] kyla dėl (1) 5G technologinės charakteristikos (architektūros) ir (2) 5G infrastruktūros tiekėjų bei jų rolės tiekimo grandinėje (angl. *supply chain*). Pirmuoju atveju, kibernetinių išpuolių rizika išaugs dėl padidėsiančių bendro galimo atakos paviršiaus ir „įėjimo taškų“: dėl mažiau centralizuotos technologinės architektūros (lyginant su 4G), tinklo branduolio funkcijos bus integruotos į periferines funcijas, todėl kai kurios infrastruktūros įrangos dalys, kaip bazinės stotelės ar antenos, taps „jautriomis“ dėl potencialiai galimo įsilaužimo į jas ir prieigos prie branduolio.[8] Be to, padidėjusi programinės įrangos reikšmė 5G tinklo įrenginiuose kels riziką dėl galimų konfigūracijos klaidų ar specialaus noro pakenkti vystant ir atnaujinant programų sistemas. Antruoju atveju, sąsajoje su išaugsiančia infrastruktūros priklausomybe nuo 5G ryšio, mobilaus ryšio operatoriai taps labiau priklausomi nuo įrangos tiekėjų, nes dėl padidėjusio įsilaužimo paviršiaus kitos valstybės arba jų remiami veikėjai gali išnaudoti įrenginius kaip prieigą prie bendro tinklo, todėl tiekėjo profilis ir reputacija įgauną svarbią reikšmę.[9] Taip pat, grėsmės rizika kiltų dėl didelio priklausomumo nuo vieno 5G ryšio infrastruktūros tiekėjo, pvz., verslo žlugimo ar įmonės pažeidžiamumo atveju. Aptariamuoju metu, didžiausių 5G įrangos pardavėjų grupę globaliu mastu sudaro 5 įmonės, kurioje pirmauja kiniškas Huawei, švediškas Ericsson ir suomiška Nokia. 2017 m. bendrai šios įmonės sudarė beveik 80% visos rinkos.[10]

Visgi, 5G ryšio kibernetinis saugumas nėra tik techninis iššūkis. Nors telekomunikacijų operatoriai gali pasitikėti tiekėjais, dėl 5G svarbos kritinei infrastruktūrai ir ekonomikai, valstybės – nebūtinai. Šis nepasitikėjimas atspindi 5G įrangos tiekimo grandinės politizaciją ir bendrai – 5G ryšio saugumizavimą. Kaip pastebėjo Jan-Peter Kleinhans, pastaruoju metu 5G ryšio saugumo diskusijoje

[5] Mathieu Duchâtel ir François Godement, „Europe and 5G: the Huawei Case”, Institute Montaigne, 2019, 4. < https://www.institutmontaigne.org/en/publications/europe-and-5g-huawei-case-part-2 > [Žiūrėta 2020-03-25]
[6] NIS Cooperation Group, „EU coordinated risk assessment of the cybersecurity of 5G networks”, 2019. < https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132 > [Žiūrėta 2020-03-25]
[7] Detalesnes kibernetines grėsmes ir jų tipus žr. ENISA, „Threat Landscape For 5G Networks”, 2019, 64. < https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks/at_download/fullReport > [Žiūrėta 2020-03-25]
[8] NIS Cooperation Group, 31.
[9] Ten pat, 32.
[10] Xuewu Gu, Christiane Heidbrink, Ying Huang, Philip Nock, Hendrik W. Ohnesorge, Andrej Pustovitovskij, „Geopolitics and the Global Race for 5G“, CGS Global Focus, 2019. < http://cgs-bonn.de/5G-Study-2019.pdf > [Žiūrėta 2020-03-25]

dominuoja klausimas: Ar kiniškų 5G gamintojų įranga kelia grėsmę nacionaliniam saugumui?[11] Egzistuoja pozicija, jog Kinijos teisinė ir politinė sistema turi neigiamos įtakos jos telekomunikacinės įrangos įmonėms, nes, pasinaudojant kiniška 5G infrastruktūra, Kinija galėtų šnipinėti kitose valstybėse. Būtent šis aspektas suteikia aktualumo 5G ryšio ir jo saugumo diskusijoje.

5G ir Huawei diskusija iliustruoja, jog valstybių pozicijos 5G grėsmės supratime išsiskiria. Nors ir nėra viešų oficialių faktų apie Huawei įmonės ir jos sąsajas su Kinijos vyriausybės šnipinėjimu svetur, Jungtinės Amerikos Valstijos (JAV) yra uždraudusios Huawei dalyvauti 5G infrastruktūros diegime.[12] Jungtinė Karalystė Huawei suteikė ribotą rolę 5G diegime: įmonei bus leista diegti infrastruktūros ne-branduolio įrangą, bet tik iki 35% visos rinkos.[13] Europos Sąjunga, pasirinkusi koordinuotą kelią diegti ir apsaugoti 5G tinklus, tiesiogiai neįvardijo uždraudžianti Huawei, tačiau pabrėžė reikiamybę taikyti apribojimus „didelės rizikos“ tiekėjams, kuriuos apspręs pačios valstybės narės.[14] Nors pačios 5G infrastruktūros diegimas vyks ateityje, ES narių pozicija Huawei klausimu yra fragmentuota. Pvz., Portugalija, Ispanija ir Italija draudimų nesvarsto, o daugelyje šalių, įskaitant ir Lietuvą, diskusija dėl draudimų ir ribojimų vyksta vyriausybiniu lygmeniu.[15]

Atsižvelgiant į valstybių pozicijų fragmentaciją šiuo klausimu, galima teigti, jog JAV esamoji administracija, santykyje su kitomis valstybėmis, pasižymi polinkiu išskirtinai sugrėsminti 5G ryšį. Iš to natūraliai kyla klausimas, kaip ir kodėl tai yra daroma? Visgi, dėl technologijos naujumo, 5G ryšys nėra nuodugniai tirtas aspektas saugumo studijų disciplinoje. Dėl šios priežasties, šiuo darbu yra norima išanalizuoti 5G ryšio saugumizacijos procesą JAV, laikantis prielaidos, jog ši valstybė yra *linkusi* saugumizuoti naujosios kartos ryšį.

Literatūros apžvalga:

5G ryšio saugumizacija yra ganėtinai nauja tema saugumo studijose. Tai lemia, jog šia tema akademinėje literatūroje tyrimų nėra daug. Visgi, atsižvelgiant į 5G tiesiogines sąsajas su kitomis temomis, esamą literatūrą galima suskirstyti į kelias grupes: 5G kaip technologinis aspektas JAV-Kinijos

[11] Jan-Peter Kleinhas, „5G vs. National Security – A European Perspective“, 2019. < https://www.stiftung-nv.de/sites/default/files/5g_vs._national_security.pdf > [Žiūrėta 2020-03-25]
[12] Nigel Inkster, „The Huawei Affair and China‘s Technology Ambitions.“ *Survival, Global Politics and Strategy*, 61, 2019. < https://www.tandfonline.com/doi/full/10.1080/00396338.2019.1568041?scroll=top&needAccess=true > [Žiūrėta 2020-03-05]
[13] Leo Kelion, „Huawei set for limited role in UK 5G networks*“*, January 28, 2020, < https://www.bbc.com/news/technology-51283059 > [Žiūrėta 2020 03 25]
[14] Europos Komisija, „Secure 5G networks: Quesions and Answers on the EU toolbox.“ 29 January, 2020 < https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_127 > [Žiūrėta 2020 03 25]
[15]Xeuwu Gu *et al.*, 46.

santykių kontekste, geopolitikoje bei kibernetinės erdvės saugumizavime. Nors akademinėje literatūroje nėra studijų, tiriančių valstybių 5G ryšio saugumizavimo procesą, tačiau joje yra pateikiama reikšmingų įžvalgų, implikuojančių į priežastis, kodėl JAV 5G problematika yra sugrėsminama.

Akademinėje literatūroje galima rasti studijų, kuriose yra tiriamas Kinijos grėsmės diskursas. Andrew S. Campion kritinės diskurso analizės metodu tyrė Kinijos grėsmės diskursą JAV.[16] Išanalizavęs JAV politinis elito kalbos aktus, autorius daro išvada, jog 2005 m. reakcijos į Kinijos nacionalinės ofšorinės naftos korporaciją (CNOOC) atspindi požiūrį į Huawei. Kinijos grėsmės ir kritinės infrastruktūros saugumo diskursas prisideda prie sėkmingo Kinijos saugumizavimo bendrame JAV diskurse.

Technologinis aspektas literatūroje yra tyrinėtas JAV-Kinijos santykių kontekste. S. Mori savo straipsnyje analizuoja JAV ir Kinijos konkurenciją karinėje, industrinėje ir skaitmeninių tinklų erdvėse.[17] Autoriaus nuomone, šis varžymasis yra kova dėl viršenybės esamos ir būsimos technologinės kartos minėtose srityse, kurios galėtų daryti įtaką šių valstybių vidaus politikai, socio-ekonominei sistemai bei visai tarptautinių santykių sistemai. N. Inkster teigimu, JAV ir Kinijos strateginė konkurencija formuos XXI a. geopolitiką, o aukštųjų technologijų sektorius yra ir bus pagrindinė „kovos“ erdvė.[18] Anot autoriaus, Kinija dirbtinio intelekto ir telekomunikacijų erdvę mato kaip raktinę sritį savo ekonominiam vystymuisi ir galiausiai – vienu iš būdų siekti hegemonijos, o JAV atitinkamai imasi atsakomųjų priemonių tam balansuoti. J. Shirfinson, kritikuodamas tradicinę realizmo galios balanso teoriją teigia, jog tiesioginė šių valstybių konfrontacija yra mažai tikėtina, tačiau vienu iš pasiūlytų scenarijumi, Kinija imasi laipsniško reliatyvios galios didinimo strategijos ekonomikos ir technologijų srityse, o JAV – atitinkamų atsakomųjų veiksmų.[19] 5G atvejis, priskirtinas aukštųjų technologijų sektoriui, gerai iliustruoja šių autorių tezes dėl dviejų didžiųjų valstybių konkurencijos.

Atsižvelgiant į JAV ir Kinijos konkurenciją, literatūroje yra ieškoma atsakymų į tai, kaip geopolitinės jėgos formuoja 5G vystymą, nes naujasis ryšys reprezentuoja dviejų supervalstybių galios varžybas, [20] kurios turi poveikį įrangos pardavėjams, operatoriams ir trečiosioms šalims, o 5G ryšio

[16] Andrew S. Campion, „From CNOOC to Huawei: securitization, the China threat, and critical infrastructure.“ *Asian Journal of Political Science,* 28(1), 2020. < https://www.tandfonline.com/doi/full/10.1080/02185377.2020.1741416 > [Žiūrėta 2020-03-28]

[17] Satoru Mori „US Technological Competition with China: The Military, Industrial and Digital Network Dimensions.” *Asia-Pacific Review,* 26(1), 2019. < https://www.tandfonline.com/doi/full/10.1080/13439006.2019.1622871 > [Žiūrėta 2020-03-28]

[18] Inkster, ten pat.

[19] Joshua Shifrinson, „The rise of China, balance of power theory and US national security: Reasons for optimism?” *Journal of Strategic Studies,* 43(2), 2020. < https://www.tandfonline.com/doi/full/10.1080/01402390.2018.1558056?journalCode=fjss20 > [Žiūrėta 2020-03-28]

[20] Stacie Hoffmann, Samantha Bradshaw, Emily Taylor, „Networks and Geopolitics: How great power rivalries infected 5G”, Oxford Information Labs, 2019. < https://oxil.uk/publications/geopolitics-of-5g/Geopolitics_5G_Final.pdf >; Xeuwu

diegimo lenktynės yra matomos kaip „mūšis dėl kalno viršūnės“.[21] Viena vertus, varžybos vyksta dėl tarptautinių 5G sistemų valdymo standartų įtvirtinimo, nes standartai nulems ne tik kaip bus įrengti 5G tinklai, bet taip pat standartizuoti finansiniai santykiai tarp veikėjų 5G ekosistemoje.[22] Tarptautinės standartų tvirtinimo organizacijos, kaip 3GPP (3rd Generation Partnership Project) ir ITU (International Telecommunications Union), veikia kaip pagrindinė politinė arena 5G standartų kovoje. Dabartinė standartizacijos būsena yra valstybių ir įmonių varžymasis dėl galios šiose organizacijose.[23] Kita vertus, yra varžomasi dėl intelektualinės nuosavybės teisių, konkrečiai – patentų, nes tai sukuria pagrindą 5G standartų įtvirtinimui, kadangi patys standartai yra grindžiami patentuotomis technologijomis.[24] Yra pastebimas patentų skaičiaus balanso geografinis pokytis: patentų teisių savininkai iš JAV, Japonijos ir Europos kiekiu nusileidžia kompanijoms iš Kinijos, Korėjos ir Taivano.[25] Be varžymosi dėl standartų ir patentų, 5G vystymas gali turėti reikšmingą poveikį ateities atviram internetui, jo valdymo normoms ir taisyklėms. Atsižvelgiant į JAV dominavimą esminėse interneto sistemose, Kinija siekia pakreipti balansą į savo pusę sukuriant integruotą 5G monopolį.[26]

5G ryšio saugumo rizikos yra tiesiogiai susijusios su kibernetine erdve, kuri literatūroje yra tyrinėta tema remiantis saugumizacijos teorija. Šios temos tyrimuose koncentruojamasi į kibernetinės erdvės saugumizavimo raidą, požymius ir valstybių lyginimus. Daug dėmesio yra skirta 2007 m. kibernetinių išpuolių prieš Estiją atvejui ir saugumizavimo raidai JAV. L. Hansen ir H. Nissenbaum identifikavo tris atskiras kibernetinės erdvės saugumizavimo formas (hypersaugumizacija, kasdieninės saugumo praktikos ir technifikacija) bei šį teorinį modelį pritaikė tiriant kibernetinius išpuolius prieš Estiją 2007 m.[27] Taip pat, remiantis šiuo modeliu, yra tiriamos ir lyginamos skirtingų valstybių kibernetinio saugumo strategijos ir su juo susijęs diskursas.[28] O. Hjalmarsson savo studijoje aiškinosi, kaip JAV Barako Obamos administracija kalbos aktais siekė saugumizuoti kibernetinę erdvę bei su ja

---

Gu *et al.*, 46; Eurasia Group, „The Geopolitics of 5G“, November 2018. < https://www.eurasiagroup.net/siteFiles/Media/files/1811-14%205G%20special%20report%20public.pdf > [Žiūrėta 2020-03-28]

[21] Paez, Danny, „Why the US must beat China in the race to 5G internet”, Inverse, August 21, 2018, “ < https://www.inverse.com/article/48228-why-china-is-winning-the-race-with-the-us-to-5g-internet> [Žiūrėta 2020-03-28]

[22] Eurasia Group, 8.

[23] Edison Lee, „Telecom Services. The Geopolitics of 5G and IoT *”,* Jefferies Franchise Note, September 2017, 39-41. < https://www.jefferies.com/CMSFiles/Jefferies.com/files/Insights/TelecomServ.pdf > [Žiūrėta 2020-03-28]

[24] Xuewei Gu *et al.*, 20.

[25] Ten pat, 20.

[26] Hoffman, 5.

[27]Lene Hansen ir Helen Nissenbaum, „ Digital Disaster, Cyber Security, and the Copenhagen School.“ *International Studies Quarterly*, 53, 2009, 17. < https://academic.oup.com/isq/article-abstract/53/4/1155/1815351 > [Žiūrėta 2020-03-28]

[28] Klingova, Katerina. "Securitization of Cyber Space in the United States of America, the Russian Federation and Estonia." Supervised by Paul Roe, Central European University Department of Political Science (2013).

susijusius referentinius objektus.[29] K. J. Scharz, išanalizavęs JAV prezidento B. Clinton administracijos laikotarpį, argumentuoja, jog kibernetinės erdvės saugumizaciją lemia technifikacijos procesas ir technokratų diskursas dėl kibernetinės erdvės techninės specifikos, kurią geriausiai supranta šioje srityje dirbantys ekspertai.[30]

Tyrimui yra pasirinktas JAV atvejis dėl kelių priežasčių. Visų pirma, ši valstybė yra viena pirmaujančių 5G diegime - 2020 m. sausį naujos kartos ryšį komerciniais tikslais įdiegusi 50-yje didžiuosiuose miestuose, o atsižvelgiant į ekspertines prognozes, 2025 m. pusę visų jungčių JAV bus naujojo ryšio pagrindu.[31] Antra, viešojoje erdvėje JAV yra linkusi politizuoti 5G ryšio diegimą, technologijos tiekimo grandines ir kibernetines grėsmes, pabrėždama Kinijos ir Huawei veiksnį. Galiausiai, JAV pasirinkta dėl jos, kaip didžiosios galios pozicijos tarptautinėje sistemoje.

Darbo objektas. JAV 5G ryšio diegimo saugumizavimo procesas.

Tyrimo problema. Nors nėra abejojama 5G ryšio būsima ekonomine nauda, tačiau valstybių pozicijos ryšio saugumo klausimais yra išsiskiriančios. Yra pastebima, jog JAV išsiskiria iš kitų valstybių polinkiu sugrėsminti 5G ryšio diegimą, tačiau nėra aišku, kaip ir kodėl 5G diegimo problemos tapo JAV saugumo darbotvarkės dalimi.

Tyrimo tikslas. Išanalizuoti 5G ryšio diegimo saugumizavimo proceso priežastis ir eigą JAV 2019-2020 metais.

Darbo metodai. Pagrindinis naudojamas metodas – diskurso analizė. Šis metodas yra pasitelktas siekiant ištirti JAV 5G ryšio problemų saugumizavimo procesą. Darbe tiriamas politinis 5G saugumo diskursas, formuojamas pagrindinių šia tema kalbėjusių išskirtų penkių aukšto politinio rango JAV pareigūnų – Prezidento, Viceprezidento, Valstybės sekretoriaus, Gynybos sekretoriaus ir Valstybės departamento kibernetinių ir tarptautinių komunikacijų bei informatikos politikos sekretoriaus padėjėjo pavaduotojo. Diskursui tirti pasitelkiama kokybinės turinio analizės metodinė prieiga, naudojama analizuojant pranešimus spaudai, politikų pareiškimus ir pasisakymus žiniasklaidoje nuo 2019 m. iki 2020 m. kovo mėn. laikotarpiu.

---

[29] Ola Hjalmarsson, „The Securitization of Cyberspace: How the Web Was Won.“ Lund University, 2013, 1. < http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=3357990&fileOId=3357996 > [Žiūrėta 2020-03-29].
[30] Kevin J. Schwarz, „The Securitization of Cyberspace through Technification.” Virginia Polytechnic Institute and State University: 2016. < https://vtechworks.lib.vt.edu/bitstream/handle/10919/71758/Schwarz_KJ_T_2016.pdf?sequence=1&isAllowed=y > [Žiūrėta 2020-03-29]
[31] GSMA Intelligence, “Forecast 5G Penetration in 2025”, < https://fingfx.thomsonreuters.com/gfx/mkt/12/8296/8227/GSMA%20Intelligence%205G%20Penetration.png > [Žiūrėta 2020-03-29]

Taip pat, darbe bus išanalizuoti 3 oficialūs su 5G saugumu susiję dokumentai/teisės aktai, siekiant išsiaiškinti kaip oficialiame/techniniame lygmenyje yra saugumizuojamos 5G problemos. Tai – 2020 m. JAV Nacionalinė Strategija 5G Apsaugoti; 2019 m. JAV prezidento dekretas, skirtas apsaugoti informacinių ir komunikacinių technologijų bei paslaugų tiekimo grandinę; 2020 m. kovą įsigaliojęs 2019 m. Saugių ir Patikimų Komunikacijų Tinklų Aktas.

Keliami tyrimo uždaviniai:

1) Išsiaiškinti, kaip pagal saugumizavimo teoriją sukonstruojamos grėsmės ir kaip vyksta sugrėsminimo procesas.
2) Išanalizuoti JAV saugumizuojančių veikėjų kalbas, pranešimus spaudai ar kitus viešus pareiškimus, žyminčius 5G problemų sugrėsminimą JAV viešajame diskurse.
3) Analizuojant JAV dokumentus atskleisti 5G sugrėsminimą oficialiajame diskurse.
4) Identifikuoti netipines priemones, iliustruojančias JAV 5G saugumizaciją ir kiniškos 5G technologijos ribojimą oficialiuosiuose dokumentuose.

Darbo struktūra: Darbą sudaro keturios dalys. Pirmojoje dalyje glaustai pristatoma saugumo studijų raida, klasikinės Kopenhagos mokyklos pristatytos saugumizacijos teorinės prielaidos ir vėlesni teorijos papildymai. Antroji dalis yra skirta išskirtų valstybės pareigūnų viešųjų pasisakymų analizei, kurioje atskleidžiama, ką atstovai kalba apie 5G problematiką, keliamas grėsmes ir priemones joms spręsti. Trečiojoje dalyje nagrinėjami trys su 5G saugumu susiję dokumentai, kuriuose bus ieškomos 5G saugumizavimo apraiškos oficialiajame diskurse. Galiausiai, ketvirtojoje dalyje bus pateiktos išvados.

1. Saugumizavimo teorija

Saugumas yra esminis konceptas saugumo studijose, kuris iš esmės yra susijęs su grėsmėmis išlikimui.[32] Nors yra sutinkama, jog pats saugumas yra siejamas su laisve nuo grėsmių, tačiau nėra bendro, vieningo ir objektyvaus saugumo apibrėžimo. Ši problema kyla viena vertus dėl to, jog saugumo konceptą galima formuluoti atsižvelgiant į ideologinius ar moralinius aspektus, todėl empiriniai įrodymai nėra pajėgūs apspręsti universalios sąvokos.[33] Kita vertus, nėra sutinkama dėl centrinio saugumo objekto, t.y., ką reikia saugoti – individą, valstybę, ar tarptautinę sistemą? Žvelgiant retrospektyviai,

[32] Alan Collins, *Contemporary Security Studies*, 4 leid., Oxford University Press: 2007, 2.
[33] Karin M. Fierke, *Critical Approaches to International Security*. 2 leid., John Wiley & Sons: 2015, 35.

saugumo koncepto ir pačios saugumo studijų disciplinos raidą paskatino Šaltojo Karo metu kilusi diskusija dėl saugumo koncepto nevientisumo.

Iki XX. a. 8 dešimtmečio, saugumo studijas dominavo tradicinė realistinė perspektyva, kurioje saugumas suprantamas iš valstybės, kaip centrinės veikėjos, pozicijos santykyje su kitomis šalimis bei išorinių grėsmių atsparumu. Tradicinis saugumas – realistinis, nes jo samprata grindžiama anarchistiniu galios balansu ir materialių karinių pajėgumų santykiu tarp suverenių valstybių. Šie požymiai pasireiškė valstybių dėmesio skyrimu geopolitikai, atgrasymui, galios balansavimui ir karinei strategijai. Istoriškai, šis požiūris sutapo su Antrojo pasaulinio karo pabaigos ir Šaltojo Karo pradžios laikotarpiu, kuomet dviejų supervalstybių – JAV ir Sovietų Sąjungos – konkurencijos kontekste, karinės galios pranašumas buvo laikomas išeitimi siekiant užsitikrinti nacionalinį saugumą.[34]

Šeštajame dešimtmetyje įvykęs biheivioralistinis pokytis socialiniuose moksluose lėmė, jog realizmo teorinių prielaidų dominavimui saugumo studijose buvo mestas iššūkis.[35] Šis pokytis sutampa ne tik su vėliau konstruktyvizmo teorijų įsigalėjimu tarptautinių santykių disciplinoje, bet ir su pokyčiu saugumo koncepto ir grėsmių sampratoje. Tai pasireiškė tuo, jog laikui bėgant akademinėje diskusijoje buvo keliami iki tol didžiąja dalimi realizmo atstovų ignoruoti ontologiniai saugumo klausimai: *Kas yra saugoma? Kas vykdo šį saugojimą? Kaip pasireiškia saugojimas? Kiek reikia saugumo?*[36] Atsižvelgiant į tradicinio saugumo apsiribojimą karinėmis grėsmėmis, kilo poreikis išplėtoti saugumo konceptą.

Dėl šios priežasties, Šaltojo Karo pabaigoje, išryškėjo disputas tarp saugumo „siaurintojų“ (angl. *narrowers*) ir „platintojų“ (angl. *wideners*).[37] „Siaurintojų“ grupei priskiriami mąstytojai, kurie, atsižvelgiant į taikią Šaltojo Karo baigtį ir sumažėjusią tiesioginės karinės konfrontacijos riziką, yra linkę išlaikyti tradicinį saugumo supratimą. Šiuo požiūriu, karinės galios balansas išlieka valstybės saugumo garantu, o pačio saugumo koncepto išplėtimas kelia riziką karinio saugumo ir tarpvalstybinių konfliktų prioretizavimo antraeiliškumui. Be to, kiekvienas prieš valstybę nukreiptas veiksnys turėtų būti traktuojamas kaip grėsmė saugumui, todėl plečiamas saugumo konceptas bei saugumo studijos prarastų darnumą, apimtų viską ir tuo pačiu nieką.

---

[34] Leo S. F. Lin, „State-centric Security and its Limitations: The case of transnational organized crime.“ Research Institute for European and American Studies, 2011, 13. < https://rieas.gr/images/rieas156.pdf > [Žiūrėta 2020-04-02]

[35] Gediminas Vitkus, „Realistinė tarptautinių santykių teorija ir Barry Buzano nedalomo saugumo koncepcija.“ Kn. Barry Buzan, Žmonės valstybės ir baimė. Vilnius: EUGRIMAS, 1997, 11.

[36] Peter Hough, „Who’s Securing Whom? The Need for International Relations to Embrace Human Security.” *St Antony's International Review*, 1(2), 2005, 72. < www.jstor.org/stable/26227012 > ; David A. Baldwin „The concept of security.“ *Review of International Studies* 23(1), 1997, 12-17. < http://www.princeton.edu/~dbaldwin/selected%20articles/Baldwin%20%281997%29%20The%20Concept%20of%20Security.pdf > [Žiūrėta 2020-04-02]

[37] Hough, 72-73.

Kad ir kaip būtų, karinės grėsmės nėra *vienintelės*, su kuriomis susiduria valstybės. SSRS žlugimas ir globalios tarptautinės sistemos konfigūracijos pokytis lėmė naujų saugumo iššūkių, grėsmių ir rizikų iškylimą. Remiantis tuo, oponuojančių akademikų grupė argumentavo, jog valstybės turėtų išplėsti savo saugumo darbotvarkes įtraukiant naujas grėsmes, kylančias iš, pvz., aplinkosaugos, ekonomikos ar teroristinių išpuolių. Dėl šios priežasties, saugumo apibrėžimas neturėtų apsiriboti vien valstybės saugumu, bet ir apimti individų ar tautų saugumą. Apibendrinant, „siaurintojų" ir „platintojų" diskusijoje buvo ieškoma išeities, kaip išplėsti ir pagilinti saugumo konceptą, neišdarkant jo loginės darnos; kaip išplėsti saugumo tyrimų lauką, įtraukiant nekarinius sektorius ir tuo pačiu išsaugant koncepto reikšmingumą?[38]

Atsižvelgiant į šio darbo temą – 5G ryšio saugumizavimą JAV, yra svarbu išsiaiškinti, kaip yra sukonstruojamos grėsmės ir kaip jos tampa valstybių nacionalinio saugumo dalimi. Atitinkamai, toliau bus aptariamas šio darbo teorinis pagrindas – Kopenhagos mokyklos išvystyta saugumizavimo/sugrėsminimo (angl. *securitization*) teorija. Šiai mokykla priskirtini mokslininkai B. Buzan ir O. Weaver svariai prisidėjo prie šiuolaikinių saugumo studijų literatūros, pasiūlę originalią tyrimų perspektyvą plačiam saugumo iššūkių spektrui. Kopenhagos mokyklos modelis suteikia galimybę tirti, kaip konkretus klausimas tampa (de)saugumizuotas, be to, tai žymi naują pokytį saugumo sampratoje ir tarsi siūlo išeitį saugumo koncepto siaurinimo ar platinimo dispute.[39] Tai pasireiškia galimybe į saugumo studijų tyrimus įtraukti ne tik tradiciškai suprantamas karines grėsmes ir nevalstybinius veikėjus, bet tuo pat metu išplėsti saugumo koncepto pritaikymą neprarandant jo darnos.[40]

1.1 Kopenhagos mokyklos saugumizacijos teorija

Kopenhagos mokyklos konceptualus saugumo studijų modelis buvo aiškiausiai išplėtotas bendroje B. Buzan, O. Waeverio ir J. de Wilde knygoje „Security: A New Framework for Analysis".[41] Šis darbas yra reikšmingas tuo, jog jame buvo sujungtos išsiskiriančios saugumo perspektyvos: B. Buzan priskiriama neorealizmo teorinė prieiga ir O. Waever konstruktyvistinis saugumizacijos aiškinimas. Taip pat, akademiniame dispute apie naujai kylančias saugumo problemas ir jų vertinimą, šiame darbe yra

[38] Bernard I. Finel, „New thinking about security: Analytical pitfalls and applications to the Americas." Vašingtonas, 1999. < https://www.oas.org/csh/docs/Foro%20sobre%20seguridad.pdf > [Žiūrėta 2020-04-03]
[39] Ten pat, 74.
[40] Ralf Emmers, „Securitization", Kn. Alan Collins, *Contemporary Security Studies*. Oxford University Press, 2013, 142.
[41] Barry Buzan, Ole Waever, and Jaap de Wilde, Security: A New Framework for Analysis, Boulder: Lynne Rienner Publishers, 1998.

siekiama pateikiamas aiškinimas, kaip saugumo problemos yra atskiriamos ir prioritetizuojamos.[42] Kopenhagos mokyklos pasiūlytas alternatyvus saugumo tyrimų modelis buvo sukurtas remiantis trimis pagrindiniais konceptais: B. Buzan suformuluotomis regionų saugumo kompleksų, saugumo sektorių idėjomis bei O. Waever pristatyta saugumizacija.[43]

Pirmasis konceptas - regionų saugumo kompleksas - B. Buzan buvo pristatytas 1983 m. Argumentuojant, jog geografiškai greta esančių valstybių saugumo tarpusavio priklausomybė lemia regioninių klasterių (saugumo kompleksų) susidarymą, šis konceptas suteikia galimybę tirti ne tik kompleksą sudarančių valstybių santykių dinamiką, bet ir išorinių galingų valstybių įsitraukimą bei to poveikį regionui.[44] Į šiuos kompleksus galima žvelgti kaip į nedideles sistemas, kurias galima tirti pritaikant tarptautinių santykių disciplinos teorijas, kaip antai galios balansą ar poliškumą.[45] Antrasis konceptas, taip pat išplėtotas B. Buzan, yra sektorinis grėsmių skirstymas, kilęs iš mokslininko siekio dekonstruoti nacionalinio saugumo sampratą ir išplėsti ją anapus karinių grėsmių, atsižvelgiant, į kurias valstybės sritis yra nukreiptos grėsmės.[46] Kopenhagos mokyklos teorijoje sektorinis grėsmių skirstymas yra papildomai išplėtojamas ir klasifikuojamas pagal specifinių santykių sąveiką: karinis saugumo sektorius – primestos prievartos santykius; politinis sektorius - valdžios, valdymo statuso ir pavaldumo santykius; ekonomikos sektorius – prekybos, produkcijos ir finansų santykius; societalinis sektorius – kolektyvinio identiteto; aplinkosaugos sektorius – žmogaus veiklos ir planetos biosferos santykius.[47] Taigi, Kopenhagos mokykloje taikomas sektorinis grėsmių skirstymas žymi poslinkį nuo tradicinių saugumo studijų vyravusios koncentracijos vien į karinį saugumą, kuris tampa vienu iš penkių sektorių. Atitinkamai, Kopenhagos mokykla nuo tradicinio saugumo perspektyvos atsispiria į tyrimų modelį įtraukdama ir nevalstybinius veikėjus.

Galiausiai, trečiasis ir labiausiai Kopenhagos mokyklą išgarsinęs konceptas - saugumizacija. Šis konceptas pirmiausia buvo suformuluotas O. Weaver[48], o vėliau, labiau sistemiškai išdirbtas bendrame Kopenhagos mokyklos darbe. Saugumizacijos teorijos atspirties taškas yra tai, jog saugumas *per se* yra

---

[42] Dovilė Jakniūnaitė, „Kritinės saugumo studijos XXI amžiuje: kur kreipti Lietuvos saugumo politikos tyrimus?." *Lietuvos metinė strateginė apžvalga*, 12, 2014, 35. <https://www.academia.edu/8238241/Kritinės_saugumo_studijos_XXI_amžiuje_kur_kreipti_Lietuvos_saugumo_politikos_tyrimus > [Žiūrėta 2020-04-04]

[43] Holger Stritzel, *Security in Translation: Securitization Theory and the Localization of Threat*, Basingstoke: Palgrave Macmillan, 2017, 14.

[44] Buzan, *Security: A New Framework for Analysis*, 11-15.

[45] Barry Buzan, Ole Weaver, *Regions and powers: the structure of international security*. Cambridge University Press, 2003, 49.

[46] People, states, and fear: The national security problem in international relations, 75.

[47] Buzan, *Security: A New Framework for Analysis*, 7.

[48] Ole Weaver, „Securitization and Desecuritization", kn. Ronnie D. Lipschutz (sud.) *On Security*, New York: Columbia University Press, 1995.

suprantamas kaip kalbos aktas.[49] Kalbos aktas yra prilyginamas veiksmo atlikimui ir tokiu būdu, objektas, apie kurį yra kalbama, įgauną papildomą reikšmę. To pavyzdys galėtų būti pažado davimas. Kai vienas žmogus duoda pažadą kitam, jis ne tik paprastai įsipareigoja kažką atlikti ar padaryti ateityje. Pažadas savaime tampa konkretaus veiksmo tipu. Remiantis šia logika, saugumo grėsmės yra suformuojamos per lingvistines praktikas, nes intersubjektyvaus proceso metu veikėjai problemas transformuoja į realias grėsmes.[50] Perfrazuojant O. Weaver, valstybės atstovas, kalbėdamas „saugumą“, tam tikrą saugumo problemą perkelia į specifinę erdvę, tokiu būdu įgaudamas teisę pasitelkti netradicines priemones ją suvaldyti.[51] Taigi, saugumizacija yra suprantama kaip procesas, kurio metu, konkreti problema, naudojant kalbos aktą, tampa saugumo problema.

Atsižvelgiant į tai, kas buvo pasakyta, kyla klausimas, kaip yra nusprendžiama, kas yra, o kas nėra saugumo problema? Jeigu yra manoma, jog saugumo darbotvarkę reikia išplėsti, atsiranda reikiamybė turėti kriterijų ar principą, pagal kurį problema būtų atsijojama nuo kitų ir priskirta prie saugumo grėsmių. Priešingu atveju, remiantis saugumizacijos logika, saugumo problemomis gali būti konstruojama bet kas, o bendra saugumo samprata taptų tokia konceptualiai plačia, jog būtų bevertė. Kopenhagos mokykla pabrėžia, jog saugumas iš esmės yra susijęs su išlikimu.[52] Šiuo požiūriu, saugumo problema yra tokia, kuri yra pristatoma kaip kelianti egzistencinę grėsmę referentinio objekto[53] išlikimui. Tai gerai iliustruoja valstybių požiūris į nacionalinį saugumą ir gynybą: užpuolimas bei karas kelia egzistencinę grėsmę valstybės išlikimui, todėl visuotinai priimtina, jog būtina turėti aukštos parengties kariuomenę, žvalgybos struktūras ir kt. Atitinkamai, egzistencinės grėsmės kontekste, valstybė įgauną legitimumą panaudoti netipines priemones (angl. *extraordinary measures*), reikalingas su šia grėsme susitvarkyti. [54] Valstybės ginkluoto užpuolimo atveju, tai būtų teisė į savigyną, nepaprastosios padėties ar karo stovio įvedimas, kuris apribotų pilietines teises ir laisves. Apibendrintai, saugumizacijos teorijoje saugumo problema yra tokia, kuri referentiniam objektui kelią egzistencinę grėsmę.

Siekiant sėkmingai pritaikyti saugumizacijos teorijos prielaidas tiriant judriojo penktosios kartos 5G ryšio saugumizavimo procesą JAV, yra svarbu apžvelgti saugumizacijos tyrimų modelio išskirtus vienetus, proceso etapus bei sėkmingos saugumizacijos sąlygas.

[49] Ten pat, 35.
[50] Jakniūnaitė, 35.
[51] Weaver, 35.
[52] Buzan, *Security: A New Framework for Analysis*, 21.
[53] Apie referentinius objektus plačiau bus kalbama vėliau.
[54] Ten pat, 21.

Saugumizavimo vienetai (angl. *types of units*). Kopenhagos mokyklos saugumo analizėje yra išskiriami trys vienetai, dalyvaujantys saugumizavimo procese:[55]

- Referentinis objektas. Bendrąja prasme, referentiniais objektais laikytina tai, kam kyla egzistencinė grėsmė ir kas turi legitimią priežastį išlikti. Tradiciniu požiūriu, referentiniu objektu yra laikoma valstybė bei tauta. Atitinkamai, valstybei kylanti egzistencinė grėsmė – suverenitetas, o tautai – identitetas. Kaip jau buvo minėta, jeigu referentinis objektas negali būti suprantamas be jam kylančios egzistencinės grėsmės, saugumizacijos proceso metu referentiniu objektu gali būti sukonstruota bet kas, o ne tik tradiciškai laikomos valstybės ir tautos. Visgi, anot autorių, kreipti dėmesį reiktų į sėkmingus referentinius objektus, kurių privalomas išlikimas yra pateisinamas ir geba mobilizuoti paramą. Vienas iš esminių kintamųjų, nulemiančių referentinių objektų sėkmę yra skalė. Skalės mažiausiame lygmenyje – individai ar nedidelės jų grupės; viduriniame – valstybės bei tautos; aukščiausias lygmuo – sisteminis (pvz., visa žmonija). Iš jų sėkmingiausias būtent antrasis.
- Saugumizuojantys veikėjai. Tai veikėjai, kurie kalbos aktu saugumizuoja problemą iki egzistencinės grėsmės referentiniui objektui. Įprastiniai saugumizuojantys veikėjai – vyriausybė, politinis elitas, kariuomenė, pilietinė visuomenė. Autoriai pabrėžia, jog saugumizuojančių veikėjų apibrėžimas gali būti problematiškas, nes kalbos aktą atliekantis veikėjas gali atstovauti individualų, organizacijos ar valstybinį lygmenius. Išeitis – koncentruotis į kalbos akto organizacinę logiką identifikuojant saugumizuojantį veikėją. Įprastai, veikėjų atskyrimas yra paprastesnis valstybiniu lygmeniu, nes vyriausybės atstovai kalba valstybės vardu.
- Įtakos veikėjai. Distinktyvus veikėjas saugumizacijos procese, galintis daryti įtaką sprendimų priėmimui saugumo srityje bei bendrai veikti sektoriaus dinamiką. Pvz., kariniame sektoriuje funkcinio veikėjo rolę gali užimti ginkluotės pramonės įmonės, samdinių kompanijos.[56] Nors vyriausybė yra esminis saugumizuojantis veikėjas sprendžiant šalies saugumo ir atsparumo iššūkius, tačiau minėti įtakos veikėjai gali paveikti formuojant užsienio ir saugumo politiką.

Kalbant apie saugumizacijos procesą ir etapus, reikia pabrėžti, jog tai yra diskursyvus, dviejų pakopų procesas, kurio metu nepolitizuotos (viešojoje erdvėje nėra kalbama) ar politizuotos (viešojoje erdvėje yra kalbama) problemos yra iškeliamos virš įprastų politinių klausimų, suteikiant problemai specialią reikšmę. Saugumizacija gali būti suprantama kaip kraštutinė politizacijos versija.[57] Pirmoji pakopa yra susijusi su konkrečios problemos, asmenų ar subjektų egzistencinės grėsmės pateikimu referentiniam

[55] Ten pat, 35-42.
[56] Ten pat, 56.
[57] Ten pat, 23.

objektui. Antrasis saugumizacijos procesas tampa sėkmingu tada, kai saugumizuojantis veikėjas įtikina atitinkamą auditoriją, jog problema išties kelia egzistencinę grėsmę, ir tokiu atveju galima imtis netipinių, anapus įprastinių politinių procedūrų ribų siūlomų priemonių.

O. Waever išskyrė, tris sąlygas, kurios gali prisidėti ir padidinti sėkmingos saugumizacijos galimybę.[58] Pirmiausia, saugumizuojantis kalbos aktas turėtų sekti įprastą „scenarijų“, t.y., egzistencinė grėsmė turėtų būti pristatyta kaip paaiškinimas, leidžiantis netipinių priemonių panaudojimą. Antra, saugumizuojantis veikėjas turėtų užimti tokią poziciją, kuri suteiktų jam pakankamai socialinio ir politinio kapitalo tam, kad įtikintų auditoriją grėsmės egzistavimu. Trečia, didesni šansai įtikinti auditoriją egzistencine grėsme yra tada, kai pastaroji grėsmė yra asocijuojama su istorine praeitimi, kurioje konkretūs objektai didžiąja dalimi yra siejami su pavojumi, žala ar priešišku nusiteikimu. Pavyzdžiui, tankas, kaip objektas suprantamas reliatyviai su panaudojimu kare, gali prisidėti vyriausybės atstovams ar saugumo ekspertams įgyvendinti sėkmingą kalbos aktą, jei kaimyninė valstybė dislokuoja tankus pasienyje. Visgi, šios sąlygos nėra savaime lemiančios saugumizacijos sėkmę. Veikiau, jos gali tik daryti įtaką saugumizacijos procesui, kurio esminis komponentas yra kalbos aktas.[59]

Apibendrinant, tradicinė Kopenhagos mokykla lėmė unikalaus analitinio saugumo tyrimų modelio iškylimą, suteikiantį galimybę aiškinti, kaip yra konstruojamos grėsmės bei kaip jos tampa saugumo darbotvarkės dalimi. Kita vertus, pirminė saugumizacijos teorija paliko daug erdvės interpretacijoms, kas atitinkamai lėmė teorijos kritiką, papildymus ir raidą. Dėl šios priežasties yra svarbu glaustai aptarti reikšmingus saugumizacijos teorijos vėlesnius aiškinimus.

1.2 Šiuolaikiniai saugumizacijos teorijos aiškinimai

Nuo pirminio pristatymo XX a. pabaigoje, saugumizacijos teorija tapo reikšminga tiriant saugumo problemas, todėl mokslininkų buvo nuolat vystoma ir plėtojama. Reikšmingai prie teorijos pildymo prisidėjusius mokslininkus galima skirti į dvi grupes: pirmoji, kurioje tyrėjai siekė į saugumizaciją įtraukti filosofines ir sociologines studijas bei koncentravosi į saugumizacijos sampratą; ir į antrąją, kurioje dėmesys yra skiriamas praktiniam saugumizacijos pritaikymui atvejo studijose.[60] Pastarojoje grupėje gilinamasi į tokius elementus kaip pozityvusis saugumas ar legitimumas. Papildomai,

[58] Ole Weaver, „The EU as a security actor: reflections from a pessimistic constructivist on postsovereign security orders.“ Kn. Morten Kelstrup (sud.) *International Relations Theory and the Politics of European Integration: Power, Security and Community*. Routledge, 2000, 252.
[59] Ten pat.
[60] Ieva Karpavičiūtė, „Securitization and Lithuania’s national security change.“ *Lithuanian Foreign Policy Review*, 36(1), 2017, 12. < https://content.sciendo.com/view/journals/lfpr/36/1/article-p9.xml?lang=en > [Žiūrėta 2020-04-05]

atsižvelgus į analitines preferencijas, saugumizacijos tyrėjus galima klasifikuoti į revizionistus, universalistus ir į kalbos aktą besikoncentruojančius mokslininkus. Kaip pabrėžia I. Karpavičiūtė, pirmoji mokslininkų grupė siekia peržiūrėti teoriją su tikslu sukurti labiau analitiškai operacionalius sėkmingos saugumizacijos kriterijus; universalistų darbais yra norima geografiškai už Vakarų išplėsti teorinį aiškinimą; trečioji grupė analizuoja kaip valstybės elito saugumo kalbos aktai ir praktikos naikina ribas tarp normalumo ir netipiškumo saugumo grėsmių srityje.[61] Taip pat svarbu atkreipti dėmesį, jog su laiku plėtėsi saugumo tyrimų laukas nuo pradinių B. Buzan ir O. Weaver identifikuotų saugumo sektorių. Pavyzdžiui, tapatybė ir migracija, visuotinė sveikata, aplinka ir energetika bei kibernetinis saugumas tapo vienomis iš pagrindinių temų naujesniuose saugumizacijos tyrimuose.

Auditorijos konceptas susilaukė nemažo dėmesio vėlesniuose saugumizacijos teorijos aiškinimuose. Tradicinėje Kopenhagos mokykloje auditorijai yra suteikiamas svarbus vaidmuo, nes problema gali būti saugumizuota tik tuo atveju, kai yra priimama auditorijos.[62] Visgi, pats konceptas susilaukė kritikų dėmesio, nes atsižvelgiant į jo svarbą, buvo menkai išvystytas ir liko aiškiai neapibrėžtas. Atsižvelgdamas į tai T. Balzaq argumentuoja, jog efektyvi saugumizacija yra ta, kuri yra orientuota į auditoriją (angl. *audience-centered*).[63] Kitaip tariant, saugumizacijos sėkmė yra didžiąja dalimi susijusi su saugumizuojančio veikėjo gebėjimu atsižvelgti ir prisitaikyti pagal auditorijos interesus, naudoti tinkamą ir artimą kalbą, jog grėsmė galėtų būti saugumizuota. Dėl šios priežasties, saugumizuojantis veikėjas gali sulaukti moralios arba formalios auditorijų paramos.[64] Tai žymi, jog saugumizacijos procese yra svarbu atkreipti dėmesį į auditorijų klasifikavimą, nes jos turi skirtingas funkcijas.

Remiantis šiomis prielaidomis, P. Roe argumentuoja, jog nors viešosios publikos parama saugumizuojančiam veikėjui yra neabejotinai reikšminga dėl moralinės paramos, tačiau, galiausiai, formali institucijų parama yra tai, kas suteikia galimybę pasitelkti netipines priemones saugumo problemai užkardyti.[65] Šį argumentą autorius pagrindžia 1998 m. Jungtinės Karalystės vyriausybės sprendimo įsitraukti į keturių dienų Irako bombardavimą kartu su JAV. Nors Ministrui Pirmininkui T. Blair pavyko įtikinti bendrąją publiką, vyriausybę bei Leiboristų partiją Irako keliama grėsme tariamai turint masinio naikino ginklus, tačiau nei viena minėtoji auditorija nesutiko pritarti papildomų priemonių

[61] Ten pat, 12-13.
[62] Buzan, *Security: A New Framework for Analysis*, 25.
[63] Thierry Balzacq, „The Three Faces of Securitization: Political Agency, Audience and Context." *European Journal of International Relations*, 11 (2), 2005. < https://journals.sagepub.com/doi/10.1177/1354066105052960 > [Žiūrėta 2020-04-05]
[64] Ten pat, 184.
[65] Paul Roe, „Actor, Audience(s) and Emergency Measures: Securitization and the UK's Decision to Invade Iraq." Peace Research Institute Oslo, 2008, 632. < https://journals.sagepub.com/doi/10.1177/0967010608098212 > [Žiūrėta 2020-04-06]

nei egzistavusios sulaikymo politikos panaudojimo. Taigi, nors grėsmė intersubjektyviai buvo suprantama ir saugumizuota, tačiau saugumizuojančio veikėjo siūlytos netipinės priemonės nebuvo priimtos.[66] Visgi, invazija į Iraką (netipinė priemonė) įvyko tik gavus Parlamento palaikymą (formali institucinė parama). Auditorijų atskyrimas ir jų išsiskiriantys paramos tipai leidžia išskirti du saugumizacijos proceso etapus. Pirmajame, problema yra identifikuojama kaip saugumo grėsmė ir ja yra siekiama gauti moralinį pritarimą. Antrajame, „mobilizacijos“ etape, yra siekiama gauti formalų palaikymą siekiant legitimaus netipinių priemonių panaudojimo.

Kad ir kaip būtų, pozicija, jog saugumizacijos pasisekimas didžiąja dalimi priklauso nuo to, ar auditorija yra įtikinama išlikimui kylančiomis grėsmėmis ir palaiko netipinių priemonių pasitelkimą, yra kritikuotina. Viena vertus, kritika kyla iš to, kad auditorijos pritarimas nėra vienareikšmis, nes yra galimybė, jog egzistuoja ne viena, o kelios varijuojančios auditorijos. Galima išskirti populiariąją, elito, technokratinę ir akademines auditorijas, kurios skirtingai gali lemti kalbos akto sėkmę.[67] Taip pat, auditorijos sąvokos neišplėtojimą vėliau pabrėžia ir patys B. Buzan ir O. Weaver, teigdami, jog saugumizacijos procese išskirti ir identifikuoti svarbias auditorijas yra ypatingai sunku, jeigu išvis įmanoma.[68]

Diskusijoje dėl saugumizacijos proceso, R. Floyd pateikė savąjį sėkmingos saugumizacijos aiškinimą, kuriame išdėstytos įžvalgos yra svarbios ir šiam darbui.[69] Šis aiškinimas kilo iš dvejopos saugumizacijos teorijos kritikos, susijusios su proceso sėkmės prielaidomis. Pirma, autorė sukritikuoja tradiciškai ir, vėliau, P. Roe ir T. Balzaq plėtotą mintį dėl auditorijos reikšmės saugumizacijoje. Pateikiant šešis skirtingus kalbos aktų ir auditorijos reakcijos į juos scenarijus, yra prieinama prie išvados, jog nėra įtikinančio ryšio tarp auditorijos sankcionuojamų kalbos aktų ir saugumizacijos proceso sėkmės.[70] Kartais auditorijos atsakas į saugumizuojantį veiksmą yra svarbus, o kartais – ne. Atsižvelgiant į tai, yra prieštaraujama tradicinei saugumizacijos prielaidai ir teigiama, jog sankcionuojanti auditorija neturi lemiamos rolės sugrėsminimo egzistavime ir pasisekime. Antroji kritikos dalis yra susijusi su

[66] Ten pat, 633.
[67] Mark B. Salter, „Securitization and Desecuritization: A Dramaturgical Analysis of the Canadian Air Transport Security Authority". *Journal of International Relations and Development,* 11(4), 2008, 321. < https://link.springer.com/article/10.1057/jird.2008.20 > [Žiūrėta 2020-04-06]
[68] Barry Buzan ir Ole Wæver, „Macrosecuritisation and Security Constellations: Reconsidering Scale in Securitization Theory." *Review of International Studies,*35(2), 2009, 253-276. < https://www.cambridge.org/core/journals/review-of-international-studies/article/macrosecuritisation-and-security-constellations-reconsidering-scale-in-securitisation-theory/B693D7C852112FA05E1999A5B9A0604A > [Žiūrėta 2020-04-07]
[69] Rita Floyd, „Extraordinary or ordinary emergency measures: What, and who, defines the 'success' of securitization?" *Cambridge review of international affairs,* 29(2), 2016. < https://www.tandfonline.com/doi/pdf/10.1080/09557571.2015.1077651 > [Žiūrėta 2020-04-08]
[70] Ten pat, 689-691.

problemų, kaip egzistencinių grėsmių įrėminimu.[71] Klasikinėje saugumizacijos teorijoje numatoma, jog problemos turi kelti grėsmę referentinio objekto išlikimui, jog būtų sėkmingai saugumizuotos. R. Floyd prieštarauja šiam teiginiui argumentuodama, jog saugumizuojantys veikėjai gali siekti netipinių priemonių legitimacijos dėl grėsmių, kurios nebūtinai yra egzistencinės, o verčiau – žalingos ar tiesiog pavojingos.[72]

Atsispiriant nuo minėtos kritikos, yra pasiūlomas alternatyvus požiūris. Saugumizacija yra sėkminga tik tuo atveju, kai saugumizuojantys veikėjai veikia atitinkamai pagal saugumizuojantį kalbos aktą, o ši veikla yra pastebima kaip elgesio pokytis bei veiksmų pateisinimas.[73] Šiuo požiūriu, saugumizacija geriausiai suprantama kaip kauzalinis procesas, kuriame centrinis dėmesys turėtų būti skiriamas saugumizuojančių veikėjų veiksmams ir elgesiui. Taigi, anot R. Floyd, saugumizacijos procesas gali būti vadinamas sėkmingu tada, kai:

- Identifikuojamos grėsmes, kurios pateisina atsaką (saugumizuojančius veiksmus) į jas;
- Yra matomas saugumizuojančio veikėjo veiklos pokytis, sprendimai;
- Šie priimti saugumizuojančio veikėjo sprendimai yra pateisinami grindžiant atsako metu įvardintomis kylančiomis grėsmėmis.[74]

Taigi, apžvelgus saugumizacijos teorinius aspektus, toliaus bus pereinama prie darbo empirinės dalies - 5G saugumizacijos JAV atvejo tyrimo. Jame kokybinio turinio analizės būdu yra siekiama ištirti saugumizuojančių veikėjų kalbos aktus norint atskleisti, ar per diskursą šios problemos yra saugumizuojamos ir perkeliamos į valstybės saugumo darbotvarkę. Viešuosiuose pasisakymuose dėmesys atkreipiamas į grėsmes ir siūlomas priemones joms suvaldyti. Vėliau, bus pateikta oficialių dokumentų analizė, siekiant išsiaiškinti, ar deklaruotos politikų 5G diegimo problemos atsispindi kaip saugumizuotos problemos oficialiame/teisiniame diskurse.

2. 5G ryšio saugumizavimas JAV viešojoje erdvėje

Šioje empirinio tyrimo dalyje yra pateikiama 5G ryšio problemų grėsminimo analizė JAV viešojoje erdvėje. Kokybinio turinio analizės metodu buvo išanalizuoti išskirtų veikėjų 32 kalbos aktai, t.y. vieši pasisakymai ir kalbos, pranešimai spaudai. Tyrimui pasirinkti 5 saugumizuojantys veikėjai, tai:

[71] Ten pat.
[72] Ten pat.
[73] Ten pat, 688.
[74] Ten pat, 684.

JAV prezidentas Donald Trump, viceprezidentas Mike Pence, valstybės sekretorius Mike Pompeo, gynybos sekretorius Mark Esper ir Valstybės departamento kibernetinių ir tarptautinių komunikacijų bei informatikos politikos sekretoriaus padėjėjo pavaduotojas (toliau – SPP) Robert Strayer. Remiantis teorine prieiga, penki pasirinkti asmenys – aukšto politinio rango JAV pareigūnai – yra priskiriami saugumizuojančiais veikėjais dėl jų reikšmingo politinio ir socialinio statuso visuomenėje.[75]

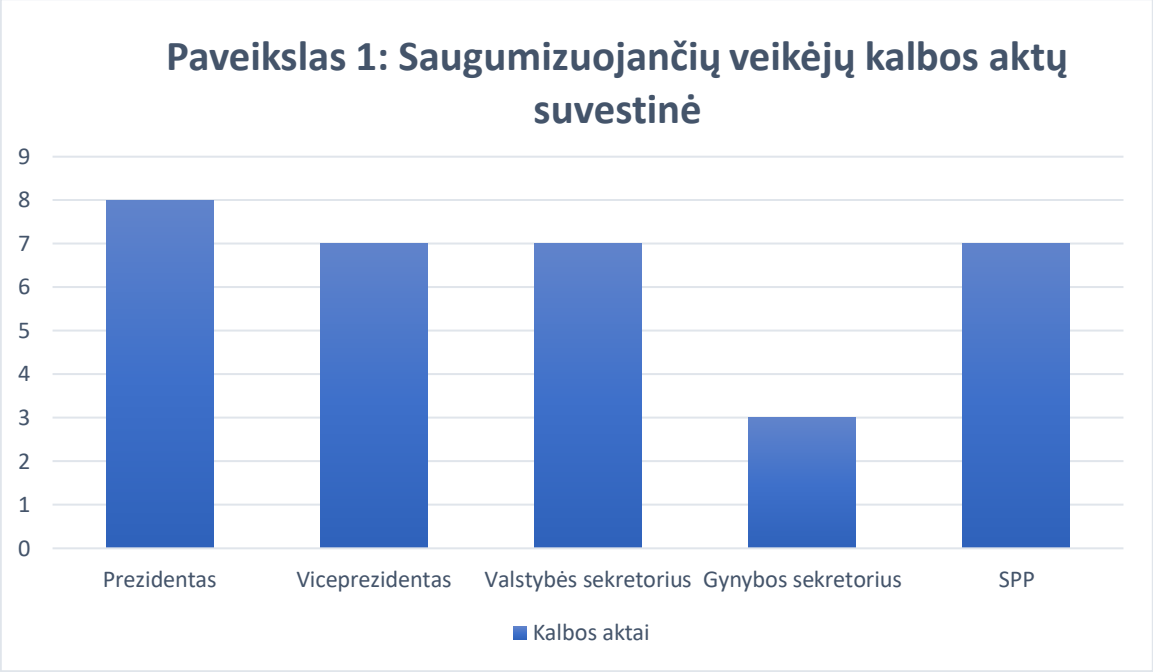
Analizuojamų kalbos aktų laikotarpis yra nuo 2019 metų iki 2020 metų kovo mėnesio. Ši data yra pasirinkta todėl, nes 2019 metais JAV viešojoje erdvėje buvo pradėta kalbėti apie 5G problemas, o 2020 metų kovo mėnesį įsigaliojo du svarbūs, su 5G saugumizacija susiję oficialūs dokumentai – JAV Nacionalinė Strategija 5G apsaugoti (angl. *National Strategy to Secure 5G*) ir 2019 metų Saugių ir Patikimų Ryšių Aktas (angl. *Secure and Trusted Communications Networks Act of 2019*), įsigaliojęs JAV prezidentui pasirašius jį 2020 metų kovo 12 dieną.

Nagrinėjami saugumizuojančių veikėjų kalbos aktai buvo skirstomi į dvi kategorijas, atsižvelgiant į teorines prielaidas, tai – grėsmes ir netipines priemones. Bendrai, analizuojant pasisakymus, buvo ieškoma, kaip išskirti veikėjai pasisakė šiais aspektais:

1) 5G ryšio problematikos įvardijimas kaip saugumo grėsmė ir kam referuojama ši grėsmė?
2) Ar yra nurodomas grėsmės šaltinis?
3) Kokias netipines priemones įvardija saugumizuojantys veikėjai norint apsisaugoti nuo grėsmės?

Iš 32 bendrų kalbos aktų, 8 priskirti Prezidentui, 7 – Viceprezidentui, 7 – Valstybės sekretoriui, 3 – Gynybos sekretoriui, 7 – SPP (žr. paveikslas 1). Svarbu atkreipti dėmesį, jog analizuojant šių veikėjų pasisakymus viešojoje erdvėje, terminai „*5G infrastruktūra*“, „*5G ryšys*“, „*5G tinklai*“ yra laikomi sinonimais.

[75] Weaver, *The EU as a security actor: reflections from a pessimistic constructivist on postsovereign security orders*, 252.



Šaltinis: autorius, remiantis tyrimo duomenimis.

Toliau, remiantis tyrimo duomenimis, šiame skyriuje bus analizuojama, kaip JAV valstybės pareigūnai 5G problematikos tema kalbėjo viešojoje erdvėje atsižvelgiant į išskirtus aspektus.

2.1 5G kaip grėsmės diskursas

Remiantis tyrimo duomenimis galima teigti, jog daugumoje pasisakymų, 5G problematika yra įvardijama kaip saugumo problema, kelianti, pirmiausia, grėsmę JAV nacionaliniam saugumui ir ekonomikai. JAV prezidentas pabrėžia, jog „Saugūs 5G tinklai bus absoliučiai gyvybiškai svarbi grandis JAV klestėjimui ir nacionaliniam saugumui 21-ame amžiuje.“[76] Papildomai, Valstybės sekretorius asmeniniame socialiniame tinkle „Twitter“ pasidalino pranešimu, kuriame argumentuoja: „Dėl #5G revoliucijos, komunikacijos tinklų saugumas yra dar labiau kritiškai svarbus JAV, mūsų partnerių ir sąjungininkų nacionaliniam saugumui.“[77] Taip pat, SPP R. Strayer atkreipia dėmesį, kad „Atsižvelgiant į 5G apimtį, apsaugoti šiuos gyvybiškai svarbius tinklus yra nepaprastai svarbu“[78] ir „Informacinių ir

[76] The White House, „*Remarks by President Trump on United States 5G Deployment*“, 2019. < https://www.whitehouse.gov/briefings-statements/remarks-president-trump-united-states-5g-deployment/ > [Žiūrėta 2020-05-10]
[77] Secretary Mike Pompeo’s [@SecPompeo] Tweet, February 27, 2019. < https://twitter.com/SecPompeo/status/1100600759383670785 > [Žiūrėta 2020-05-18]
[78] U.S. Department of State, „*Remarks at the 2019 Internet Governance Forum USA Conference*“, July, 2019. < https://www.state.gov/remarks-at-the-2019-internet-governance-forum-usa-conference/ > [Žiūrėta 2020-05-18]

Telekomunikacinių Technologijų, ar ITT, saugumas yra esminis nacionalinio saugumo elementas. ITT sudarantys tinklai ir paslaugos vaidina kritinę rolę kiekvienos tautos saugume ir klestėjime.“[79] Taigi, saugumizuojančių veikėjų diskursas, o konkrečiai – frazės „absoliučiai gyvybiškai svarbi“, „kritiškai“, „nepaprastai svarbus“, leidžia daryti išvadą, jog yra akcentuojamas ne tik 5G apsaugojimo poreikis, bet pabrėžiama, jog nesaugūs tinklai keltų egzistencinę grėsmę JAV nacionaliniam saugumui ir ekonomikai.

Analizuojant kalbos aktus pastebima, jog juose yra dažnai minima 5G reikšmė kritinei infrastruktūrai ir paslaugoms, intelektinės nuosavybės ir asmeninės informacijos saugumui. Pavyzdžiui, valstybės sekretorius teigia, jog „5G tinklai palies kiekvieną mūsų gyvenimo aspektą, įskaitant elektros tinklus, autonomines transporto priemones, išmanią gamybą, medicininį gydymą ir asmeninius duomenis.“[80], o prezidentas: „Greitai, didžioji dalis mūsų kritinės infrastruktūros bus prijungta šių naujų tinklų.“[81], taip pat „Dešimtys milijardų naujų prietaisų ir jutiklių bus sujungti į internetą 5G ryšiu per ateinančius artimiausius metus, įskaitant elektros paskirstymą.“[82] Atsižvelgiant į būsimą platų 5G pritaikymą visuomenėje, didės kritinės infrastruktūros priklausomybė nuo šio naujosios kartos ryšio. Todėl, kaip yra argumentuojama viešuose pasisakymuose, neapsaugotas 5G ryšys kelia grėsmę valstybės kritinei infrastruktūrai, kritinėms paslaugoms bei privačiai informacijai dėl galimo šnipinėjimo ar funkcionavimo trikdymo.

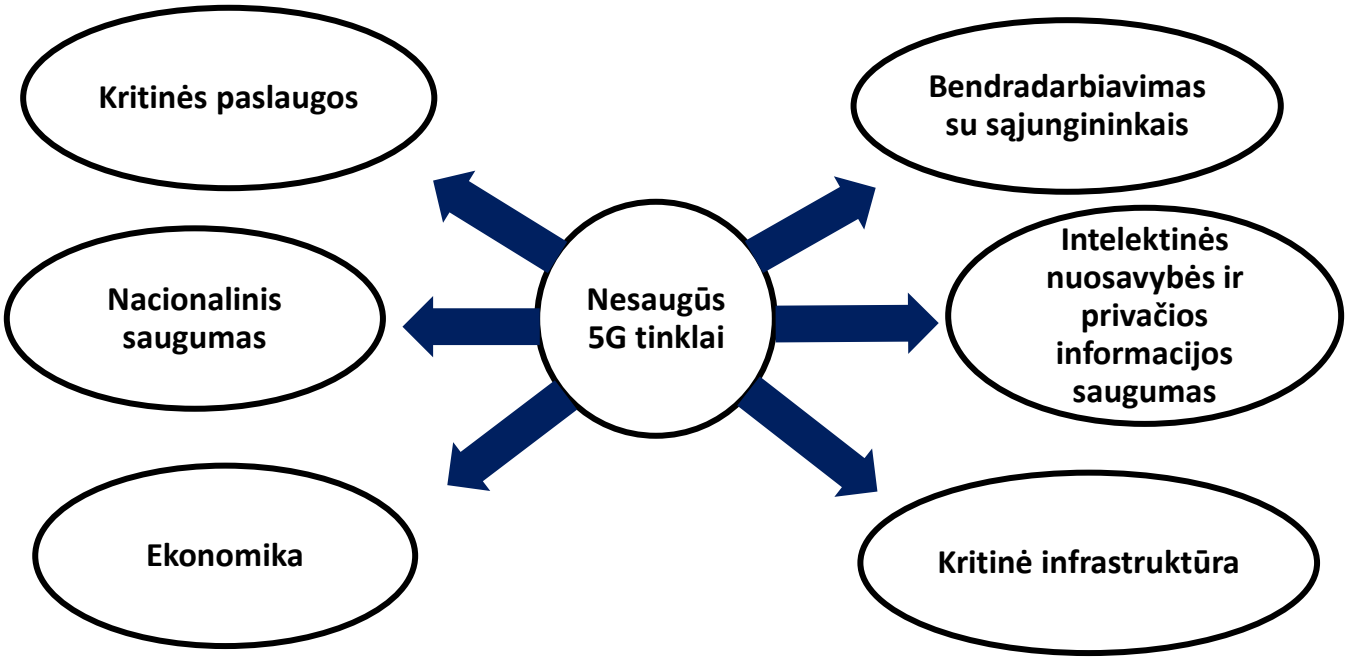
Papildomai, viešuose pasisakymuose yra pabrėžiama nesaugaus 5G ryšio grėsmė JAV bendradarbiavime su sąjungininkais. JAV gynybos sekretorius teigia, jog įdiegtos nesaugios 5G technologijos „galėtų pakenti mūsų galimybėms dalintis žvalgybine informacija, atlikti planavimus ar saugiai komunikuoti [NATO] aljanse.“[83]. Gynybos sekretorius pabrėžia, jog gebėjimas veikti kartu su sąjungininkais bendruose komunikacijų tinkluose tarnauja kaip galios daugiklis, tačiau tuo pat metu tai lemia padidėjusią riziką ir kelia pavojų karinei sąveikai, jei tinklai nėra saugūs. Šiai pozicijai antrina ir valstybės sekretorius. Anot jo, „Nepakankamas saugumas kliudys JAV dalintis tam tikra informacija

[79] U.S. Department of State, „*Press Briefing with Deputy Assistant Secretary Robert Strayer, Cyber and International Affairs and Information Policy, Bureau of Economic and Business Affairs*“, May 8, 2019. < https://www.state.gov/press-briefing-with-deputy-assistant-secretary-robert-strayer-cyber-and-international-affairs-and-information-policy-bureau-of-economic-and-business-affairs-2/ > [Žiūrėta 2020-05-18]
[80] U.S. Department of State, „United States Welcomes the EU's Acknowledgement of the Unacceptable Risks Posed by Untrusted 5G Suppliers“, January 30, 2020. < https://www.state.gov/united-states-welcomes-the-eus-acknowledgement-of-the-unacceptable-risks-posed-by-untrusted-5g-suppliers/ > [Žiūrėta 2020-05-18]
[81] The White House, „Raising the Bar to Protect Federal Government and Private-Sector Data“, July 25, 2019. < https://www.whitehouse.gov/articles/raising-bar-protect-federal-government-private-sector-data/ > [Žiūrėta 2020-05-18]
[82] U.S. Department of State, „*Remarks at the 2019 Internet Governance Forum USA Conference*“.
[83] Council on Foreign Relations, „*U.S. Defense Priorities and Policies: A Conversation With Secretary Mark T. Esper*“, December 13, 2019. < https://www.cfr.org/event/us-defense-priorities-and-policies-conversation-secretary-mark-t-esper-0 > [Žiūrėta 2020-05-18]

patikimuose tinkuose.“[84] Taip pat, M. Pompeo teigimu, nesaugaus bendro 5G tinklo atveju „kai kuriais atvejais, yra rizika, jog mes negalėsime skirti amerikietiškų resursų, amerikietiškų ambasadų ir karinių forpostų.“[85] Taigi, nesaugūs 5G tinklai JAV kelia grėsmę bendradarbiavime su sąjungininkais, konkrečiai įvardinant jautrios žvalgybinės informacijos dalijimąsi ir karinį sąveikumą.

Apibendrinus galima teigti, jog visi JAV valstybės pareigūnai viešuose pasisakymuose apie 5G problematiką kalba grėsmės kontekste. Nors pasisakymuose dažnai teigiama, jog neapsaugoti 5G tinklai kelia ypatingą grėsmę JAV nacionaliniam saugumui ir ekonomikai, taip pat yra atkreipiamas dėmesys ir į kitas sritis, kaip kritinė infrastruktūra ar kritinės paslaugos (žr. paveikslas 2).

Paveikslas 2: Nesaugių 5G tinklų grėsmės referentiniai objektai, įvardinti saugumizuojančių veikėjų



Šaltinis: autorius, remiantis tyrimo duomenimis. Rodyklės kryptis rodo, kam keliama grėsmė.

2.2 Grėsmės šaltinis ir 5G saugumas

Keliuose saugumizuojančių veikėjų viešuosiuose pasisakymuose yra minimas nekonkretus 5G tinklų grėsmės šaltinis. Pavyzdžiui, JAV prezidentas atkreipia dėmesį, jog: „Su šiomis jungtimis,

[84] Stephen Castle, „*Pompeo Attacks China and Warns Britain Over Huawei Security Risks*“, May 8, 2019. < https://www.nytimes.com/2019/05/08/technology/pompeo-huawei-britain.html > [Žiūrėta 2020-05-18]
[85] Derek B. Johnson „*Pompeo: Huawei deals threatens info-sharing with allies*“, February 22, 2019. < https://fcw.com/articles/2019/02/22/pompeo-huawei-info-sharing.aspx > [Žiūrėta 2020-05-18]

amerikiečių tėvynė bus kelių mygtukų paspaudimų atstumu nuo valstybinių ir nusikalstamų kibernetinių veikėjų su pajėgumais ir motyvacija padaryti žalą amerikiečiams.“ Taigi, 5G tinklų saugumui grėsmę kelia nusikalstama kibernetine veikla užsiimantys tiek valstybiniai, tiek nevalstybiniai veikėjai.

Visgi, visi saugumizuojantys veikėjai daugumoje viešų pasisakymų kaip grėsmės šaltinį tiesiogiai įvardija Kiniją ir kiniškas 5G infrastruktūros įrangos gamintojas – Huawei, o rečiau – ZTE. „[...] mes manome, jog Huawei yra nesuderinamas su JAV saugumo interesais“, pabrėžė viceprezidentas M. Pence.[86] Kalbėdamas apie Huawei, JAV prezidentas akcentavo, jog „[...]mes įžvelgiame milžinišką saugumo problemą Huawei atžvilgiu.“[87] Papildomai, valstybės sekretorius teigė, jog Huawei kelia grėsmę JAV, nes šios įmonės įdiegta 5G infrastruktūra keltų amerikietiškų technologijų vagysčių ir įsibrovimo į privačią žmogaus informaciją riziką.[88]

Kinija ir Huawei, kaip grėsmė 5G tinklų saugumui, yra įvardijama daugumoje kalbos aktuose. Pirmiausia, Huawei technologinių komponentų diegimas 5G infrastruktūroje kelia grėsmę dėl Huawei, kaip „didelės rizikos“ tiekėjo reputacijos, kuris turi „ilgą intelektinės nuosavybės vagysčių ir korupcijos įstatymų pažeidimų istoriją“, pvz., JAV Huawei yra kaltinama dėl intelektualinės nuosavybės vagystės iš kitos mobilių telekomunikacijų įmonės T-Mobile.[89] Antra, yra manoma, jog Huawei keltų grėsmę 5G tinklų saugumui dėl Kinijos įstatyminės bazės. Kinijos Nacionalinis Žvalgybos Įstatymas įpareigoja įmones, įskaitant 5G technologijų pardavėjus kaip Huawei, „bendradarbiauti su žvalgybos ir saugumo tarnybomis be nepriklausomos teisinės kontrolės.“[90] Kitaip tariant, Kinijos teisinė sistema suteikia galimybę vyriausybei nurodyti Huawei dalintis informacija ir imtis slaptų, nedeklaruotų veiksmų. Todėl „Jei kiniškos kompanijos toliau tęs pamatinės 5G infrastruktūros statybas, jie bus geresnėje pozicijoje pasinaudoti prieiga“ prie kritinės infrastruktūros ir informacijos.[91]

---

[86] The White House, „*Remarks by Vice President Pence and Prime Minister Trudeau of Canada in Joint Press Statements*“, May 30, 2019. < https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-prime-minister-trudeau-canada-joint-press-statements-ottawa-canada/ > [Žiūrėta 2020-05-18]

[87]The White House, „*Remarks by President Trump and Prime Minister Trudeau of Canada Before Bilateral Meeting*“, December 3, 2019. < https://www.whitehouse.gov/briefings-statements/remarks-president-trump-prime-minister-trudeau-canada-bilateral-meeting-london-united-kingdom/ > [Žiūrėta 2020-05-18]

[88] U.S. Department of State, „*Remarks to the Future Farmers of America*“, March 4, 2019. < https://www.state.gov/remarks-to-the-future-farmers-of-america/ > [Žiūrėta 2020-05-18]

[89] U.S. Department of State, *„Press Briefing with Deputy Assistant Secretary Robert Strayer“*, October 15, 2019. < https://www.state.gov/telephonic-press-briefing-with-deputy-assistant-secretary-robert-strayer-cyber-and-international-affairs-and-information-policy-bureau-of-economic-and-business-affairs/ > [Žiūrėta 2020-05-18]

[90] U.S. Department of State, *„Press Briefing with Deputy Assistant Secretary Robert Strayer, Cyber and International Affairs and Information Policy, Bureau of Economic and Business Affairs“*, May 8, 2019. < https://www.state.gov/press-briefing-with-deputy-assistant-secretary-robert-strayer-cyber-and-international-affairs-and-information-policy-bureau-of-economic-and-business-affairs-2/ > [Žiūrėta 2020-05-18]

[91] U.S. Department of State, *„Press Briefing with Deputy Assistant Secretary Robert Strayer*“, July 11, 2019. < https://www.state.gov/press-briefing-with-deputy-assistant-secretary-robert-strayer/ > [Žiūrėta 2020-05-18]

Remiantis šia logika, R. Strayer teigia, jog kiniškų 5G tiekėjų „gali būti paprašyta pažeisti tinklo saugumą siekiant, pavyzdžiui, pavogti asmeninę informaciją ar intelektinę nuosavybę, vykdyti šnipinėjimą ar trikdyti kritines paslaugas.“[92] Papildomai, valstybės sekretorius M. Pompeo sugrėsmina Huawei ir kitas Kinijos valstybės remiamas technologijų kompanijas, pavadindamas jas Trojos arkliais Kinijos žvalgybos tarnyboms.[93] Apie Kinijos ir Huawei grėsmę 5G tinklų saugumui pabrėžia ir kiti išskirti saugumizuojantys veikėjai, pavyzdžiui, gynybos sekretorius atkreipia dėmesį, jog „Priklausomybė nuo kiniškų 5G tiekėjų, pavyzdžiui, galėtų daryti mūsų partnerių kritines sistemas pažeidžiamas trikdymams, manipuliacijai ir šnipinėjimui.“[94]

Svarbu paminėti, jog be įvardintų Kinijos ir kiniškų 5G infrastruktūros pardavėjų grėsmės, saugumizuojančių veikėjų pasisakymuose pasitaiko tiesiogiai neįvardintų nepatikimų tiekėjų ir nesaugios tiekimo grandinės grėsmės deklaravimų. Pavyzdžiui, R. Strayer teigimu, „JAV nori užtikrinti, jog mes, mūsų partneriai bei sąjungininkai išlaikytume saugius ir patikimus komunikacijų tinklus bei tiekimo grandines, jog sumažintume nesankcionuotos prieigos ir žalingos kibernetinės veiklos rizikas.“[95] Taip pat, JAV prezidentas pabrėžia: „Yra kritiškai svarbu, jog mes naudotume saugius ir patikimus technologijų tiekėjus, komponentus ir tiekimo grandinę.“[96] Kad ir kaip būtų, atsižvelgiant į pasisakymų kontekstą, saugumizuojantys veikėjai grėsmę dėl nepatikimų tiekėjų ir tiekimo grandinės vis tik asocijuoja su kiniškomis 5G įrangos gamintojomis ir jų priklausomybe nuo Kinijos vyriausybės.

Šioje vietoje atsispindi 5G saugumizavimo JAV geopolitinis aspektas. Faktiškai, 5G infrastruktūros įrangą globaliu mastu gali tiekti 5 įmonės, dvi iš jų – kiniškos Huawei ir ZTE. Nors apie tai bus plačiau rašoma netipinių priemonių poskyryje, tačiau daugumoje kalbos aktuose, įvardinus didelės rizikos tiekėjų ir nesaugios tiekimo grandinės grėsmę, vėliau yra ši grėsmė yra sugretinama su kiniškomis kompanijomis ir siūloma jų atsisakyti. Pavyzdžiui, R. Strayer argumentuoja, jog JAV nori užtikrinti savo ir sąjungininkų saugius ir patikimus komunikacijų tinklus ir tiekimo grandines, bet tuo pat metu pabrėžia svarbą atkreipti į Huawei ir kitų kiniškų informacinių technologijų keliamą grėsmę.[97]

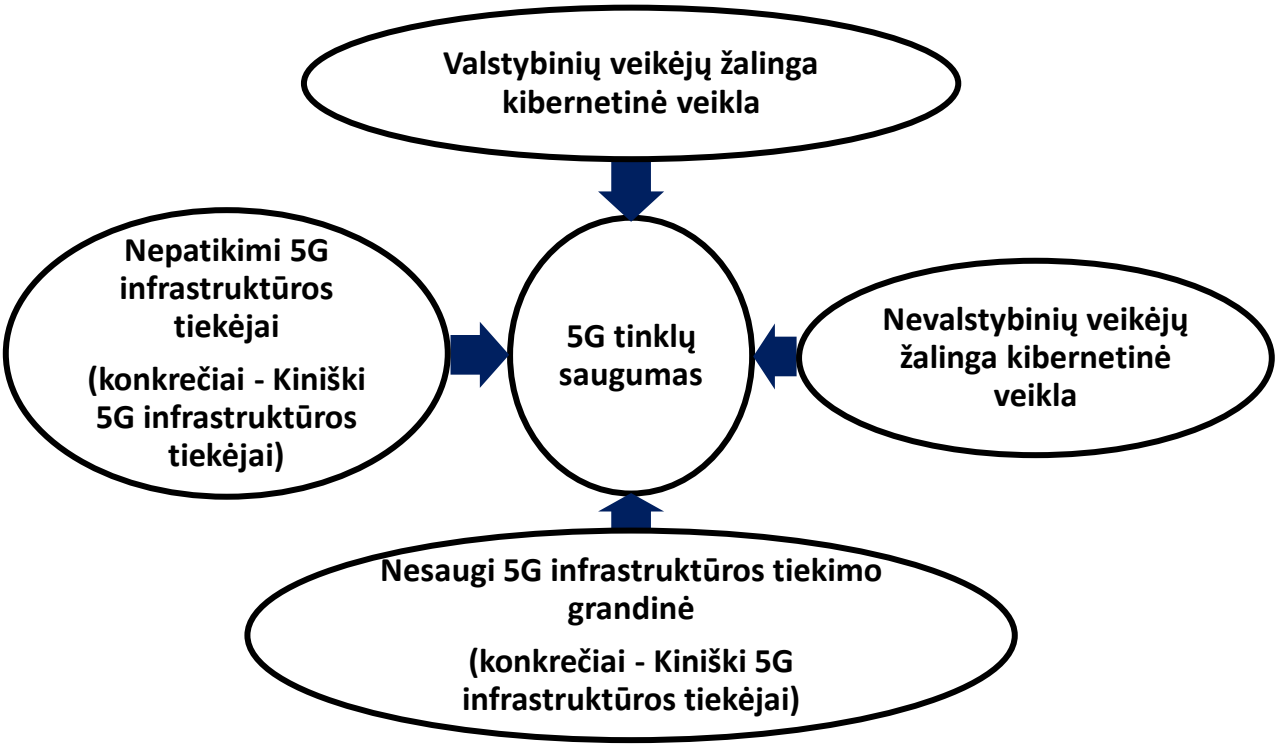
---

[92] Ten pat.
[93] U.S. Embassy in Luxembourg, „*Secretary Pompeo and Secretary Esper Speak at Munich Security Conference 2020*”, February 19, 2020. < https://lu.usembassy.gov/secretary-pompeo-and-secretary-esper-speak-at-munich-security-conference-2020/ > [Žiūrėta 2020-05-18]
[94] U.S. Department of Defense, „*As Prepared Remarks by Secretary of Defense Mark T. Esper at the Munich Security Conference*”, February 15, 2020. < https://www.defense.gov/Newsroom/Speeches/Speech/Article/2085577/as-prepared-remarks-by-secretary-of-defense-mark-t-esper-at-the-munich-security/ > [Žiūrėta 2020-05-18]
[95] U.S. Department of State, „*Remarks at Press Availability”,* February 26, 2019. < https://www.state.gov/remarks-at-press-availability/ > [Žiūrėta 2020-05-18]
[96] The White House, *„Remarks by President Trump and President Niinistö of the Republic of Finland in Joint Press Conference”*, October 2, 2019. < https://www.whitehouse.gov/briefings-statements/remarks-president-trump-president-niinisto-republic-finland-joint-press-conference/ > [Žiūrėta 2020-05-18]
[97] U.S. Department of State, „*Remarks at Press Availability*”, February 26, 2019

Taip pat, yra kalbama apie poreikį diegiant 5G tinklus naudoti tik patikimus teikėjus – tris nekiniškas įrangos pardavėjus – europietiškus Nokia, Ericsson bei Pietų Korėjos Samsung, kurios nėra kontroliuojamos autoritarinių vyriausybių.[98] Tokiu būdu JAV siekia, jog kitose valstybėse nebūtų naudojamos kiniškos 5G technologijos.

Apibendrintai, kaip grėsmę 5G tinklų saugumui, JAV saugumizuojantys veikėjai išskyrė valstybinių ir nevalstybinių veikėjų žalingą kibernetinę veiklą, nepatikimus 5G infrastruktūros tiekėjus ir nesaugia infrastruktūros tiekimo grandinę. (žr. paveikslas 3)

Paveikslas 3: Saugumizuojančių veikėjų išskirtos grėsmės 5G tinklų saugumui



Šaltinis: autorius, sudaryta remiantys tyrimo duomenimis.

[98] Cybersec Forum, „*Robert Strayer, Deputy Assistant Secretary of State, U.S. Department of State*", January 9, 2020. 1:25-1:42. < https://www.youtube.com/watch?v=nnmTlHwPGVg > [Žiūrėta 2020-05-18]

2.3 Netipinės priemonės

Analizuojant kalbos aktus buvo kreipiamas dėmesys, ar kalbant apie 5G grėsmes, kartu aukšto politinio rango JAV pareigūnai kalbėjo ir apie netipines priemones, padėsiančias apsisaugoti nuo kylančių grėsmių.

Viena iš saugumizuojančių veikėjų išskirtų netipinių priemonių 5G saugumui užtikrinti – poreikis JAV turėti rizika grįstą vertinimą ir kriterijus, kurie apsaugotų nuo nepatikimų 5G infrastruktūros tiekėjų dalyvavimo ryšių diegime. Kaip pabrėžė D. Trump, „yra kritiškai svarbu, jog mes naudotume saugius ir patikimus technologijų tiekėjus, komponentus ir tiekimo grandinę.“[99] R. Strayer teigia, jog „mes turėtume atidžiai įvertinti ir išskirti tiekėjus, kontroliuojamus užsienio vyriausybių, kuriose nėra reikšmingų stabdžių ir atsvarų jų galiai priversti tuos tiekėjus bendradarbiauti su žvalgybos ir saugumo tarnybomis.“[100] Taigi, atsižvelgiant į nepatikimų 5G infrastruktūros tiekėjų ir nesaugios infrastruktūros grandinės grėsmes, yra siūloma JAV sukurti apsaugos mechanizmą, suteikiantį galimybę drausti didelės rizikos tiekėjams dalyvauti 5G diegime.

Ši netipinė priemonė tiesiogiai yra susijusi su daugelio saugumizuojančių veikėjų išsakytu poreikiu siekti alternatyvos Huawei 5G technologijoms. Taip galima teigti todėl, nes visi penki aukšto rango JAV pareigūnai išskyrė Huawei kaip grėsmę ir pasisakė už svarbą rinktis kitus, patikimus tiekėjus. Pavyzdžiui, viceprezidentas M. Pence argumentuoja, jog yra svarbu bendradarbiauti su kitomis pasaulinėmis telekomunikacijų įmonėmis, kad „vystyti 5G alternatyvas Huawei“.[101] R. Strayer antrina šiai pozicijai dėl alternatyvos Huawei, siūlydamas naudoti kitus, anot jo, patikimus 5G infrastruktūros tiekėjus – Nokia, Ericsson ir Samsung.[102]

Saugumizuojantys veikėjai akcentuoja ir netipinę priemonę skatinti saugių 5G tinklų diegimą užsienio valstybėse. R. Strayer teigimu, yra svarbu raginti kitas valstybes jog jos, kaip ir JAV, turėtų saugumo mechanizmą ir taikytų saugumo standartus, suteikiančius galimybę įvertinti 5G tiekėjų patikimumą ir jų santykį su vyriausybe, kurioje pardavėjai yra įsikūrę.[103] Papildomai, yra įvardijamas poreikis kartu su kitomis valstybėmis įgyvendinti Prahos 5G saugumo konferencijoje paskelbtus siūlymus tarptautiniu lygmeniu, kaip netipinę priemonę apsaugoti 5G ryšio tinklus nuo priešiškų veikėjų

---

[99] The White House, „*Remarks by President Trump and President Niinistö of the Republic of Finland in Joint Press Conference*”, October 2, 2019.
[100] U.S. Department of State, *„Press Briefing with Deputy Assistant Secretary Robert Strayer*“, July 11, 2019.
[101] The White House, „*Remarks by Vice President Pence and Taoiseach Varadkar of Ireland in Joint Press Statement*, September 3, 2019. < https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-taoiseach-varadkar-ireland-joint-press-statement-dublin-ireland > [Žiūrėta 2020-05-18]
[102] Cybersec Forum, ten pat.
[103] U.S. Department of State, „*Press Briefing with Deputy Assistant Secretary Robert Strayer Cyber and International Affairs and Information Policy Bureau of Economic and Business Affairs*“, April 10, 2019. < https://www.state.gov/press-briefing-with-deputy-assistant-secretary-robert-strayer-cyber-and-international-affairs-and-information-policy-bureau-of-economic-and-business-affairs/ > [Žiūrėta 2020-05-08]

dalyvavimo diegiant infrastruktūrą.[104] JAV skatina kitas valstybes atsižvelgti į Prahos 5G konferencijos siūlymus, kaip geriausias saugumo praktikas, diegiant 5G infrastruktūrą. Prie šių priemonių taip pat galima paminėti vienintelio JAV prezidento išskirtą daugiašalio Mėlynojo Taško Tinklo (angl. *Blue Dot Network*) iniciatyvos vystymą. Šia iniciatyva yra siekiama, jog ateities infrastruktūra, įskaitant 5G, būtų statoma remiantis saugumo, skaidrumo ir atskaitomumo principais, kad pasaulio valstybės turėtų prieigą prie tvaraus, patikimo ir aukštos kokybės infrastruktūros vystymo.[105] Visgi, iniciatyva, į kurią be JAV yra įsitraukusios Australija ir Japonija, yra tik ankstyvojoje įgyvendinimo stadijoje.

Apibendrinus šią empirinę tyrimo dalį galima teigti, jog išskirti 5 JAV aukšto politinio rango pareigūnai savo 5G problematiką kalbos aktais konstravo kaip saugumo grėsmės. Daugelyje pasisakymų pabrėžiama, jog 5G tinklų saugumas yra gyvybiškai svarbus, nes neapsaugoti 5G tinklai kelia grėsmę tokioms sritims kaip JAV nacionalinis saugumas, ekonomika ar kritinė infrastruktūra. Nors, kalbant apie grėsmės 5G saugumui šaltinius, išskirti valstybiniai ir nevalstybiniai žalinga kibernetine veikla užsiimantys veikėjai, daugiausiai minimas grėsmės šaltinis – kiniška 5G infrastruktūros tiekėja Huawei ir jos santykis su Kinijos vyriausybe. Visi saugumizuojantys veikėjai išskyrė jog, viena vertus, Huawei 5G infrastruktūra yra kelianti grėsmę saugumui ne tik dėl šios įmonės, kaip didelės rizikos tiekėjos, reputacijos ir nesaugios tiekimo grandinės. Kita vertus, pabrėžiama Kinijos įstatyminė bazė, tariamai lemianti Huawei priklausomybę nuo Kinijos vyriausybės, dėl ko kyla rizika dėl 5G tinklų šnipinėjimo, trikdymo ar net sabotavimo.

Kalbant apie netipines priemones, buvo pabrėžtas poreikis JAV turėti mechanizmą, leidžianti įvertinti ir išskirti nepatikimus 5G infrastruktūros tiekėjus, siekiant apsaugoti naujuosius tinklus. Tiesa, apie šią netipinę priemonę nėra detaliai kalbama, nes nėra konkrečiai įvardijimas naujų institucijų ar teisinės bazės kūrimas, specialų įgaliojimų suteikimas. Tokį mechanizmą turėti yra skatinamos ir kitos valstybės. Be to, kaip netipinė priemonė buvo išskirtas tikslas JAV kartu su kitomis valstybėmis tarptautiniu lygmeniu įgyvendinti Prahos 5G saugumo konferencijos nutarimus, kurie tarnautų kaip saugumo standartai, vėlgi, apsaugantys nuo nepatikimų tiekėjų.

Visgi, dažniausiai akcentuota netipinė priemonė – Huawei 5G infrastruktūros atsisakymas ir alternatyvaus, patikimo 5G tiekėjo pasirinkimas, konkrečiai – Nokia, Ericsson ar Samsung 5G

[104] The White House, „*Readout of Vice President Mike Pence's Meeting with President Andrzej Duda of Poland*“, September 2, 2019. < https://www.whitehouse.gov/briefings-statements/readout-vice-president-mike-pences-meeting-president-andrzej-duda-poland/ > [Žiūrėta 2020-05-18]

[105] The White House, „*Remarks by President Trump and Prime Minister Modi of India in Joint Press Statement*“, February 25, 2020.

technologijų diegimas. Galima argumentuoti, jog veikėjų minimos netipinės priemones yra tiesiogiai orientuotos į būtent Huawei ir Kinijos keliamos grėsmės suvaldymą. Atsižvelgiant į globalų JAV ir Kinijos varžymąsi, 5G ryšio saugumizaciją JAV turi geopolitinį aspektą, dėl kurio yra ne tik siekiama bendrai išvengti 5G ryšio grėsmės, bet ir norima kiniškoms technologijoms neleisti įsigalėti kitose pasaulio šalyse.

3. 5G saugumizavimas JAV oficialiuose dokumentuose

Šioje dalyje yra pateikiama trijų oficialių JAV dokumentų kokybinė turinio analizė, norint išsiaiškinti, kaip 5G problematika yra saugumizuota oficialiame JAV diskurse. Šių oficialių dokumentų analizė yra pasirinkta todėl, nes dokumentas formaliai indikuoja konkrečios problemos tapimu valstybės saugumo darbotvarkės dalimi. Analizei pasirinkti šie dokumentai: 1) 2020 m. kovo mėn. pristatyta JAV Nacionalinė Strategija 5G apsaugoti (angl. *National Strategy to Secure 5G of the United States of America*); 2) 2019 m. JAV Prezidento dekretas informacinėms ir komunikacinėms technologijoms bei paslaugų tiekimo grandinei apsaugoti; 3) 2020 m. kovą įsigaliojęs 2019 m. Saugių ir Patikimų Komunikacijų Tinklų Aktas (angl. *Secure and Trusted Communications Networks Act of 2019*).

3.1 JAV Nacionalinė Strategija 5G apsaugoti

2020 m. kovo mėnesį Baltieji Rūmai pristatė Nacionalinę Strategiją 5G apsaugoti (angl. *National Strategy to Secure 5G of the United States of America*). Joje yra pabrėžiama šio naujojo kartos ryšio svarba, paminint, jog tai bus pirminis JAV klestėjimo ir saugumo XXI a. „variklis“. Technologija lems pokytį transformuodama, kaip visuomenė dirbs, mokysis, komunikuos ir gyvens. Atitinkamai yra atsižvelgiama, jog tai lems naujas rizikas ir didins pažeidžiamumą, nes 5G infrastruktūra „taps patraukliu taikiniu nusikaltėliams ir svetimšaliams priešininkams (angl. *foreign adversaries*).[106]

Strategijoje yra išskiriami keturi skirsniai, apibendrinantys JAV administracijos viziją 5G plėtros ir rizikų valdymo klausimu:

- Lengvinti 5G ryšio plėtrą valstybės viduje;

[106] The White House, „*National Strategy to Secure 5G*“, March 2020. < https://www.whitehouse.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf > [Žiūrėta 2020-05-01]

- Įvertinti rizikas ir identifikuoti esminius 5G infrastruktūros saugumo principus;
- Valdyti rizikas, kylančias JAV ekonomikai ir nacionaliniam saugumui naudojant 5G infrastruktūrą;
- Skatinti atsakingą 5G infrastruktūros vystymą ir plėtrą globaliu mastu.[107]

Grėsmių išskyrimas ir atsakas į jas yra minimi paskutiniuose trijuose skirsniuose. Prieš išskiriant jas galima konstatuoti, jog bendrąja prasme, su 5G ryšiu susijusios saugumo problemos kelia grėsmę JAV ekonomikai ir nacionaliniam saugumui.

Siekiant apsaugoti JAV ekonomiką ir nacionalinį saugumą, antrajame punkte yra atkreipiamas dėmesys į kibernetines grėsmes. Šioje vietoje kibernetines grėsmes suprantamos kaip įsilaužimas į 5G infrastruktūrą su tikslu 1) vogti informaciją dėl finansinės naudos ir 2) rinkti žvalgybinę informaciją bei sekti. Nors strategijoje minima, kad įsilaužimus galėtų vykdyti nusikaltėliai (individai ar grupuotės) ar svetimšaliai priešininkai (priešiškos valstybės), tačiau konkreti valstybė nėra įvardijama. Atitinkamai, viena vertus, JAV administracija reguliariai vertins ir charakterizuos ekonomikai, nacionaliniam saugumui kylančias rizikas dėl kibernetinių grėsmių ir pažeidžiamumų pačioje 5G infrastruktūroje. Tai bus daroma pasitelkiant tarpvyriausybinį, tarpinstitucinį ir privataus sektoriaus bendradarbiavimą. Kita vertus, JAV vyriausybė, bendradarbiaudama su privačiu sektoriumi, vystys ir plėtos 5G infrastruktūros saugumo principus – kibernetinio saugumo, tiekimo linijų saugumo, valdymo bei viešosios sveikatos geriausias praktikas.

Trečiajame punkte dėmesys skiriamas nacionaliniam saugumui ir ekonomikai kylančioms grėsmėms dėl 5G infrastuktūros tiekimo grandinės ir „didelės rizikos“ tiekėjų keliamų rizikų. Strategijoje yra pabrėžiamas numatomas siekis užtikrinti, jog „nacionalinės kritinės funkcijos[108] ir nacionalinės esminės funkcijos[109] būtų atsparios 5G grėsmėms“.[110] To įgyvendinimui, bus imamasi federalinių infrastruktūrų, įskaitant 5G, apsaugos ir tiekimo grandinės rizikų suvaldymo. JAV vyriausybė identifikuos ir vystys šių rizikų standartus, gaires ir praktikas atsakingoms institucijoms. Taip pat, šiame punkte atsižvelgiama į grėsmių prevenciją, kurias galimai keltų „didelės rizikos“ tiekėjai. JAV sukūrė teisinius rėmus, suteikiančius galimybę valdžiai uždrausti 5G infrastruktūros sandėrius, kurių tiekėjai būtų susiję priešiškomis valstybėmis ir tokiu būdu keltų riziką nacionaliniam saugumui. Verta pabrėžti,

[107] Ten pat, 1.
[108] Nacionalinės kritinės funkcijos – vyriausybės ir privataus sektoriaus veikla, kurios sutrikdymas turėtų didelį neigiamą poveikį visuomenės sveikatai ir apsaugai, nacionaliniam ekonominiam saugumui.
[109] Nacionalinės esminės funkcijos – valstybės funkcijos, kurios pasitelkiamos katastrofos atvejo metu palaikyti stabilumą šalyje.
[110] National Strategy to Secure 5G, 4.

jog prevencinės priemonės šioms dvejoms grėsmėms užkardyti yra paremtos dviem teisės aktais, kurie bus toliau aptarti darbe kaip oficialiojo diskurso JAV 5G saugumizacijoje dalis.

Galiausiai, paskutinis strategijos punktas yra orientuotas į tarptautinį 5G ryšio vystymąsi, siekiant skatinti saugią ir patikimą 5G įrangos ir paslaugų prieinamumą globalioje rinkoje. Nors ir nėra pažymima sąsaja su grėsmėmis ekonomikai ir nacionaliniu saugumu, JAV vyriausybė išskiria reikiamybę išsaugoti ir didinti JAV lyderystę bei įtaką tarptautinių standartų vystyme ir jų priėmime. Taip pat, vienu iš strategijos tikslų yra įvardijamas tarptautinių 5G saugumo principų vystymas ir įgyvendinimas, pabrėžiant dvišalę ir daugiašalę bendradarbiavimo platformas siekiant realizuoti 2019 m. gegužę Prahos 5G Saugumo Konferencijoje priimtus saugumo principus. Papildomai, šiame punkte yra išreiškiamas JAV vyriausybės siekis skatinti 5G įrangos pardavėjų įvairovę ir rinkos konkurencingumą. Tai bus daroma kartu su privačiu sektoriumi ir tarptautiniais partneriais kuriant atskaitomybės mechanizmus, technologinių komponentų skaidrumą, teisingą finansavimą bei didinti 5G technologinio vystymo konkurencija. Pažymima, jog šios priemonės taptų įrankiu, padėsiančiu apsaugoti amerikietiškas atvirumo, saugumo ir sąveikumo vertybes, bei prisidėtų prie labiau saugaus globalaus tinklo.

Apibendrinant, išanalizavus JAV Nacionalinę Strategiją 5G apsaugoti galima teigti, jog 5G ryšio saugumas yra išskiriamas kaip svarbi JAV administracijos bendros saugumo darbotvarkės dalis. Tai strategijoje grindžiama argumentu, jog 5G infrastruktūros apsaugojimas yra esminis faktorius užtikrinant JAV nacionalinį saugumą ir ekonomiką. Trijuose iš keturių strategijos punktuose yra įvardijamos su 5G susijusios grėsmės ir JAV administracijos priemonės jas suvaldyti (žr. lentelė 1). Grėsmės šaltiniu strategijoje įvardijami nusikaltėliai, kuriuos galima laikyti kaip vidinį grėsmės šaltinį, bei priešiškas valstybes kaip išorinės grėsmės šaltinį. Iš esmės, išskirtos grėsmės kyla dėl kibernetinių išpuolių ir 5G infrastruktūros pažeidžiamumo rizikos; didelės rizikos tiekėjų ir tiekimo grandinės grėsmių. Iš strategijos galima spręsti, jog JAV 5G saugumo sampratoje svarbus ir tarptautinis lygmuo. Tai pasireiškia administracijos siekiu didinti lyderystę ir įtaką standartus kuriančiose organizacijose. Taip pat, yra norima skatinti tarptautinių saugumo standartų vystymą ir įgyvendinimą (Prahos Saugumo konferencijos nutarimai), bei bendros 5G rinkos konkurencingumą ir tiekėjų įvairovę.

1 lentelė. Su 5G susijusių grėsmės ir atsakas į jas JAV Nacionalinėje Strategijoje 5G apsaugoti

Su 5G susijusios grėsmės	Atsakas į grėsmes
Kibernetinės grėsmės ir pažeidžiamumas 5G Infrastruktūroje (informacijos vagystės; žvalgybinės informacijos rinkimas ir stebėjimas)	1) Grėsmių nacionaliniam saugumui, ekonomikai ir kitoms sritims identifikavimas ir charakterizavimas 2) 5G infrastruktūros saugumo principų vystymas ir taikymas 3) Tarpvyriausybinis, tarpinstitucinis ir privataus sektoriaus bendradarbiavimas,
Tiekimo grandinės grėsmės valstybinei 5G infrastruktūrai	1) Atitinkamas teisinis pagrindas[111] 2) Federalinių Įsigijimų Saugumo Tarybos įkūrimas 3) Rizikų suvaldymo, gairių, standartų ir praktikų atitinkamoms institucijoms vystymas.
„Didelės rizikos“ 5G infrastruktūros tiekėjų keliamos grėsmės	1) Teisinis pagrindas, leidžiantis uždrausti sandorius su tiekėjais, turinčiais sąsajų su priešiška valstybe ir dėl to keliančiais grėsmę nacionaliniam saugumui.[112]
Globalios 5G rinkos nekonkurencingumas, infrastruktūros tiekėjų neįvairovė	1) Bendradarbiavimas su tarptautiniais partneriais ir privačiu sektoriumi siekiant sąžiningo finansavimo, komponentų skaidrumo, konkurencingumo technologijų vystyme ir kt.

Šaltinis: sudaryta autoriaus, remiantis JAV Nacionaline Strategija 5G apsaugoti

3.2 JAV Prezidento dekretas informacinėms ir komunikacinėms technologijoms bei paslaugų tiekimo grandinei apsaugoti

2019 m. gegužės 15 d. JAV prezidentas D. Trump pasirašė dekretą, skirtą apsaugoti informacinės ir komunikacinių technologijas bei paslaugų tiekimo grandinę (angl. *Executive Order on Securing the Information and Communications Technology and Services Supply Chain*).[113] Šio dekreto turinio kokybinė analizė yra pasirinkta dėl kelių priežasčių. Visų pirma, tai yra oficialus dokumentas, į kurį referuojama prieš tai nagrinėtoje JAV 5G saugumo strategijoje. Antra, šiame dekrete ne tik yra nurodomos dėl 5G kylančios grėsmės ir šaltiniai, bet pats dokumentas suteikia teisinį pagrindą netipinei

[111] U.S. Congress, „Federal Acquisition Supply Chain Security Act of 2018“, 2018. < https://www.congress.gov/bill/115th-congress/senate-bill/3085/text > [Žiūrėta 2020-05-02]
[112] The White House, „Executive Order on Securing the Information and Communications Technology and Services Supply Chain“, 2019. < https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/ > [Žiūrėta 2020-05-02]
[113] The White House, „Executive Order on Securing the Information and Communications Technology and Services Supply Chain“, 2019.

priemonei, suteikianti teisinį pagrindą atsakui į saugumo problemą. Svarbu paminėti, jog nors dekrete nėra tiesiogiai minimas 5G ryšys, jį suprasti reikia „informacijos ir komunikacijų technologijų ir paslaugų“[114] sąvokos rėmuose, yra paaiškinta kaip programinė, techninė įranga ar kiti produktai, skirta įvairioms informacijos ir duomenų funkcijoms bei komunikacijai.

Grėsmė ir grėsmės šaltinis. Lyginant su 5G saugumo strategija, dekrete yra nurodomas ir kelis kartus paminimas vienas išorinis grėsmės šaltinis – priešiškos valstybės. Remiantis grėsmės šaltiniu, yra atkreipiamas dėmesys iš išskiriamos dvi grėsmės. Pirmoji grėsmė yra ta, jog priešiškos valstybės „vis labiau kuria ir išnaudoja pažeidžiamumus informacinėse ir komunikacinėse technologijose bei paslaugose“.[115] Tai pasireiškia kenksmingais kibernetiniais veiksmais (kibernetiniais išpuoliais), ekonominiu bei pramoniniu šnipinėjimu. Antra ir esminė šiame dokumente formuluojama grėsmė yra JAV informacinių ir komunikacinių technologinių infrastruktūros įsigijimas iš asmenų ar įmonių, susijusių su priešiškomis valstybėmis.[116] Ši problema 5G saugumo strategijoje yra išskirta kaip „didelės rizikos“ tiekėjų grėsmė.

Referentinis objektas. Atsižvelgiant į paminėtas grėsmes, dekrete yra išskiriama, *kam* jos kelia grėsmę: „[...] tokiu būdu sudarydamos neįprastą ir netipinę grėsmę JAV nacionaliniam saugumui, užsienio politikai ir ekonomikai.“[117] Taip pat atkreipiamas dėmesys, jog informacinės ir komunikacinės technologijos bei paslaugos yra svarbios kritinei infrastruktūrai ir skaitmeninei ekonomikai. Todėl žalinga kibernetinė veikla ir jau minėtas ekonominis ir pramoninis šnipinėjimas kelia grėsmę ne tik pačiai JAV, bet ir jos piliečiams.

Dekretą galima vertinti kaip netipinę priemonę įgalinantį teisės aktą, suteikiančią pagrindą užtikrinti 5G saugą nuo „didelės rizikos“ veikėjų. Taip pat, tai yra oficialaus/teisinio diskurso pavyzdys, žymintis 5G saugumizavimą JAV, išskiriant infrastruktūros tiekimo grandinės saugumo problemas. Iš esmės, šiuo dekretu yra paskelbiama nepaprastoji padėtis, įgalinanti vyriausybę blokuoti technologijų įsigijimus, turinčius sąsajų su priešiškomis valstybėmis.[118] Tokiu būdu JAV vyriausybė nori užtikrinti, jog 5G ir būsimų ryšio kartų infrastruktūra būtų įdiegta apsaugant nacionalinio saugumo interesus.

Šis prezidento dekretas yra suformuluotas taip, jog „didelės rizikos“ infrastruktūros pardavėjų rizika būtų sukontroliuota pasitelkus įvairių vyriausybės sričių bendradarbiavimą.[119] Tokiu būdu, JAV Prekybos departamentui yra numatytos ypatingos galios, nes jo sekretorius, konsultuodamasis su kitų

[114] Ten pat.
[115] Ten pat.
[116] Ten pat.
[117] Ten pat.
[118] Ten pat.
[119] National Strategy to Secure 5G, 4.

dekrete numatytų institucijų (pvz., valstybės ar gynybos departamentų) atstovais, gali drausti JAV kompanijoms įsigyti ir naudoti į juodąjį sąrašą įtrauktų įmonių telekomunikacinę įrangą. Draudimas grindžiamas įvertinus, jog sandėris galėtų sukelti „katastrofiškų efektų riziką JAV kritinės infrastruktūros bei skaitmeninės ekonomikos saugumui ar atsparumui“ ar keltų „nepriimtiną riziką JAV nacionaliniam saugumui arba JAV piliečių saugumui“.[120]

Papildomai, dekretu Nacionalinį žvalgybos direktoriaus biuras (angl. *Office of the Director of National Intelligence*) yra įpareigojamas reguliariai vertinti telekomunikacijų technologijų keliamų grėsmių analizę JAV ir piliečiams.[121] Analizėje, kaip pabrėžiama, turėtų būti įvertintos pavojingos technologijos grėsmės JAV vyriausybei, kritinei infrastruktūrai bei kitiems subjektams. Taip pat, Nacionaliniam saugumo departamentui yra nurodoma kasmet teikti įmonių, technologijų programų sistemų, įrangos ir paslaugų grėsmių JAV nacionaliniam saugumui metinį vertinimą.

Kita vertus, dekretą galima vertinti geopolitiškai, atsižvelgiant į JAV-Kinijos konkurenciją. Jau kitą dieną po dekreto paskelbimo, tai yra, 2019 m. gegužės mėnesio 16 dieną, didžiausią pasaulyje kinišką telekomunikacijų įrangos gamintoja Huawei ir 68 bendrovės filialai įvairiose pasaulio valstybėse buvo įtraukti į draudžiamųjų įmonių sąrašą.[122] Papildomai, 2019 m. rugpjūčio 19 dieną, į sąrašą buvo įtrauktos dar 46 Huawei dukterinės įmonės.[123] Sprendimas įtraukti Huawei ir su ja susijusias įmones yra grindžiamas tuo, jog Huawei ir įmonės yra įsitraukusios į veiklas, keliančias grėsmę JAV nacionaliniam saugumui, bei priešingas užsienio politikos interesams. Konkrečiai, Huawei yra kaltinama teikiant nesankcionuotas finansines paslaugas Iranui, taip pat neteisėtu intelektinės nuosavybės, prekybos ir technologinių paslapčių pasisavinimu JAV. Galima argumentuoti, jog nors teoriškai į draudžiamųjų įmonių, susijusių su JAV priešiškomis valstybės, sąrašą gali būti įtraukta bet kuri kita įmonė, ši netipinė priemonė buvo sukurta orientuojantis konkrečiai į politikų pabrėžtą Kinijos ir Huawei šnipinėjimo grėsmę 5G JAV infrastruktūrai.

Apibendrinant, dekretas atspindi saugumizuotą problemą oficialiajame/teisiniame JAV diskurse. Jame yra išreiškiamas vyriausybės poreikis apsaugoti JAV nacionalinį saugumą, ekonomiką ir užsienio

---

[120] Ten pat.

[121] Bendrame pasauliniame grėsmių JAV įvertinime, pabrėžiama, jog JAV naudojama užsienyje sukurta 5G infrastruktūra kelia užsienio valstybių įsilaužimo ir veiklos trikdymo grėsmę. Plačiau žr. Daniel R. Coats, „*Worldwide Threat Assessment of the US Intelligence Community*“, 2019, 16. < https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf > [Žiūrėta 2020-05-04]

[122] Bureau of Industry and Security, „*Addition of Entities to the Entity List*“, 2019. < https://www.federalregister.gov/documents/2019/05/21/2019-10616/addition-of-entities-to-the-entity-list > [Žiūrėta 2020-05-04]

[123] Bureau of Industry and Security, „*Addition of Certain Entities to the Entity List and Revision of Entries on the Entity List*“, 2019 < https://www.federalregister.gov/documents/2019/08/21/2019-17921/addition-of-certain-entities-to-the-entity-list-and-revision-of-entries-on-the-entity-list > [Žiūrėta 2020-05-04]

politiką draudžiant grėsmę keliančius 5G infrastruktūros tiekėjus. Šiuo požiūriu, grėsmė atsirastų tada, jei kritinė infrastruktūra būtų įsigyjama iš „didelės rizikos“ tiekėjo, kuris būtų susijęs su priešiška JAV valstybe. Taigi, pirmoji dekrete išskirta netipinė priemonė yra „didelės rizikos“ tiekėjų draudimas, įgalinant Prekybos departamentą apspręsti, kurie tiekėjai keltų grėsmę JAV nacionaliniam saugumui. Praktikoje tai pasireiškia kiniškos Huawei įtraukimu į juodąjį sąrašą ir faktiniu uždraudimu jai tiekti 5G infrastruktūros komponentus JAV. Antroji netipinė priemonė – nurodymai dvejoms už saugumą atsakingoms vyriausybinėms institucijoms kasmet tirti ir įvertinti 5G infrastruktūros keliamas grėsmes JAV ir jos piliečiams, bei pačios 5G infrastruktūros komponentus – programines sistemas ir įrangos pažeidžiamumus.

3.3 2019 m. Saugių ir Patikimų Komunikacijų Tinklų Aktas

Saugių ir Patikimų Komunikacijų Tinklų Aktas (angl. *Secure and Trusted Communications Networks Act of 2019*), pirmąkart pristatytas JAV Kongrese 2019 m., įgavo teisinę galią 2020 m. kovo 12 d. jį pasirašius JAV prezidentui. Šio dokumento analizė yra svarbi dėl kelių priežasčių. Visų pirma, įstatymas reprezentuoja ne tik 5G ryšio saugumizaciją JAV oficialiajame diskurse, bet ir suteikia teisinį pagrindą kelių netipinių priemonių įgyvendinimui. Antra, šis įstatymas rodo JAV įstatymų leidžiamųjų institucijų formalią paramą imtis priemonių apsaugant 5G tinklus.

Iš esmės, įstatymu yra įgalinamos trys priemonės 5G ryšiams JAV apsaugoti:[124]

- Federalinei Komunikacijų Komisijai (angl. *Federal Communications Commissions*) yra uždraudžiama skirti Federalines subsidijas nepatikimų 5G tiekėjų telekomunikacinės įrangos įsigijimui ar priežiūrai. Tokiu būdu yra sukuriamas mechanizmas, apsaugantis JAV nacionalinį saugumą nuo nesaugios 5G infrastruktūros.
- Įteisinama kompensavimo programa, skirta atlyginti telekomunikacinių paslaugų tiekėjams, kurie privalės pašalinti nepatikimų ir JAV nacionaliniam saugumui riziką keliančių pardavėjų telekomunikacijų infrastruktūrą ir pakeisti į patikimą.

[124] U.S. Congress, *„Secure and Trusted Communications Networks Act of 2019“*, March 12, 2020. < https://www.congress.gov/bill/116th-congress/house-bill/4998 > [Žiūrėta 2020-05-18]

- Įpareigojama įkurti programą telekomunikacinių paslaugų tiekėjams, kuria būtų dalinamasi informacija apie potencialias. 5G tinklų saugumo ir pažeidžiamumo bei tiekimo grandinės rizikomis.

Taigi, šiuo įstatymu siekiama užtikrinti JAV 5G tinklų saugumą nuo grėsmę keliančių tiekėjų ir esamą tų nesaugių tiekėjų infrastruktūrą pakeisti į naująją. Svarbu atkreipti dėmesį, jog įstatymo tekste nėra tiesiogiai įvardijami nesaugūs tiekėjai, keliantys riziką nacionaliniam saugumui. Visgi, Senatoriaus R. Wicker spaudos pranešime yra akcentuojama, jog šiuo įstatymu yra siekiama apsaugoti JAV komunikacijų tinklus nuo „grėsmės, kylančios iš užsienio tiekėjų, tokių kaip Huawei ir ZTE.“[125] JAV prezidento spaudos pranešime yra nurodoma, kad naujuoju aktu yra užtikrinamas JAV komunikacinių tinklų saugumas nuo priešiškų valstybių.[126] Taip pat, šioje vietoje yra svarbu prisiminti, jog JAV prezidento dekretu buvo suteiktas teisinis pagrindas į juodąjį sąrašą įtraukti valstybės nacionaliniam saugumui ar užsienio politikos interesams grėsmę keliančias įmones. Tik Huawei, viena iš nedaugelio 5G infrastruktūros komponentų tiekėjų, atsirado šiame sąraše. Taigi, atsižvelgiant į politikų pasisakymus ir esamus faktus, galima išvada, jog Saugių ir Patikimų Komunikacijų Tinklų Aktas yra tiesiogiai susijęs su Kinijos ir kiniškų 5G infrastruktūros tiekėjų keliama grėsme JAV.

Papildomai, šis teisės aktas indikuoja, jog JAV vyriausybė turėjo formalų institucijų pritarimą dėl egzistuojančių 5G grėsmių saugumui bei paramą imtis priemonių 5G ryšiui apsaugoti. Taip galima teigti atsižvelgiant į tai, kad prie Saugių ir Patikimų Komunikacijų Tinklų Akto kūrimo prisidėjo tiek demokratų, tiek respublikonų partijų nariai, o pats teisės aktas buvo priimtas ir Kongrese, ir Senate. Taip pat, kalbant apie auditorijos palaikymą 5G problematikos saugumizavime JAV, galima paminėti „Public Opinion Strategies“ 2020 m. atliktą apklausą.[127] Apklausos rezultatai rodo, jog iš 1200 apklaustųjų, 74% amerikiečių mano, jog Huawei turėtų būti pašalintas iš JAV, o 84% sutiko su teiginiu, jog JAV yra svarbu laimėti 5G diegimo varžybas prieš Kiniją. Atsižvelgiant į tai, jog siekiant apsaugoti 5G tinklų saugumą JAV vyriausybė ėmėsi priemonių, lėmusių kiniškų tiekėjų draudimą ir pašalinimą iš 5G diegimo,

[125] U.S. Senate, *„Wicker Statement on Senate Passage of Secure and Trusted Communications Networks Act“*, February 27, 2020. < https://www.commerce.senate.gov/2020/2/wicker-statement-on-senate-passage-of-secure-and-trusted-communications-networks-act >

[126] The White House, *„President Donald J. Trump Is Committed To Safeguarding America's Vital Communications Networks And Securing 5G Technology“,* March 12, 2020. < https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-committed-safeguarding-americas-vital-communications-networks-securing-5g-technology/ > [Žiūrėta 2020-05-18]

[127] 5G Action Now, „*New Poll Shows 84% Of Americans Believe Winning The 5g Race Against China Is Crucial*“, January 23, 2020. < https://5gactionnow.com/new-poll-012320/ > [Žiūrėta 2020-05-19]

minėtoji apklausa parodo visuomenės moralų pritarimą priemonių legitimizavimui bei taikymui praktikoje.

4. Išvados

Šiame darbe buvo siekiama išsiaiškinti, kaip ir kodėl JAV judrusis penktosios kartos (5G) ryšys ir jo diegimas tapo valstybės saugumo politikos dalimi. Siekiant rasti atsakymus į šį galvosūkį, buvo remiamasi Kopenhagos mokyklos suformuluotuotu saugumizacijos teoriniu modeliu. Atsižvelgiant į teorinį aiškinimą, saugumizacija - dviejų pakopų procesas, kuomet kalbos aktų vartojimu konkreti problema intersubjektyviai yra transformuojama į saugumo problemą, kuriai pašalinti yra pateisinamas ypatingų, netipinių priemonių panaudojimas.

Pasirinktų penkių JAV aukšto politinio rango pareigūnų 32 kalbos aktų analizė parodo, jog 5G problematika viešojoje erdvėje buvo konstruojama kaip ypatinga grėsmė tokiems referentiniams objektams kaip, pavyzdžiui, nacionalinis saugumas, ekonomika ar kritinė infrastruktūra. Šios grėsmės iš esmės atsispindi ir išanalizavimus tris JAV oficialius dokumentus. Šių dokumentų analizė žymi teisinį pagrindą 5G grėsmėms panaikinti skirtas priemones, apie kurias buvo kalbama viešojoje erdvėje, tiesa, ne apie visas. Todėl **pirmoji išvada** - JAV yra įvykęs 5G ryšys yra saugumizuotas, kuris žymi, jog saugumizuojančių veikėjų pasisakymai iššaukė politinius sprendimus, perkėlusius 5G į nacionalinę saugumo darbotvarkę bei nebuvo tiesiog deklaratyvūs.

Antroji išvada yra ta, jog 5G ryšio saugumizavimas yra susijęs su kiniška 5G infrastruktūros įrangos gamintojos Huawei ir Kinijos veiksniu. Viešojoje erdvėje Huawei ir tariamai šios įmonės priklausomumas nuo Kinijos vyriausybės yra dažniausiai akcentuojamas grėsmės šaltinis. Atitinkamai, nors ir oficialių dokumentų diskurse Huawei bei Kinija nėra įvardijamos, tačiau įgalintomis netipinėmis priemonėmis yra faktiškai uždraudžiama ir apsisaugoma iš esmės nuo kiniško 5G diegimo JAV. Taigi galima teigti, jog saugumizuojant 5G tinklus JAV, yra siekiama apsisaugoti nuo grėsmių, kurios kiltų įdiegus kiniškas 5G technologijas. Kinijos veiksnys JAV 5G saugumizavime tuo pačiu metu išryškina geopolitinį aspektą. Turint omenyje strateginę Kinijos bei JAV konkurenciją, įskaitant technologijų erdvę, galima teigti, jog JAV saugumizuoja 5G ne tik dėl saugumo sumetimų, bet siekdama ekonomiškai slopinti kiniškų telekomunikacinės įrangos gamintojų uždraudžiant jas JAV bei skatinant kitas valstybes rinktis alternatyvias tiekėjas.

Trečioji išvada - JAV 5G tinklų saugumas yra suprantamas ne tik nacionaliniu, tačiau ir tarptautiniu lygmeniu. Nesaugūs 5G tinklai keltų grėsmę JAV užsienio politikai ir kariniam bendradarbiavimui su sąjungininkais. Tai yra pastebima tiek saugumizuojančių veikėjų pasisakymuose, tiek oficialiuosiuose dokumentuose. Galima teigti, jog šis požiūris lemia JAV užsienio politikos aspektą – siekį įtikinti valstybes priimti 5G tiekėjų saugumo vertinimo mechanizmą, tarptautinius 5G saugumo standartus, konkrečiai – Prahos 5G saugumo konferencijos nutarimus, bei rinktis alternatyvą kiniškai Huawei 5G technologijai. Taip pat, bendradarbiauti su privačiu sektoriumi skatinant globalios 5G tiekėjų rinkos konkurencingumą

Literatūros sąrašas

1. Buzan, Barry ir Ole Weaver, *Regions and powers: the structure of international security*. Cambridge University Press, 2003.
2. Buzan, Barry, Ole Waever, and Jaap de Wilde, *Security: A New Framework for Analysis*, Boulder: Lynne Rienner Publishers, 1998.
3. Collins, Alan *Contemporary security studies*, 4 leid., Oxford University Press: 2007.
4. Emmers, Ralf, „Securitization.“ Kn. Alan Collins (sud.), *Contemporary Security Studies*. Oxford University Press, 2013.
5. Fierke, Karin M., *Critical approaches to international security*. 2 leid., John Wiley & Sons: 2015.
6. Stritzel, Holger, *Security in Translation: Securitization Theory and the Localization of Threat*, Basingstoke: Palgrave Macmillan, 2017.
7. Vitkus, Gediminas, *Realistinė tarptautinių santykių teorija ir Barry Buzano nedalomo saugumo koncepcija*. Kn. Barry Buzan, Žmonės valstybės ir baimė. Vilnius: EUGRIMAS, 1997.
8. Weaver, Ole „Securitization and Desecuritization“, Kn. Ronnie D. Lipschutz (sud.) *On Security*, New York: Columbia University Press, 1995.
9. Weaver, Ole, „The EU as a security actor: reflections from a pessimistic constructivist on postsovereign security orders.” Kn. Morten Kelstrup (sud.) *International Relations Theory and the Politics of European Integration: Power, Security and Community.* Routledge, 2000.

Straipsniai internetiniuose žurnaluose

1. 5G Action Now, „New Poll Shows 84% Of Americans Believe Winning The 5g Race Against China Is Crucial“, January 23, 2020. < https://5gactionnow.com/new-poll-012320/ > [Žiūrėta 2020-05-19]
2. Baldwin, David A., „The concept of security.“ *Review of International Studies*, 23(1), 1997. < http://www.princeton.edu/~dbaldwin/selected%20articles/Baldwin%20%281997%29%20The%20Concept%20of%20Security.pdf > [Žiūrėta 2020-04-02]
3. Balzacq, Thierry, „The Three Faces of Securitization: Political Agency, Audience and Context.“ *European Journal of International Relations*, 11 (2), 2005. < https://journals.sagepub.com/doi/10.1177/1354066105052960 > [Žiūrėta 2020-04-05]
4. Buzan, Barry ir Ole Wæver, „Macrosecuritisation and Security Constellations: Reconsidering Scale in Securitization Theory.“ *Review of International Studies*,35(2), 2009. < https://www.cambridge.org/core/journals/review-of-international-studies/article/macrosecuritisation-and-security-constellations-reconsidering-scale-in-securitisation-theory/B693D7C852112FA05E1999A5B9A0604A > [Žiūrėta 2020-04-07]
5. Campion, S. Andrew „From CNOOC to Huawei: securitization, the China threat, and critical infrastructure.“ *Asian Journal of Political Science*, 28(1), 2020. < https://www.tandfonline.com/doi/full/10.1080/02185377.2020.1741416 > [Žiūrėta 2020-03-28]
6. Floyd, Rita „Extraordinary or ordinary emergency measures: What, and who, defines the ‘success’ of securitization?“ *Cambridge review of international affairs*, 29(2), 2016. < https://www.tandfonline.com/doi/pdf/10.1080/09557571.2015.1077651 > [Žiūrėta 2020-04-08]
7. Hansen, Lene ir Helen Nissenbaum, „ Digital Disaster, Cyber Security, and the Copenhagen School.“ *International Studies Quarterly*, 53, 2009. < https://academic.oup.com/isq/article-abstract/53/4/1155/1815351 > [Žiūrėta 2020-03-28]
8. Hjalmarsson, Ola „The Securitization of Cyberspace: How the Web Was Won.“ Lund University, 2013. < http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=3357990&fileOId=3357996 > [Žiūrėta 2020-03-29].

9. Hough, Peter „Who's Securing Whom? The Need for International Relations to Embrace Human Security." *St Antony's International Review*, 1(2), 2005, 72. < www.jstor.org/stable/26227012 > [Žiūrėta 2020-04-02]
10. Inkster, Nigel, „The Huawei Affair and China's Technology Ambitions." *Survival, Global Politics and Strategy*, 61, 2019. < https://www.tandfonline.com/doi/full/10.1080/00396338.2019.1568041?scroll=top&needAccess=true > [Žiūrėta 2020-03-05]
11. Jakniūnaitė, Dovilė, „Kritinės saugumo studijos XXI amžiuje: kur kreipti Lietuvos saugumo politikos tyrimus?." *Lietuvos metinė strateginė apžvalga,* 12, 2014. <https://www.academia.edu/8238241/Kritinės_saugumo_studijos_XXI_amžiuje_kur_kreipti_Lietuvos_saugumo_politikos_tyrimus > [Žiūrėta 2020-04-04]
12. Karpavičiūtė, Ieva, „Securitization and Lithuania's national security change." *Lithuanian Foreign Policy Review*, 36(1), 2017. <https://content.sciendo.com/view/journals/lfpr/36/1/article-p9.xml?lang=en > [Žiūrėta 2020-04-05]
13. Mori, Satoru, „US Technological Competition with China: The Military, Industrial and Digital Network Dimensions." *Asia-Pacific Review*, 26(1), 2019. < https://www.tandfonline.com/doi/full/10.1080/13439006.2019.1622871 > [Žiūrėta 2020-03-28]
14. Salter, Mark B., „Securitization and Desecuritization: A Dramaturgical Analysis of the Canadian Air Transport Security Authority". *Journal of International Relations and Development*, 11(4), 2008. < https://link.springer.com/article/10.1057/jird.2008.20 > [Žiūrėta 2020-04-06]
15. Schwarz, J. Kevin, „The Securitization of Cyberspace through Technification." Virginia Polytechnic Institute and State University: 2016. < https://vtechworks.lib.vt.edu/bitstream/handle/10919/71758/Schwarz_KJ_T_2016.pdf?sequence=1&isAllowed=y > [Žiūrėta 2020-03-29]
16. Shifrinson, Joshua „The rise of China, balance of power theory and US national security: Reasons for optimism?" *Journal of Strategic Studies*, 43(2), 2020. < https://www.tandfonline.com/doi/full/10.1080/01402390.2018.1558056?journalCode=fjss20 > [Žiūrėta 2020-03-28]

Internetiniai Šaltiniai

1. Bureau of Industry and Security, „Addition of Certain Entities to the Entity List and Revision of Entries on the Entity List", 2019 < https://www.federalregister.gov/documents/2019/08/21/2019-17921/addition-of-certain-entities-to-the-entity-list-and-revision-of-entries-on-the-entity-list > [Žiūrėta 2020-05-04]
2. Bureau of Industry and Security, „Addition of Entities to the Entity List", 2019. < https://www.federalregister.gov/documents/2019/05/21/2019-10616/addition-of-entities-to-the-entity-list > [Žiūrėta 2020-05-04]
3. Coats, Daniel R. „Worldwide Threat Assessment of the US Intelligence Community", 2019, 16. < https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf > [Žiūrėta 2020-05-04]
4. Danny, Paez, „Why the US must beat China in the race to 5G internet." Inverse, August 21, 2018. " < https://www.inverse.com/article/48228-why-china-is-winning-the-race-with-the-us-to-5g-internet > [Žiūrėta 2020 03 25]
5. Duchâtel, Mathieu ir Godement, François, "Europe and 5G: the Huawei Case", Institute Montaigne, 2019. < https://www.institutmontaigne.org/en/publications/europe-and-5g-huawei-case-part-2 > [Žiūrėta 2020-03-25]

6. ENISA, „Threat Landscape For 5G Networks.” 2019 < https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks/at_download/fullReport > [Žiūrėta 2020-03-25]
7. Eurasia Group, „The Geopolitics of 5G.“ November 2018. < https://www.eurasiagroup.net/siteFiles/Media/files/181114%205G%20special%20report%20public.pdf > [Žiūrėta 2020-03-25]
8. Europos Komisija, „Secure 5G networks: Quesions and Answers on the EU toolbox.“ 29 January, 2020 < https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_127 > [Žiūrėta 2020-03-25]
9. Finel, I. Bernard „New thinking about security: Analytical pitfalls and applications to the Americas.” Vašingtonas, 1999. < https://www.oas.org/csh/docs/Foro%20sobre%20seguridad.pdf > [Žiūrėta 2020-04-01]
10. Gartner, „Wireless Infrastructure Revenue Forecast, Worldwide, 2018-2021.“ 2019. < https://www.gartner.com/en/newsroom/press-releases/2019-08-22-gartner-forecasts-worldwide-5g-network-infrastructure > [Žiūrėta 2020 03 35]
11. GSMA Intelligence, „Forecast 5G Penetration in 2025.“ 2020. https://fingfx.thomsonreuters.com/gfx/mkt/12/8296/8227/GSMA%20Intelligence%205G%20Penetration.png > [Žiūrėta 2020 03 25]
12. GSMA, „Mobile Internet Connectivity Global Factsheet“, 2019. <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/07/Mobile-Internet-Connectivity-Global-Factsheet.pdf > [Žiūrėta 2020 03 25]
13. Hoffman, Stacie, Samantha Bradshaw ir Emily Taylor, „Networks and Geopolitics: How great power rivalries infected 5G.” Oxford Information Labs, 2019. < https://oxil.uk/publications/geopolitics-of-5g/Geopolitics_5G_Final.pdf > [Žiūrėta 2020-03-25]
14. Kelion, Leo, „Huawei set for limited role in UK 5G networks.“ January 28, 2020, < https://www.bbc.com/news/technology-51283059 > [Žiūrėta 2020 03 25]
15. Kleinhas, Jan-Peter, „5G vs. National Security – A European Perspective.“ 2019. < https://www.stiftung-nv.de/sites/default/files/5g_vs._national_security.pdf > [Žiūrėta 2020-03-25]
16. Klingova, Katerina, „Securitization of Cyber Space in the United States of America, the Russian Federation and Estonia.” Central European University Department of Political Science, 2013. < https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjHtsiprMzpAhUNJZoKHagiBQAQFjAAegQIARAB&url=http%3A%2F%2Fwww.etd.ceu.hu%2F2013%2Fklingova_katarina.pdf&usg=AOvVaw3SX4lzwm5qd1cmqNCDRlVK >
17. Lee, Edison „Telecom Services. The Geopolitics of 5G and IoT.” Jefferies Franchise Note, September 2017, 39-41. < https://www.jefferies.com/CMSFiles/Jefferies.com/files/Insights/TelecomServ.pdf > [Žiūrėta 2020-03-25]
18. Lin, Leo S. F., „State-centric Security and its Limitations: The case of transnational organized crime.“ Research Institute for European and American Studies, 2011, 13. < https://rieas.gr/images/rieas156.pdf > [Žiūrėta 2020-04-02]
19. NIS Cooperation Group, „EU coordinated risk assessment of the cybersecurity of 5G networks.” 2019. < https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132 > [Žiūrėta 2020-03-25]
20. Roe, Paul, „Actor, Audience(s) and Emergency Measures: Securitization and the UK's Decision to Invade Iraq.“ Peace Research Institute Oslo, 2008. < https://journals.sagepub.com/doi/10.1177/0967010608098212 > [Žiūrėta 2020-04-06]

21. Secretary Mike Pompeo's [@SecPompeo] Tweet, February 27, 2019. < https://twitter.com/SecPompeo/status/1100600759383670785 > [Žiūrėta 2020-05-18]
22. Statista, „Global revenue from telecommunications services from 2005 to 2019.“ 2020. <https://www.statista.com/statistics/268628/worldwide-revenue-from-telecommunications-services-since-2005/> [Žiūrėta 2020 03 25]
23. Xuewu Gu, Christiane Heidbrink, Ying Huang, Philip Nock, Hendrik W. Ohnesorge, Andrej Pustovitovskij, „Geopolitics and the Global Race for 5G.“ CGS Global Focus, 2019. < http://cgs-bonn.de/5G-Study-2019.pdf > [Žiūrėta 2020-03-25]

Publicistiniai šaltiniai:

1. The White House, „*Remarks by President Trump on United States 5G Deployment*“, 2019. < https://www.whitehouse.gov/briefings-statements/remarks-president-trump-united-states-5g-deployment/ > [Žiūrėta 2020-05-10]
10. The White House, „*Remarks by President Trump and Prime Minister Trudeau of Canada Before Bilateral Meeting*“, December 3, 2019. < https://www.whitehouse.gov/briefings-statements/remarks-president-trump-prime-minister-trudeau-canada-bilateral-meeting-london-united-kingdom/ > [Žiūrėta 2020-05-18]
11. U.S. Department of State, „*Remarks to the Future Farmers of America*“, March 4, 2019. < https://www.state.gov/remarks-to-the-future-farmers-of-america/ > [Žiūrėta 2020-05-18]
12. U.S. Department of State, *„Press Briefing with Deputy Assistant Secretary Robert Strayer“*, October 15, 2019. < https://www.state.gov/telephonic-press-briefing-with-deputy-assistant-secretary-robert-strayer-cyber-and-international-affairs-and-information-policy-bureau-of-economic-and-business-affairs/ > [Žiūrėta 2020-05-18]
13. U.S. Department of State, *„Press Briefing with Deputy Assistant Secretary Robert Strayer, Cyber and International Affairs and Information Policy, Bureau of Economic and Business Affairs“*, May 8, 2019. < https://www.state.gov/press-briefing-with-deputy-assistant-secretary-robert-strayer-cyber-and-international-affairs-and-information-policy-bureau-of-economic-and-business-affairs-2/ > [Žiūrėta 2020-05-18]
14. U.S. Department of State, *„Press Briefing with Deputy Assistant Secretary Robert Strayer*“, July 11, 2019. < https://www.state.gov/press-briefing-with-deputy-assistant-secretary-robert-strayer/ > [Žiūrėta 2020-05-18]
15. U.S. Embassy in Luxembourg, „*Secretary Pompeo and Secretary Esper Speak at Munich Security Conference 2020*“, February 19, 2020. < https://lu.usembassy.gov/secretary-pompeo-and-secretary-esper-speak-at-munich-security-conference-2020/ > [Žiūrėta 2020-05-18]
16. U.S. Department of Defense, „*As Prepared Remarks by Secretary of Defense Mark T. Esper at the Munich Security Conference*“, February 15, 2020. < https://www.defense.gov/Newsroom/Speeches/Speech/Article/2085577/as-prepared-remarks-by-secretary-of-defense-mark-t-esper-at-the-munich-security/ > [Žiūrėta 2020-05-18]
17. U.S. Department of State, „*Remarks at Press Availability”,* February 26, 2019. < https://www.state.gov/remarks-at-press-availability/ > [Žiūrėta 2020-05-18]
18. The White House, *„Remarks by President Trump and President Niinistö of the Republic of Finland in Joint Press Conference”*, October 2, 2019. < https://www.whitehouse.gov/briefings-statements/remarks-president-trump-president-niinisto-republic-finland-joint-press-conference/ >
19. Cybersec Forum, „*Robert Strayer, Deputy Assistant Secretary of State, U.S. Department of State*“, January 9, 2020. 1:25-1:42. < https://www.youtube.com/watch?v=nnmTlHwPGVg > [Žiūrėta 2020-05-18]

2. U.S. Department of State, „*Remarks at the 2019 Internet Governance Forum USA Conference*“, July, 2019. < https://www.state.gov/remarks-at-the-2019-internet-governance-forum-usa-conference/ > [Žiūrėta 2020-05-18]
20. The White House, „*Remarks by Vice President Pence and Taoiseach Varadkar of Ireland in Joint Press Statement*, September 3, 2019. < https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-taoiseach-varadkar-ireland-joint-press-statement-dublin-ireland > [Žiūrėta 2020-05-18]
21. U.S. Department of State, „*Press Briefing with Deputy Assistant Secretary Robert Strayer Cyber and International Affairs and Information Policy Bureau of Economic and Business Affairs*“, April 10, 2019. < https://www.state.gov/press-briefing-with-deputy-assistant-secretary-robert-strayer-cyber-and-international-affairs-and-information-policy-bureau-of-economic-and-business-affairs/ > [Žiūrėta 2020-05-08]
22. The White House, „*Readout of Vice President Mike Pence's Meeting with President Andrzej Duda of Poland*“, September 2, 2019. < https://www.whitehouse.gov/briefings-statements/readout-vice-president-mike-pences-meeting-president-andrzej-duda-poland/ > [Žiūrėta 2020-05-18]
23. U.S. Senate, „Wicker Statement on Senate Passage of Secure and Trusted Communications Networks Act“, February 27, 2020. < https://www.commerce.senate.gov/2020/2/wicker-statement-on-senate-passage-of-secure-and-trusted-communications-networks-act >
24. The White House, „President Donald J. Trump Is Committed To Safeguarding America's Vital Communications Networks And Securing 5G Technology“, March 12, 2020. < https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-committed-safeguarding-americas-vital-communications-networks-securing-5g-technology/ > [Žiūrėta 2020-05-18]
3.U.S. Department of State, „*Press Briefing with Deputy Assistant Secretary Robert Strayer, Cyber and International Affairs and Information Policy, Bureau of Economic and Business Affairs*“, May 8, 2019. < https://www.state.gov/press-briefing-with-deputy-assistant-secretary-robert-strayer-cyber-and-international-affairs-and-information-policy-bureau-of-economic-and-business-affairs-2/ > [Žiūrėta 2020-05-18]
4. U.S. Department of State, „United States Welcomes the EU's Acknowledgement of the Unacceptable Risks Posed by Untrusted 5G Suppliers“, January 30, 2020. < https://www.state.gov/united-states-welcomes-the-eus-acknowledgement-of-the-unacceptable-risks-posed-by-untrusted-5g-suppliers/ > [Žiūrėta 2020-05-18]
5. The White House, „Raising the Bar to Protect Federal Government and Private-Sector Data“, July 25, 2019. < https://www.whitehouse.gov/articles/raising-bar-protect-federal-government-private-sector-data/ > [Žiūrėta 2020-05-18]
6. Council on Foreign Relations, „*U.S. Defense Priorities and Policies: A Conversation With Secretary Mark T. Esper*“, December 13, 2019. < https://www.cfr.org/event/us-defense-priorities-and-policies-conversation-secretary-mark-t-esper-0 > [Žiūrėta 2020-05-18]
7. Stephen Castle, „*Pompeo Attacks China and Warns Britain Over Huawei Security Risks*“, May 8, 2019. < https://www.nytimes.com/2019/05/08/technology/pompeo-huawei-britain.html > [Žiūrėta 2020-05-18]
8. Derek B. Johnson „*Pompeo: Huawei deals threatens info-sharing with allies*“, February 22, 2019. < https://fcw.com/articles/2019/02/22/pompeo-huawei-info-sharing.aspx > [Žiūrėta 2020-05-18]
9. The White House, „*Remarks by Vice President Pence and Prime Minister Trudeau of Canada in Joint Press Statements*“, May 30, 2019. < https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-prime-minister-trudeau-canada-joint-press-statements-ottawa-canada/ > [Žiūrėta 2020-05-18]

Oficialūs dokumentai:

1. The White House, „*National Strategy to Secure 5G*“, March 2020. < https://www.whitehouse.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf > [Žiūrėta 2020-05-01]
2. U.S. Congress, „Federal Acquisition Supply Chain Security Act of 2018“, 2018. < https://www.congress.gov/bill/115th-congress/senate-bill/3085/text > [Žiūrėta 2020-05-02]
3.The White House, „Executive Order on Securing the Information and Communications Technology and Services Supply Chain“, 2019. < https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/ > [Žiūrėta 2020-05-02]
4. U.S. Congress, „Secure and Trusted Communications Networks Act of 2019“, March 12, 2020. < https://www.congress.gov/bill/116th-congress/house-bill/4998 > [Žiūrėta 2020-05-18]

Priedai

Priedas 1: Saugumizuojančių veikėjų kalbos aktų suvestinė

Kategorija	Saugumizuojantis veikėjas	Citata anglų k.	Vertimas į lietuvių kalbą	Interpretacija	Šaltinis/Data
Grėsmės	Prezidentas	1) „But, no, we find a tremendous security problem with respect to Huawei.“, - D. Trump	1) Bet, ne, mes įžvelgiame milžinišką saugumo problemą Huawei atžvilgiu.	Huawei 5G infrastruktūros įranga kelia didelę saugumo problemą JAV.	https://www.whitehouse.gov/briefings-statements/remarks-president-trump-prime-minister-trudeau-canada-bilateral-meeting-london-united-kingdom/ / 2019-12-03
		2) „But I do think it’s a security risk. It’s a security danger.“ „It is a security risk, in my opinion, in our opinion. We’re building it and we’ve started. But we’re not using Huawei.“, - D. Trump	2) Bet aš manau, jog tai yra saugumo rizika. Tai yra saugumo pavojus. Tai yra saugumo rizika, mano nuomone, mūsų nuomone. Mes tai statome ir esame pradėję. Bet mes nenaudojame Huawei.	Huawei 5G infrastruktūros įranga yra įvardijama kaip saugumo problema, pavojus. JAV diegia 5G tinklą, tačiau Huawei nėra jame nėra naudojamas.	https://www.whitehouse.gov/briefings-statements/remarks-president-trump-chancellor-merkel-federal-republic-germany-bilateral-meeting/ / 2019-12-04
		3) „Taking into account that secure Fifth Generation (5G) wireless communications networks will be vital to both future prosperity and national security“	3) Atsižvelgiant į tai, jog Penktosios kartos (5G) bevieliai komunikacijos tinklai bus gyvybiškai svarbūs ateities klestėjimui ir nacionaliniam saugumui.	Nesaugūs 5G tinklai kels grėsmę valstybės ekonomikai ir nacionaliniam saugumui. Įprasminamas egzistencinės grėsmės motyvas.	https://www.whitehouse.gov/briefings-statements/joint-statement-president-united-states-donald-j-trump-prime-minister-boyko-borissov-bulgaria/ / 2019-10-25

		4) „Romania is committed to working with the United States to combat the cybersecurity threats posed by Chinese vendors in 5G networks.“	4) Rumunija yra įsipareigojusi dirbti su JAV kovoje su kibernetinėmis grėsmėmis, kurias kelia kiniški tiekėjai 5G tinkluose.	Kiniški tiekėjai kelia kibernetinio saugumo grėsmes 5G tinkluose.	https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-celebrating-strong-partnership-romania/ / 2019-08-20
		5) „We also seek to avoid the security risks that accompany Chinese investment in 5G telecommunications networks.“, - D. Trump	5) Mes taip pat siekiame išvengti saugumo grėsmių, kurias lydi kiniškos investicijos į 5G telekomunikacijų tinklus.	Kiniškos investicijos į 5G telekomunikacijų tinklus kelia saugumo grėsmes.	https://www.whitehouse.gov/briefings-statements/joint-statement-president-united-states-donald-j-trump-president-romania-klaus-iohannis/ / 2019-08-20
		6) „At the same time, as we expand digital trade, we must also ensure the resilience and security of our 5G networks. This is essential to our shared safety and prosperity.“, - D. Trump	6) Tuo pačiu metu, kai mes plečiame skaitmeninę prekybą, mes taip pat privalome užtikrinti mūsų 5G tinklų atsparumą ir saugumą. Tai yra gyvybiškai svarbu mūsų bendram saugumui ir klestėjimui.	Nesaugus ir neatsparus 5G tinklas kelia grėsmę saugumui ir ekonomikai.	https://www.whitehouse.gov/briefings-statements/remarks-president-trump-g20-leaders-special-event-digital-economy-osaka-japan/ / 2019-07-25
		7) „Soon, much of our critical infrastructure will connect to these new networks. With those connections, the American homeland will be just a few clicks away from nation-state and criminal cyber actors with the capability and motivation to do Americans harm.“	7) Greitai, didžioji dalis mūsų kritinės infrastruktūros bus prijungta šių naujų tinklų. Su šiomis jungtimis, amerikiečių tėvynė bus kelių paspaudimų atstumu nuo valstybinių ir nusikalstamų kibernetinių veikėjų su pajėgumais ir motyvacija padaryti žalą amerikiečiams.	Valstybinių ir kriminalinių kibernetinių veikėjai išpuoliai kelia grėsmę JAV kritinei infrastruktūrai ir JAV piliečiams. Grėsmės šaltinis – valstybinių ir nusikalstamų veikėjų kibernetiniai išpuoliai.	https://www.whitehouse.gov/articles/raising-bar-protect-federal-government-private-sector-data/ / 2019-07-25

		8) „Secure 5G networks will absolutely be a vital link to America's prosperity and national security in the 21st century.“, - D. Trump	8) Saugūs 5G tinklai bus absoliučiai gyvybiškai svarbi grandis JAV klestėjimui ir nacionaliniam saugumui 21-ame amžiuje a.	Nesaugūs 5G tinklai kels grėsmę JAV ekonomikai ir nacionaliniam saugumui.	https://www.whitehouse.gov/briefings-statements/remarks-president-trump-united-states-5g-deployment/ / 2019-04-12
	Viceprezidentas	1) „To protect intellectual property rights and the privacy of our citizens and our national security, we've taken strong steps to curtail illegal behavior of Chinese companies like Huawei and ZTE. And we've urged our allies around the world to build secure 5G networks that don't give Beijing control of our most sensitive infrastructure and data as well“, - M. Pence	1) Kad apsaugoti mūsų piliečių intelektualinės nuosavybės teises ir mūsų nacionalinį saugumą, mes ėmėmės stiprių žingsnių sumažinti nelegalių Kinijos kompanijų kaip Huawei ir ZTE elgesį. Taip pat, mes toliau skatiname savo sąjungininkus pasaulyje diegti saugius 5G tinklus, kurie nesuteiktų Pekinui mūsų jautrios infrastruktūros ir informacijos kontrolės.	Grėsmės šaltiniu yra nurodoma Kinija ir su ja siejamos Huawei ir ZTE kompanijos. Dėl 5G kyla grėsmė JAV nacionaliniam saugumui, intelektualinės nuosavybės teisėms, jautrios infrastruktūros ir informacijos kontrolės praradimas.	https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-frederic-v-malek-memorial-lecture/ / 2019-10-24
		2) „Perhaps the greatest challenge NATO will face in the coming decades is how we must all adjust to the rise of the People's Republic of China. And adjust we must. For determining how to meet the challenge of Chinese 5G technology[...]“, - M. Pence	2) Turbūt didžiausias iššūkis, su kuriuo susidurs NATO artėjančiais dešimtmečiais, yra kaip mes visi turėsime prisitaikyti prie Kinijos augimo. O prisitaikyti mes privalome. Kad nuspręsti, kaip sutikti Kinijos 5G technologijų iššūkį[...].	Įvardijama Kinija, kurios 5G technologijos yra iššūkis. Kinijos kaip grėsmės motyvas.	https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-nato-engages-alliance-70/ / 2019-04-03
		3) „[...] we consider Huawei incompatible with the security interests of the United States of America“; „The simple fact is that the legal framework within China gives the Chinese government access to	3) Mes manome, jog Huawei yra nesuderinamas su JAV saugumo interesais. Paprastas faktas yra tai, jog Kinijos teisinė sistema Kinijos vyriausybei suteikia prieigą prie informacijos ir duomenų, surinktų kiniškų	Huawei 5G infrastruktūra yra nesuderinama ir prieštarauja JAV saugumo interesams, nes Kinijos teisinė sistema suteiks Kinijos vyriausybei prieigą	https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-prime-minister-trudeau-canada-joint-press-statements-

		information and data that is collected by Chinese companies like Huawei. And to have a 5G network worldwide that has access to sensitive national security information, we believe, is incompatible with the national security interests of the United States.“ , - M. Pence	kompanijų kaip Huawei. Ir turėti 5G tinklą pasaulio mastu, kuris suteikia prieigą prie jautrios nacionaliniam saugumui informacijos, mes tikime, yra nesuderinama su JAV nacionalinio saugumo interesais.	prie užsienio valstybių jautrios nacionaliniam saugumui informacijos.	ottawa-canada/ / 2019-05-30
		4) „It is well known that Chinese law requires Chinese telecom companies to provide Beijing’s vast security apparatus with access to any data that touches their network. And we believe, in the United States, that there’s no place for untrusted vendors anywhere in our secure 5G supply chain“, - M. Pence	4) Yra gerai žinoma, jog Kinijos įstatymas reikalauja kiniškų telekomunikacijų kompanijų suteikti plačiam Pekino saugumo aparatui prieigą prie bet kokių duomenų, kuriuos liečia jų tinklai. Ir mes tikime, jog JAV niekur nėra vietos nepatikimiems tiekėjams mūsų saugioje 5G tiekimo grandinėje.	Dėl Kinijos teisinės bazės, kiniškos telekomunikacijų įrangos tiekėjos yra grėsmė JAV 5G tiekimo grandinės saugumui.	https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-taoiseach-varadkar-ireland-joint-press-statement-dublin-ireland/ / 2019-09-03
	Valstybės sekretorius	1) „Huawei has at least two things that threaten the United States. One is that they – there’s a risk that they’ll steal American technology, and frankly, use those systems to invade your privacy. That is, they do telecommunications equipment that provide backbone services for networks, handsets all throughout the IT infrastructure and soon will be moving across the entire world with their new 5G rollout of their equipment. „But second, Huawei also presents a more traditional national security threat. Huawei is owned by the state of China and has deep connections to	1) „Huawei turi bent du dalykus, kurie kelia grėsmę JAV. Pirma yra tai, jog yra rizika, kad jie vogs amerikietiškas technologijas ir, atvirai, naudos tas sistemas įsibrauti į jūsų privatumą. Tai yra, jie gamina telekomunikacinę įrangą, kuri taps visos IT infrastruktūros, tinklų, mobiliųjų telefonų stuburu ir greit plėsis visame pasaulyje su 5G, kuriame bus jų įranga.“ Bet antra, Huawei taip pat kelia labiau tradicinę nacionalinio saugumo grėsmę. Huawei yra valdomas Kinijos valstybės ir turi gilius ryšius su jų žvalgybos tarnybomis. Tai turėtų duoti signalą	Kiniška 5G infrastruktūros įrangos gamintoja Huawei kelia technologijų vagystės ir privatumo įsibrovimo grėsmę. Taip pat, Huawei sąsajos su Kinijos vyriausybe kelia grėsmę nacionaliniam saugumui dėl galimo šnipinėjimo.	https://www.state.gov/remarks-to-the-future-farmers-of-america/ / 2019-03-04

		their intelligence service. That should send off flares for everybody who understands what the Chinese military and Chinese intelligence services do. We have to take that threat seriously.“, - M. Pompeo	kiekvienam kas supranta, ką Kinijos kariuomenė ir Kinijos žvalgybos tarnybos daro. Mes turime priimt šią grėsmę rimtai.		
		2) „5G networks will touch every aspect of our lives, including electrical grids, autonomous vehicles, smart manufacturing, medical treatments, and personal data. Given that 5G will support these and other vital applications, the United States does not assess it is possible to adequately mitigate risk by limiting the role of an untrusted vendors to only certain parts of the network.“, - M. Pompeo	2) 5G tinklai palies kiekvieną mūsų gyvenimo aspektą, įskaitant elektros tinklus, autonomines transporto priemones, išmanią gamybą, medicininį gydymą ir asmeninius duomenis. Atsižvelgiant, jog 5G rems šias ir kitas gyvybiškai svarbias sritis, JAV neįvertina, jog yra įmanoma sumažinti riziką ribojant nepatikimų tiekėjų rolę tik konkrečiuose tinklo dalyse.	Nepatikimi 5G infrastruktūros tiekėjai kelia riziką kritinei infrastruktūrai, net jei ir yra ribojama jų įranga tam tikrose tinklo dalyse.	https://www.state.gov/united-states-welcomes-the-eus-acknowledgement-of-the-unacceptable-risks-posed-by-untrusted-5g-suppliers/ / 2020-01-30
		3) „[...] we must adapt our alliance to confront emerging threats too, whether that’s Russian aggression, uncontrolled migration, cyber attacks, threats to energy security, Chinese strategic competition – including technology in 5G“, - M. Pompeo	4) [...] Mes privalome pritaikyti savo aljansą atremti kylančias grėsmes taip pat, ar tai būtų Rusijos agresija, nekontroliuojama migracija, kibernetinės atakos, grėsmės energetiniui saugumui, Kinijos strateginė konkurencija – įskaitant technologiją 5G.	NATO, įskaitant ir pačiai JAV, strateginė Kinijos konkurencija, kuri pasireiškia 5G technologijose, yra grėsmė.	https://www.state.gov/remarks-at-the-meeting-of-the-north-atlantic-council-in-foreign-ministers-session-1/ / 2019-04-04
		4) „China’s National Intelligence Law makes clear that the Chinese Communist Party (CCP) can force any 5G supplier headquartered in China to turn over data and take other actions in secret.“ „With 5G capabilities, the CCP could use Huawei or ZTE’s access to steal private or proprietary	4) Kinijos Nacionalinis Žvalgybos Įstatymas aiškiai nurodo, jog Kinijos Komunistų Partija (KKP) gali priversti kiekvieną Kinijoje įsikūrusį 5G tiekėją tiekti informaciją ir imtis kitų veiksmų slapčia. Su 5G pajėgumais, KKP galėtų pasinaudoti Huawei ar ZTE prieiga, jog pavogtų privačią ar jiems	Kiniškų 5G tiekėjų infrastruktūra yra grėsmė, nes Kinijos vyriausybė tiekėjus naudotų kaip įrankį šnipinėjimui bei kritinių visuomenės funkcijų sutrikdymui.	https://www.state.gov/europe-must-put-security-first-with-5g/ / 2019-12-02

		information, or use “kill switches” to disrupt critical future applications like electrical grids and telesurgery centers.“, - M. Pompeo	palankią informaciją arba panaudoti avarinį išjungimą siekiant sutrikdyti ateities kritines funkcijas visuomenėje, kaip elektros tinklus ir telechirurgijų centrus.		
		5) „The company is deeply tied not only to China but to the Chinese Communist Party. And that connectivity, the existence of those connections, puts American information that crosses the networks at risk“, - M. Pompeo	Kompanija yra giliai susieta su ne tik Kinija bet ir Kinijos Komunistų Partija(KPP). Ir tas jungiamumas, tų jungčių egzistavimas kelia riziką amerikietiškai informacijai, kuri kertas tas jungtis.	Huawei 5G infrastruktūra keltų grėsmę JAV informaciniam saugumui dėl įmonės sąsajų su Kinija ir KPP.	https://www.cnbc.com/2019/05/23/cnbc-transcript-united-states-secretary-of-state-mike-pompeo-speaks-with-cnbcs-squawk-box-today.html / 2019-03-23
		6) „If a country adopts Huawei technology and puts it in some of their critical information systems, we won't be able to share information with them, we won't be able to work alongside them. In some cases, there's a risk we won't be able to co-locate American resources, American embassies and American military outposts.", - M. Pompeo	Jei valstybė priims Huawei technologiją ir įdiegs ją į kai kurias kritinės informacijos sistemas, mes nebegalėsime dalintis informacija su ja, mes nebegalėsime dirbti greta jų. Kai kuriais atvejais, yra rizika, jog mes negalėsime skirti amerikietiškų resursų, amerikietiškų ambasadų ir amerikietiškų karinių forpostų.	Huawei 5G infrastruktūra sąjungininkų kritinėje infrastruktūroje keltų grėsmę informacijos dalijimuisi su JAV	https://fcw.com/articles/2019/02/22/pompeo-huawei-info-sharing.aspx / 2019-02-22
		6) „Huawei and other Chinese state-backed tech companies are Trojan horses for Chinese intelligence“, - M. Pompeo	6) Huawei ir kitos Kinijos valstybės remiamos technologijų kompanijos yra Trojos arkliai Kinijos žvalgybos tarnyboms.	Kiniškų 5G technologijų infrastruktūra kelia Kinijos žvalgybos tarnybų šnipinėjimo grėsmę.	https://lu.usembassy.gov/secretary-pompeo-and-secretary-esper-speak-at-munich-security-conference-2020/ / 2020-02-19
		7) „Insufficient security will impede the United States’ ability to share certain information within trusted networks.“, - M. Pompeo	7) Nepakankamas saugumas kliudys JAV dalintis tam tikra informacija patikimuose tinkluose.	Nesaugūs 5G tinklai kels grėsmę jautrios informacijos dalijimuisi tarp JAV ir sąjungininkių.	https://www.nytimes.com/2019/05/08/technology/pompeo-huawei-britain.html / 2019-05-08

		8) „With the #5G revolution, the security of communications networks is all the more critical to the national security of the U.S. and our partners and allies.“, - M. Pompeo	8) Dėl #5G revoliucijos, komunikacijos tinklų saugumas yra dar labiau kritiškai JAV, mūsų partnerių ir sąjungininkų nacionaliniam saugumui.	5G tinklai yra kritiškai svarbūs JAV nacionaliniam saugumui.	https://twitter.com/SecPompeo/status/1100600759383670785 / 2019-02-27
	Gynybos sekretorius	1) „Reliance on Chinese 5G vendors, for example, could render our partners' critical systems vulnerable to disruption, manipulation, and espionage. It could also jeopardize our communication and intelligence sharing capabilities, and by extension, our alliances.“, - M. Esper	1) Priklausomybė nuo kiniškų 5G tiekėjų, pavyzdžiui, galėtų daryti mūsų partnerių kritines sistemas pažeidžiamas trikdymams, manipuliacijai ir šnipinėjimui. Taip pat, tai keltų grėsmę mūsų komunikacijai ir žvalgybinės informacijos galimybėmis, bei visam aljansui.	Priklausomybė nuo kiniškų 5G tiekėjų kelia grėsmę valstybių kritinei infrastruktūrai dėl jos pažeidžiamumo, t.y., trikdymo, manipuliavimo ir šnipinėjimo. Taip pat, kyla grėsmė žvalgybinės informacijos dalijimuisi su sąjungininkais.	https://www.defense.gov/Newsroom/Speeches/Speech/Article/2085577/as-prepared-remarks-by-secretary-of-defense-mark-t-esper-at-the-munich-security/ / 2020-02-15
		2) „Our ability to share information and operate on common communications networks serves as a force multiplier – but, it also comes with increased risk. To guard against this, we must help our allies develop their own cyber resiliency. China is the greatest threat. And the Chinese government is perpetrating the greatest intellectual property theft in human history. Chinese businesses are in thrall to the government, and any nation that partners with Chinese firms to build 5G networks put their own networks at risk. This not only	2) Mūsų gebėjimas dalintis informacija ir veikti bendruose komunikacijų tinkluose tarnauja kaip galios daugiklis – bet, tai taip pat ateina su padidėjusia rizika. Siekiant apsisaugoti nuo to, mes privalome padėti savo sąjungininkams vystyti jų pačių kibernetinį atsparumą. Kinija yra didžiausia grėsmė. Ir Kinijos vyriausybė nusikalstamai vykdo didžiausią intelektinės nuosavybės vagystę žmonijos istorijoje. Kinijos verslai yra kontroliuojami vyriausybės ir kiekviena tauta, kuri bendradarbiauja	Kiniški 5G tinklai kelia grėsmę ne tik sąjungininkų, taigi ir JAV, informacijos dalijimuisi ar karinei sąveikai, bet kartu stato į pavojų ir verslo institucijas.	https://www.defense.gov/Explore/News/Article/Article/1966758/esper-describes-dods-increased-cyber-offensive-strategy/ / 2019-09-20

		jeopardizes military interoperability and intelligence sharing, but can also compromise commercial institutions such as banks, hospitals and media outlets.“, - M. Esper	su Kinijos firmomis statant 5G tinklus, rizikuoja savo pačių tinklais. Tai ne tik kelia pavojų karinei sąveikai, bet ir tokioms verslo institucijoms kaip bankai, ligoninės ar žiniasklaidai.		
		3) „NATO members must be vigilant in adopting technologies and products such as 5G that could undermine our ability to share intelligence, conduct planning, or communicate securely across the alliance.“, - M. Esper	NATO narės privalo būti budrios diegdamos technologijas ir produktus kaip 5G, kurie galėtų pakenti mūsų galimybėms dalintis žvalgybine informacija, atlikti planavimus ar saugiai komunikuoti aljanse.	Nesaugūs 5G tinklai kelia grėsmę NATO narių, įskaitant JAV, informaciniam saugumui ir planavimui.	https://www.cfr.org/event/us-defense-priorities-and-policies-conversation-secretary-mark-t-esper-0 / 2019-12-13
	Valstybės departamento Kibernetinių ir Tarptautinių Komunikacijų bei Informatikos Politikos Sekretoriaus padėjėjo pavaduotojas	1) „The security of information and communications technology networks and services is critical to the national security and prosperity of all nations. These networks and services are attractive targets for foreign adversaries and other bad actors. The United States wants to ensure that we and our partners and allies maintain secure and reliable communications networks and supply chains to reduce the risks of unauthorized access and malicious cyber activity. To this end, the United States is asking other governments and the private sector to consider the threat posed by Huawei and other Chinese information technology companies “, - R. Strayer	1) Informacinių ir komunikacinių technologijų tinklų ir paslaugų saugumas yra kritinis visų tautų nacionaliniam saugumui ir klestėjimui. Šie tinklai ir paslaugos yra patrauklūs taikiniai priešiškoms valstybės ir kitiems blogiems veikėjams. JAV nori užtikrinti, jog mes, mūsų partneriai bei sąjungininkai išlaikytume saugius ir patikimus komunikacijų tinklus bei tiekimo grandines, jog sumažintume nesankcionuotos prieigos ir žalingos kibernetinės veiklos rizikas. Siekiant tai užtikrinti, JAV prašo kitų vyriausybių ir privataus sektoriaus apsvarstyti Huawei ir kitų kiniškų informacinių technologijų kompanijų keliamą grėsmę.	Nesaugūs 5G tinklai kelia grėsmę JAV nacionaliniam saugumui ir ekonomikai. Grėsmės šaltinis – priešiškos valstybės ir blogi veikėjai, konkrečiai – dide kiniškos informacinių technologijų kompanijos. Grėsmė nacionaliniam saugumui kiltų dėl nesaugių ir nepatikimų 5G tinklų bei tiekimo grandinių.	https://www.state.gov/remarks-at-press-availability/ / 2019-02-26
		2) „Well, fundamentally the challenge will be how do you secure	2) Na, iš esmės, iššūkis bus kaip tu apsaugosi infrastruktūros	Kiniškos įrangos tiekimo kompanijos	https://www.youtube.com/watch?v=nnmTl

		software updates to the infrastructure into the firmware that's on inside the networks when it's being supplied by companies that are under the control or domination of the Chinese Communist Party.", - R. Strayer	programinės sistemos atnaujinimus tinklų įrangoje, kuri yra tiekiama kompanijų, kontroliuojamų ar dominuojamų Kinijos Komunistų Partijos.	yra grėsmė 5G infrastruktūros saugumui, nes jos yra kontroliuojamos Kinijos Komunistų Partijos.	HwPGVg / 2020-01-09
		3) „Those connections are going to empower a vast array of new critical services, from autonomous vehicles and transportation systems to telemedicine to automated manufacturing as well as empowering our traditional critical infrastructure such as the provision of electricity through the smart grid. With all these services relying on 5G the stakes for safeguarding our critical networks could not be higher. „If Chinese companies continue to build the underlying 5G infrastructure they will be in a better position to take advantage of their access to this data. Those vendors, of course, could be asked to play a role in undermining network security to, for example, steal personal information or intellectual property or to conduct espionage or to disrupt the critical services", - R. Strayer	3) Šios jungtys įgalins daugybę naujų kritinių paslaugų, nuo autonominių automobilių ir transporto sistemų iki medicinos iki automatizuotos pramonės, taip pat kaip ir įgalins mūsų tradicinę kritinę infrastruktūrą, kaip elektros tiekimą per išmanų tinklą. Visoms šioms paslaugoms remiantis 5G, apsaugoti mūsų kritinius tinklus negalėtų būti svarbiau. Jei kiniškos kompanijos tęs pamatinės 5G infrastruktūros statybas, jie bus geresnėje pozicijoje pasinaudoti prieiga prie šios informacijos. Šių tiekėjai, žinoma, gali būti paprašyta pažeisti tinklo saugumą siekiant, pavyzdžiui, pavogti asmeninę informaciją ar intelektinę nuosavybę, vykdyti šnipinėjimą ar trikdyti kritines paslaugas.	Nesaugūs 5G ryšys yra grėsmė JAV kritinei infrastruktūrai ir kritinėms paslaugoms. Grėsmę 5G tinklo saugumui kelia kiniškos kompanijos, kurios galės naudotis neteisėta prieiga prie informacijos siekiant kenksmingos veiklos, kaip šnipinėjimas, informacijos vagystė.	https://www.state.gov/press-briefing-with-deputy-assistant-secretary-robert-strayer/ / 2019-07-11
		4) „Along with deterring, countering, and contesting malicious foreign state behavior and improving network defenses, we also must focus on the security of our	4) Greta žalingo užsienio valstybės elgesio atgrasymo ir užkirtimo, bei tinklų gynybos gerinimo, mes taip pat privalome skirti dėmesį mūsų telekomunikacinių tinklų ir tiekimo	5G tinklai – gyvybiškai svarbūs, todėl yra pabrėžiama ypatinga svarba apsaugoti tiekimo	https://www.state.gov/remarks-at-the-2019-internet-governance-forum-usa-

		telecommunications networks and supply chains, especially when it comes to the Fifth Generation of wireless technology, or 5G. Given 5G's scope, the stakes for safeguarding these vital networks could not be higher.", - R. Strayer	grandinių saugumui, ypač kai kalbame apie Penktosios Kartos bevielę technologiją, ar 5G. Atsižvelgiant į 5G apimtį, apsaugoti šiuos gyvybiškai svarbius tinklus yra nepaprastai svarbu.	grandinę ir pačius tinklus.	conference/ / 2019-07-25
		5) „So one adversary that can undermine the integrity of the network or the availability of the network could well cause those critical infrastructure of the future that relies on 5G to be disrupted and the citizen services that are being supplied by it to be disrupted as well.", - R. Strayer	5) Taigi priešininkas, kuris gali pakenkti tinklo integralumui arba tinklo prieinamumui, gali sutrikdyti 5G ryšiu paremtą ateities kritinę infrastruktūrą, taip pat kaip ir sutrikdyti šiuo ryšiu teikiamas paslaugas piliečiams.	Nesaugi 5G infrastruktūra kelia kritinės infrastruktūros ir paslaugų trikdymo grėsmę.	https://www.state.gov/telephonic-press-briefing-with-deputy-assistant-secretary-robert-strayer-cyber-and-international-affairs-and-information-policy-bureau-of-economic-and-business-affairs/ / 2019-10-15
		6) „So 5G will really start touching all parts of our lives because it will be the underlying infrastructure for so much of the critical services that are provided to the public. So if a 5G network fails, there would be significant ramifications for all parts of society.", - R. Strayer	6) Taigi 5G tikrai pradės liesti visas mūsų gyvenimo dalis, nes tai bus pamatinė infrastruktūra daugumai visuomenei teikiamų kritinių paslaugų. Jei 5G tinklai žlugtų, tai turėtų reikšmingų neigiamų pasekmių visoms visuomenės dalims.	Neapsaugoti 5G tinklai kelia grėsmę visuomenei, kurio sutrikdymas kelia riziką kritinės infrastruktūrai ir kritinėms paslaugoms.	https://www.state.gov/press-briefing-with-deputy-assistant-secretary-robert-strayer-cyber-and-international-affairs-and-information-policy-bureau-of-economic-and-business-affairs/ / 2019-04-10
		7) „The security of Information Communications Technology, or ICT, is an essential element of national security. The networks and services that comprise ICT play a critical role in the safety, security and prosperity of each nation.	7) Informacinių ir Telekomunikacinių Technologijų, ar ITT, saugumas yra esminis nacionalinio saugumo elementas. ITT sudarantys tinklai ir paslaugos vaidina kritinę rolę	Nesaugūs 5G tinklai kelia grėsmę nacionaliniam saugumui ir ekonomikai.	https://www.state.gov/press-briefing-with-deputy-assistant-secretary-robert-strayer-cyber-and-international-

		[...]equipment vendors that are subject to unchecked or extrajudicial control by a foreign power. These vendors could be ordered to undermine network security, to skim personal information, conduct espionage, or to disrupt those critical services that are provided by the 5G network. A significant cause for concern are a number of Chinese laws that compel their companies to cooperate with intelligence and security services without independent judicial controls.“, - R. Strayer	kiekvienos tautos saugume ir klestėjime. [...] įrangos tiekėjai, kurie yra gali būti kontroliuojami užsienio galios neprižiūrimai arba be teismo sprendimo. Šiems pardavėjams gali būti įsakyta pakenkti tinklo saugumui, naršyti asmeninį informaciją, vykdyti šnipinėjimą ir sutrikdyti tas kritines paslaugas, kurios yra teikiamos 5G tinklo pagrindu. Reikšminga susirūpinimo priežastis – skaičius Kinijos įstatymų, verčiančių jos įmonėms bendradarbiauti su žvalgybos ir saugumo tarnybomis be nepriklausomos teisinės kontrolės.	Grėsmę 5G tinklų saugumui kelia nepatikimi ir užsienio vyriausybių kontroliuojami įrangos tiekėjai, kuriems gali būti nurodyti vykdyti žalingą veiklą. Grėsmės šaltinis – kiniškos telekomunikacijų įmonės dėl Kinijos teisinės bazės, menančios, jog tos įmonės yra kontroliuojamos vyriausybės.	affairs-and-information-policy-bureau-of-economic-and-business-affairs-2/ / 2019-05-08
Netipinės priemonės	Prezidentas	1) „To guarantee that the infrastructure of the future is built in a safe, transparent, and accountable manner, the United States is working with a range of partners, including Australia and Japan, to create the Blue Dot Network, a major initiative to ensure countries around the world to have access to private sector-led, sustainable, and trustworthy options for high-quality infrastructure development, and that’s what’s happening.“, - D. Trump	1) Norint užtikrinti, jog ateities infrastruktūra būtų pastatyta saugiu, skaidriu ir atskaitingu būdu, JAV dirba su skaičiumi partneriais, įskaitant Australiją ir Japoniją, siekiant sukurti Mėlyno Taško Tinklą (angl. *Blue Dot Network*), svarbią iniciatyvą, skirtą užtikrinti, jog valstybės pasaulyje turėtų prieigą prie privataus sektoriaus vedamų, tvarių ir patikimų aukštos kokybės infrastruktūros vystymo pasirinkimų ir tai vyksta.	Pabrėžiamas daugiašalis Mėlynojo Taško Tinklo (angl. *Blue Dot Network*), iniciatyvos vystymas, kuria siekiama kurti standartus ir vertinti infrastruktūros projektus.	https://www.whitehouse.gov/briefings-statements/remarks-president-trump-prime-minister-modi-india-joint-press-statement-2/ / 2019-01-25
		2) „It is critical that we use safe and trustworthy technology providers, components, and supply chains.“, - D. Trump	„Yra kritiškai svarbu, jog mes naudotume saugius ir patikimus technologijų tiekėjus, komponentus ir tiekimo grandinę.“	Netipinė priemonė – 5G infrastruktūroje naudoti tik patikimus	https://www.whitehouse.gov/briefings-statements/remarks-president-trump-

				tiekėjus, komponentus ir tiekimo grandines.	president-niinisto-republic-finland-joint-press-conference/ / 2019-10-02
	Viceprezidentas	1) „We'll also continue to take steps to promote alternatives in 5G, in our country and in Canada and all across our allies. We believe we can create and are creating viable alternatives to Huawei that don't compromise privacy, that don't compromise security.“, - M. Pence	1) Mes taip pat žengiame pirmyn skatindami 5G alternatyvas mūsų valstybėje, Kanadoje ir pas visas sąjungininkes. Mes tikime, jog galime sukurti ir kuriame perspektyvias alternatyvas Huawei, kurios nekelia pavojaus privatumui, nekelia pavojaus saugumui.	Pabrėžiamas siekis rinktis alternatyvius 5G infrastruktūros tiekėjus, o ne Huawei.	https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-prime-minister-trudeau-canada-joint-press-statements-ottawa-canada/ / 2019-05-30
		2) „[...] we're working with telecom companies across the world to develop 5G alternatives to Huawei.“, - M. Pence	1) Mes dirbame su telekomunikacijų įmonėmis globaliai vystadami 5G alternatyvas Huawei.	Pabrėžiama reikiamybė bendradarbiauti su 5G privačiu sektoriumi globaliai, siekiant alternatyvos Huawei.	https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-taoiseach-varadkar-ireland-joint-press-statement-dublin-ireland/ / 2019-09-03
		3) „And we also spoke today — and perhaps we can again — about the United States' concerns about 5G and our desire to work with Iceland and other freedom-loving nations to find alternatives to essentially China's state-based 5G operation.“, - M. Pence	3) „Ir mes taip pat kalbėjomės šiandien – ir, galbūt, galėsime dar kartą – apie JAV susirūpinimą 5G ir mūsų troškimą dirbti kartu su Islandija ir kitomis laisvę mylinčiomis tautomis rasti alternatyvas iš esmės Kinijos valstybinės 5G operacijai“.	Kiniškų telekomunikacijų diegiamas 5G ryšys – Kinijos valstybinė operacija, kuriai reikia rasti alternatyvą.	https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-prime-minister-jakobsdottir-iceland-bilateral-meeting-keflavik-iceland/ / 2019-09-04
		4) „The leaders agreed that the development of 5G networks will bring economic benefits as well as security risks, and pledged to work closely together to advance	4) „Lyderiai sutiko, jog 5G tinklų vystymas atneš ekonominę naudą taip pat kaip saugumo grėsmes, bei įsipareigojo artimai bendradarbiauti remiant Prahos 5G Saugumo	Prahos 5G Saugumo Protokolų įgyvendinimas tarptautiniu lygmeniu kaip netipinė priemonė	https://www.whitehouse.gov/briefings-statements/readout-vice-president-mike-pences-meeting-

		implementation of the Prague Protocols on 5G Security to ensure that malign actors are kept out of developing our critical infrastructure.“	Protokolų įgyvendinimą siekiant užtikrinti, kad piktybiški veikėjai būtų saugomi nuo mūsų kritinės infrastruktūros vystymo.“	apsaugoti 5G ryšio tinklus nuo priešiškų veikėjų.	president-andrzej-duda-poland/ / 2019-09-02
	Gynybos sekretorius	1) „To counter this, we are encouraging allied and U.S. tech companies to develop alternative 5G solutions, and we are working alongside them to test these technologies at our military bases as we speak.“, - M. Esper	1) Tam atremti, mes raginame sąjungininkų ir JAV technologijų kompanijas vystyti alternatyvius 5G sprendimus, bei dirbame greta jų testuodami šias technologijas mūsų karinėse bazėse esamuoju metu.	Netipinė priemonė – bendradarbiavimas su technologijų kompanijomis siekiant alternatyvos Huawei 5G technologijoms.	https://lu.usembassy.gov/secretary-pompeo-and-secretary-esper-speak-at-munich-security-conference-2020/ / 2020-02-19
	Valstybės departamento Kibernetinių ir Tarptautinių Komunikacijų bei Informatikos Politikos Sekretoriaus padėjėjo pavaduotojas	1) „What we really need is trusted vendors. Those vendors are European Nokia and Ericsson, as well as Samsung. And we need to have a dynamic innovative future in telecommunications technology that will meet all of our needs for the future [...] that we can have a shared prosperity and shared security that will not cause our data to be exfiltrated into the hands of authoritarian governments.“, - R. Strayer	1) Ko mums iš tikro reikia tai patikimų tiekėjų. Tie tiekėjai europietiška Nokia ir Ericsson, taip pat Samsung. Ir mums reikia turėti dinamišką inovatyvią telekomunikacinių technologijų ateitį, kuri atitiks mūsų poreikius, [...] jog mes galėtume turėti bendrą klestėjimą ir saugumą, kuris neleis mūsų duomenims būti išfiltruotiems į autoritarinių vyriausybių rankas.	Išskiriama netipinė priemonė – naudoti tik patikimus 5G infrastruktūros tiekėjus – Nokia, Ericsson ar Samsung – kaip alternatyvą Kinijos tiekėjus.	https://www.youtube.com/watch?v=nnmTlHwPGVg / 2020-01-09
		2) „It’s going to be very important for us to have a risk-based approach to carefully evaluate the hardware and software equipment vendors that are going to supply this next generation of networks. We should evaluate closely and exclude vendors that are subject to the control of a foreign government that has no meaningful checks and balances on	2) Mums bus labai svarbu turėti rizika grįstą prieigą, jog galėtume atsargiai įvertinti įrangos ir programinės sistemos pardavėjus, kurie tieks šiems naujos kartos tinklams. Mes turėtume atidžiai įvertinti ir išskirti užsienio vyriausybių kontroliuojamus tiekėjus, kuriose nėra reikšmingų stabdžių ir atsvarų jų galiai priversti	Netipinė priemonė – vertinti, taikyti kriterijus ir uždrausti tuos 5G infrastruktūros įrangos tiekėjus, kurie yra kontroliuojami užsienio valstybių.	https://www.state.gov/press-briefing-with-deputy-assistant-secretary-robert-strayer/ / 2019-07-11

		its power to compel cooperation of those vendors with its intelligence and security agencies.“, - R. Strayer	tuos tiekėjus bendradarbiauti su žvalgybos ir saugumo tarnybomis.		
		3) „The United States is urging countries to adopt a risk-based security framework for the construction of all elements of 5G networks, including a careful evaluation of hardware and software equipment vendors in the supply chain. We urge nations to consider whether vendors could be ordered to undermine network security—to steal personal information, conduct industrial espionage, disrupt critical services, or conduct cyber-attacks.“, - R. Strayer	3) JAV skatina kitas valstybes priimti rizika grįstą saugumo sistemą, kuria būtų vertinami pardavėjai 5G infrastruktūros tiekimo grandinėje. Mes raginame tautas apsvarstyti, ar tiems tiekėjams galėtų būti nurodyta pakenkti tinklų saugumui – vogti asmeninę informaciją, vykdyti pramoninę žvalgybą, trikdyti kritines paslaugas ar vykdyti kibernetines atakas.	Netipinė priemonė – skatinti kitas valstybes taikyti gerinti komunikacinio saugumo standartus, atsižvelgiant į tiekėjus.	https://www.state.gov/remarks-at-the-2019-internet-governance-forum-usa-conference/ / 2019-07-25
		4) „[...] the next step, of course, is to have mitigation and security measures. In that regard, we think it’s very important to build off of this baseline that there be security measures that accurately and adequately assess and address the ability of a state actor to compromise a supplier or vendor of 5G technology.“, - R. Strayer	4) [...] kitas žingsnis, žinoma, turėti rizikos mažinimo ir saugumo priemones. Šiuo atžvilgiu mes manome, jog yra labai svarbu sukurti pagrindą, jog jame būtų saugumo priemonės, kurios taikliai ir adekvačiai įvertintų ir adresuotų valstybinio veikėjo galimybę kompromituoti 5G technologijos tiekėją ar pardavėjas.	Netipinė priemonė – apsaugos sistema, kuri leistų įvertinti valstybinių veikėjų įtaką ir galimybę kompromituoti 5G technologijų tiekėjus.	https://www.state.gov/telephonic-press-briefing-with-deputy-assistant-secretary-robert-strayer-cyber-and-international-affairs-and-information-policy-bureau-of-economic-and-business-affairs/ / 2019-10-15
		5) „We are urging countries around the world to carefully consider how they adopt a risk-based framework for security relative to the construction of 5G networks. That includes looking at the supply chain	5) Mes raginame viso pasaulio šalis atidžiai apsvarstyti, kaip jos priima rizika pagrįstą saugumo sistemą, susijusią su 5G tinklų statybą, įskaitant pardavėjų, kurie būtų jų 5G infrastruktūros dalis, tiekimo grandinės peržiūrą.	Netipinė priemonė – skatinti kitas valstybes priimti rizika grįstą 5G tinklų saugumo sistemą, kurioje būtų atsižvelgiama į tinklo komponentų pardavėjų	https://www.state.gov/press-briefing-with-deputy-assistant-secretary-robert-strayer-cyber-and-international-affairs-and-

		of the vendors that would be part of their 5G infrastructure. In particular, we think it's very important that countries deploying 5G networks consider the relationship between a foreign government where a vendor is headquartered and the companies themselves in that country.", - R. Strayer	Konkrečiai, mes manome, jog yra labai svarbu, kad 5G tinklus diegiančios valstybės apsvarstytų santykius tarp užsienio vyriausybės, kurioje yra įsikūręs pardavėjas, ir pačių bendrovių toje šalyje.	tiekimo grandinę ir jų santykio su vyriausybe, kurioje pardavėjai yra įsikūrę.	information-policy-bureau-of-economic-and-business-affairs/ / 2019-04-10
		6) „As countries around the world make their decision about how to build out 5G, we urge them to refer to these best practices that are embodied in the Prague Proposals, as it's called, so that they can incorporate those security ideas into the critical networks from the very start, before they build them out.", - R. Strayer	6) Kai viso pasaulio valstybės priima savo sprendimą dėl to, kaip įsirengti 5G, mes juos skatiname tai daryti atsižvelgiant į šias geriausias praktikas, įkūnytas Prahos pasiūlymuose, kaip jie pavadinti, jog jie galėtų inkorporuoti tas saugumo idėjas į kritinius tinklus nuo pačio starto, prieš juos pradedant statyti.	Netipinė priemonė – skatinti kitas šalis priimti Prahos pasiūlymus diegiant 5G tinklus.	https://www.state.gov/press-briefing-with-deputy-assistant-secretary-robert-strayer-cyber-and-international-affairs-and-information-policy-bureau-of-economic-and-business-affairs-2/ / 2019-05-08

Summary

The latest development of a state-of-the-art fifth-generation wireless (5G) technology has seen its beginning of deployment in the spring of 2019. Despite common understanding of upcoming economic and societal benefits this technology will bring, countries have also emphasized the question of the importance of securing 5G networks for its crucial part in critical infrastructure. One of the main questions regarding the security of 5G has been the trustworthiness of Chinese 5G infrastructure suppliers, mainly Huawei, to national security. The so-called Huawei debate has highlighted a politization of 5G supply chains and different stance of countries regarding securitization, the U.S. being inclined to securitize the matter move visibly than others. For this reason, the purpose of this thesis was to find out how did the 5G network securitization process in the U.S. was implemented and why.

To answer this, the qualitative analysis of five U.S. high ranking political officers' speech acts was carried out in order to find out how 5G problems were constructed as threats to security. Also, three official documents/legal acts were analyzed to explore what kind of exceptional measures were legally adopted to secure 5G from the declared problems in the official/legal discourse. The following findings of the analysis were concluded:

The first finding is that the securitization process of 5G in the US was concluded, meaning that the speech acts of securitizing actors called out political decisions which moved regarded problems of 5G to the national security agenda, and were not only declarative by nature. 5G problems were presented as extraordinary threats to referent objects such as national security, economy, or critical infrastructure. Therefore, extraordinary measures were taken to deal with the threats, as the document analysis shows.

Furthermore, the securitization of 5G in the U.S. is tied to Chinese 5G infrastructure manufacturer Huawei and China's factor. As the analysis shows, Huawei and its supposed dependency on China's Government was presented as a main source of threat. It can be argued, in one hand, the securitization occurred to prevent from possible threats that would be caused by Chinese 5G technologies if installed in the U.S. networks. In addition, one of the reasons for the securitization could be named as the geopolitical and strategic U.S.-China competition in the field of technology.

Finally, as the analysis points, the security of 5G networks in the U.S. is understood not only on national but also on international level. It is believed that unsecure 5G networks would cause harm to U.S. foreign policy and military cooperation with its allies. This gives an argument to explain the U.S.

intent to persuade other countries to adopt 5G development security mechanisms regarding suppliers, to apply international 5G security standards as named in the Prague 5G Security proposals, and also choose alternatives to Huawei 5G technology.